Mathematics of Public Key Cryptography. Version 2.0

Steven D Galbraith

October 31, 2018

Contents

Preface

The book has grown from lecture notes of a Master's level course in mathematics, for students who have already attended a cryptography course along the lines of Stinson's or Smart's books. The book is therefore suitable as a teaching tool or for self-study. However, it is not expected that the book will be read linearly. Indeed, we discourage anyone to start reading with either Part 1, Part 2 or Part 3. The best place to start, for an understanding of mathematical cryptography, is probably Part 5 (replacing all references to "algebraic group G" by $\mathbb{F}_p^*$). For an introduction to RSA and Rabin one could start reading at Part 6 and ignore most references to the earlier parts.

Exercises are distributed throughout the book, so that the reader performing self-study can do them at precisely the right point in their learning. Readers may find exercises denoted by ★ somewhat more difficult than the others, but it would be dangerous to assume that everyone's experience of the exercises will be the same.

Despite our best efforts, it is inevitable that the book will contain errors and misleading statements. Errata will be listed on the author's webpage for the book. Readers are encouraged to being any errors to the attention of the author.

I would like to thank Royal Holloway, University of London and the University of Auckland, each of which in turn was my employer for a substantial time while I was writing the book. I also thank the EPSRC, who supported my research with an advanced fellowship for the first few years of writing the book.

The book is dedicated to Siouxsie and Eve, both of whom tolerated my obsession with writing for the last four years.

Steven Galbraith
Auckland
2011

Notation

Basic mathematical notation

$\varnothing$	The empty set
$\#S$	The number of elements in the finite set S
$S - T$	Set difference of sets S and T
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	integers, rationals, reals and complex numbers
$\mathbb{N}$, $\mathbb{Z}_{>0}$	Natural numbers
$\mathbb{Z}/r\mathbb{Z}$	Integers modulo r
$\mathbb{F}_q$	Finite field of $q = p^m$ elements
$\mathbb{Z}_p$, $\mathbb{Q}_p$	p-adic ring, field, where p (sometimes also called l) is a prime.
$\langle g_1, \ldots, g_n \rangle$	Group generated by $g_1, \ldots, g_n$
$(g_1, \ldots, g_n)$	Ideal generated over a ring R by $g_1, \ldots, g_n \in R$
$\varphi(n)$	Euler phi function
$\zeta(n)$	Riemann zeta function
$\lambda(N)$	Carmichael lambda function
$a \mid b, a \nmid b$	b is/is not a multiple of a
q_n, r_n	Quotient and remainder in n-th step of Euclidean algorithm
s_n, t_n	Numbers arising in the extended Euclidean algorithm to compute $\gcd(a, b)$, they satisfy $r_n = as_n + bt_n$
h_n/k_n	Convergents of a continued fraction expansion
$\log_2(x)$	Logarithm to base 2
$\log(x)$	Natural logarithm
$[0, 1]$	$\{x \in \mathbb{R} : 0 \leq x \leq 1\}$
$\approx$	Approximately equal (we do not give a precise definition), such as $\pi \approx 3.1415$
$(a_{l-1} \ldots a_1 a_0)_2$	Binary representation of an integer a
$\underline{v}, \underline{w}$	Vectors
$\underline{0}$	Zero vector
$\underline{e}_i$	i-th unit vector
I_n	$n \times n$ identity matrix
$\langle \underline{x}, \underline{x} \rangle$	Inner product
$\|\underline{x}\|$	Euclidean length of a vector (2 norm)
$\| \cdot \|_a$	ℓ_a-norm for $a \in \mathbb{N}$
$\mathrm{span}\{\underline{v}_1, \ldots, \underline{v}_n\}$	Span of a set of vectors
$\mathrm{rank}(A)$	Rank of a matrix A
$M_n(R)$	$n \times n$ matrices over the ring R
$\lfloor x \rfloor$	Round $x \in \mathbb{R}$ down to an integer
$\lceil x \rceil$	Round $x \in \mathbb{R}$ up to an integer
$[x], \lfloor x \rceil$	Closest integer to x, with $[1/2] = \lfloor 1/2 \rceil = 1$

Notation for polynomials and fields

$\mathbb{F}_q$	Finite field of $q = p^m$ elements
$F(x)$	Irreducible polynomial defining a finite field
θ	Generator of a finite field
$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$	Trace
$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ or N	Norm map with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$
$\Bbbk$	Ground field, always assumed to be perfect
$\mathrm{char}(\Bbbk)$	The characteristic of $\Bbbk$ (either 0 or a prime)
$\overline{\Bbbk}$	An algebraic closure of $\Bbbk$
$\Bbbk'$	A field extension of $\Bbbk$ contained in $\overline{\Bbbk}$
$\mathrm{Gal}(\Bbbk'/\Bbbk)$	Galois group if $\Bbbk'/\Bbbk$ is Galois
trdeg	Transcendence degree
$F(x)$	Polynomial of degree d
$F'(x)$	The derivative of the polynoial $F(x)$
$R(F,G), R_x(F(x),G(x))$	Resultant of polynomials
$R_1(x), R_i(x), T(x)$	Polynomials arising in polynomial factorisation algorithms of Section 2.12
$\deg(F(x)), \deg_x(F(x))$	Degree of polynomial
$\deg(f(\underline{x}))$	Total degree of polynomial
F	Polynomial in $\mathbb{F}_q[x]$ of degree m defining $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/(F(x))$
$\mathbb{Z}_F$	Ring of integers of number field F
$\mathrm{Cl}(\mathcal{O})$	Class group of order $\mathcal{O}$
$h(\mathcal{O})$	Class number of order $\mathcal{O}$

Notation for algorithms and complexity

$O(f)$	Big O notation
$o(f)$	Little o notation
$\tilde{O}(f)$	Soft O notation
$\Omega(f)$	Big Omega notation
$\Theta(f)$	Big Theta notation
$\leq_R$	Reduction
$\mathrm{len}(a)$	The bit-length of a
$\mathrm{wt}(m)$	The Hamming weight of m (number of ones in binary expansion)
$M(n)$	The cost of multiplication of two n-bit integers
$M(d,q) = M(d\log(dq))$	The cost of multiplying two degree d polynomials over $\mathbb{F}_q$
$s \leftarrow S$	$s \in S$ chosen according to an (implicit) distribution on S
$L_N(a,c)$	Subexponential function
O, A	Oracle

Notation for algebraic geometry

$G_a(\Bbbk)$	Additive group $(\Bbbk, +)$
$G_m(\Bbbk)$	Multiplicative group $(\Bbbk^*, .)$
mult	Multiplication map in an algebraic group
inverse	Inverse map in an algebraic group
$[g]$	Orbit or equivalence class of g under an automorphism
G/ψ	Set of orbits/equivalence classes of G under the automorphism ψ
$\mathbb{A}^n(\Bbbk)$	Affine space, points $(x_1, \ldots, x_n)$
$\mathbb{P}^n(\Bbbk)$	Projective space, points $(x_0 : \ldots | x_n)$
$(x_0 : \cdots : x_n)$	Homogeneous coordinate for point of $\mathbb{P}^n$
$\equiv$	Equivalence of $(n+1)$-tuples to define projective space
$\underline{x}$	Either $(x_1, \ldots, x_n) \in \mathbb{A}^n(\Bbbk)$ or $(x_0 : \cdots : x_n) \in \mathbb{P}^n(\Bbbk)$
X, Y	Algebraic set
$X(\Bbbk)$	$\Bbbk$-rational points of X

$V(I)$	Zero set of the ideal I
(S)	Ideal over $\Bbbk[\underline{x}]$ generated by the set S
$I_{\Bbbk}(X), I(X)$	Ideal over $\Bbbk$ corresponding to the algebraic set X over $\Bbbk$
$\mathrm{rad}(I)$	Radical of the ideal I
$\Bbbk[X]$	Coordinate ring of algebraic set X
$\Bbbk(X)$m $\Bbbk(C)$	Function field of X (resp. C)
F, K, L	Function field
U_i	Subset of $\mathbb{P}^n$ comprising all points $(x_0 : \cdots : x_n)$ with $x_i \neq 0$
φ_i	Rational map $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ with image U_i
φ	Rational map φ_n
φ_i^*	Homogenisation map from $\Bbbk[y_1, \ldots, y_n]$ to $\Bbbk[x_0, \ldots, x_n]$
φ_i^{-1}	Rational map $\mathbb{P}^n \to \mathbb{A}^n$
φ_i^{-1*}	De-homogenisation $\Bbbk[x_0, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$
$X \cap \mathbb{A}^n$	Abbreviation for $\varphi_n^{-1}(X \cap U_n)$
$\overline{f}$	Homogenisation of the polynomial f
$\overline{I}$	Homogenisation of the ideal I
$\overline{X}$	Projective closure of algebraic set $X \subseteq \mathbb{A}^n$
$\mathcal{O}(X)$	Regular functions on variety X
$\dim(X)$	Dimension of the algebraic variety X
ϕ	Rational map or morphism of varieties
$\mathfrak{p}$	A prime ideal of a ring
$S^{-1}R$	The localiation of a ring with respect to a multiplicative set S
$R_{\mathfrak{p}}$	The localisation of a ring at the prime ideal $\mathfrak{p}$
$\mathcal{O}_{P,\Bbbk}(X), \mathcal{O}_P$	Local ring of X at P.
$\mathfrak{m}_{P,\Bbbk}(X), \mathfrak{m}_P$	Maximal ideal of $\mathcal{O}_{P,\Bbbk}(X)$
$J_{X,P}$	Jacobian matrix of $X = V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ at P
C	Curve
E	Elliptic curve
$C(\Bbbk)$, $E(\Bbbk)$	The $\Bbbk$-rational points of C (resp. E)
$\mathcal{O}_E, \mathcal{O}_C$	Point at infinity on a curve
$\iota(P)$	If $P = (x, y)$ then $\iota(P) = (x, -y - a_1x - a_3)$
$v_P(f)$	Valuation of function $f \in \Bbbk(C)$ at point P
t_P	Uniformizer at P
$l(x, y)$	Line between points P_1 and P_2 on an elliptic curve
$v(x)$	Vertical line on an elliptic curve
$\mathrm{Hom}_{\Bbbk}(E_1, E_2), \mathrm{End}_{\Bbbk}(E)$	Homomorphisms/endos of elliptic curves
$T_l(E)$	Tate module of an elliptic curve
$x(P), x_P, y(P), y_P$	Coordinates of the point $P = (x_P, y_P) \in C(\overline{\Bbbk})$
π_q	q-power Frobenius map
P_0	A given k-rational point on a curve
$\Phi_n(x)$	n-th cyclotomic polynomial
$G_{q,n}$	Cyclotomic subgroup of $\mathbb{F}_{q^n}^*$ of order $\Phi_n(q)$
g	An element of $G_{q,n}$
θ	Generator over $\mathbb{F}_q$ of a finite field $\mathbb{F}_{q^2}$
$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ or Tr	Trace map with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$
$\mathbb{T}_n$	Algebraic torus
comp	Torus compression function
decomp	Torus decompression function
$\star$	Partial group operation for $\mathbb{T}_2$

V_n	Trace of g^n in LUC
U	Hypersurface in the construction of $\mathbb{T}_6$
p_U	Rational parameterisation of the hypersurface U
$\chi_g(x)$	Characteristic polynomial over $\mathbb{F}_{q^2}$ of element of $\mathbb{F}_{q^6}$
t_n	Trace of g^n in XTR
$F(x), H(x)$	Polynomials in $\Bbbk[x]$ used to define a curve
$E(x, y)$	Weierstrass equation $y^2 + H(x)y - F(x)$
a_1, a_2, a_3, a_4, a_6	Coefficients of Weierstrass equation
D	Divisor
$\mathrm{div}(f)$	Divisor of the function f
$\mathrm{Supp}(D)$	Support of a divisor
$\mathrm{Div}_{\Bbbk}(C)$	Divisors on C defined over $\Bbbk$
$\mathrm{Div}^0_{\Bbbk}(C)$	Degree zero divisors on C defined over $\Bbbk$
$\mathrm{Prin}_{\Bbbk}(C)$	Principal divisors on C
$\overline{D}$	Divisor class
$\mathrm{Pic}^0_{\Bbbk}(C)$	Degree zero divisor class group of curve C over $\Bbbk$
$\equiv$	Linear equivalence (i.e., equivalence of divisors)
$v' \mid v$	Extension of valuations
R_v	Valuation ring
$\mathfrak{m}_v$	Maximal ideal of the valuation
$\mathcal{L}_{\Bbbk}(D)$	Riemann-Roch space for divisor D
$\ell_{\Bbbk}(D)$	Dimension of Riemann-Roch space for D
$D \leq D'$	Ordering relation on divisors
DivEff	Set of all effective divisors
$\mathrm{Pic}^d_{\Bbbk}(X)$	Divisor class group (degree d divisor class group of X over the field k)
$\deg_x a(x)$	Degree in x of the polynomial $a(x)$
$\deg(\phi)$	Degree of the morphism ϕ
$\deg(D)$	Degree of the divisor D
ϕ^*	Pullback under a morphism
ϕ_*	Pushforward under a morphism
g	genus of curve C
$\partial F/\partial x$	Standard partial differentiation of polynomials or rational functions
$h dx$	Differential on C
$\Omega_{\Bbbk}(C)$	Set of differentials on C over $\Bbbk$
ω	Differential on C
ω_E	Invariant differential on elliptic curve E
$\mathrm{div}(\omega)$	Divisor of a differential on C
$(C, P), (E, O)$	A *pointed curve*, i.e., a curve over $\Bbbk$ together with a specified $\Bbbk$-rational point.
τ_Q	Translation map
$[n]$	Multiplication by n map on an elliptic curve (or torus or Abelian variety)
$E[n]$	Points of order dividing n on an elliptic curve
$\mathrm{Twist}(E)$	Set of classes of twists of E
$E^{(d)}$	Quadratic twist of E
$\mathrm{Hom}_{\Bbbk}(E_1, E_2)$	Group of isogenies from E_1 to E_2 over $\Bbbk$
$\mathrm{End}_{\Bbbk}(E)$	Ring of isogenies from E to itself over $\Bbbk$
$\ker(\phi)$	Kernel of an isogeny
t_∞	Uniformizer on elliptic curve at $\mathcal{O}_E$
$P(T)$	Characteristic polynomial of Frobenius

$\hat{\phi}$	Dual isogeny
$\deg_s(\phi)$	Separable degree
$\deg_i(\phi)$	Inseparable degree
$(Y : X_d : \cdots : X_0)$	Variables for projective non-singular equation of hyperelliptic curve
$C^\dagger$	Image of hyperelliptic curve C under map swapping ∞ and zero
ρ_P	Birational map from hyperelliptic curve taking P to infinity
$(u(x), v(x))$	Mumford representation for semi-reduced divisors
∞^+, ∞^-	Points at infinity on a hyperelliptic curve
$\text{monic}(u(x))$	Monic polynomial obtain by dividing by the leading coefficient
$\text{div}(u(x), y - v(x))$	Greatest common divisor of $\text{div}(u(x))$ and $\text{div}(y - v(x))$
$u^\dagger, v^\dagger, v^\ddagger$	Polynomials arising in Cantor reduction and reduction at infinity
$D^\dagger$	Semi-reduced divisor arising from Cantor's reduction
D_∞	Effective Divisor on a hyperelliptic curve of degree g with support only at infinity
$(u(x), v(x), n)$	Divisor $\text{div}(u(x), y - v(x)) \cap \mathbb{A}^2 + n(\infty^+) + (g - \deg(u(x)) - n)(\infty^-)$
J_C	Jacobian variety of the curve C
Θ	Mumford theta divisor
$L(t)$	L-polynomial of the curve C over $\mathbb{F}_q$
α_i	Roots of $P(T)$ and reciprocal roots of $L(t)$ for curve C over $\mathbb{F}_q$
$\mathbb{K}/\Bbbk$	Fields in Weil descent attack

Notation for algorithms in algebraic groups

NAF	Non-adjacent form
w-NAF or NAF_w	Width w non-adjacent form
$\mathcal{D}$	Digit set for an expansion
digit	Function assigning to an integer and integer in $\mathcal{D}$
weight	Weight of the expansion
$\log_g(h)$	Discrete logarithm problem ($g \in G$)
r	Large prime, the order of $g \in G$
$\pmod m$	Modular reduction to signed residue
$\overline{1}$	Coefficient -1 in a signed expansion
PH	Pohlig-Hellman algorithm
BSGS	Baby-step-giant-step algorithm
$\mathcal{S}_j$	Sets for representation problem and product DLP
L_j	Lists for generalised birthday algorithm
LSB_m	m least signficant bits
MSB_m	m most signficant bits, or bits specifying a decomposition of the domain into equal partitions
HNP	Hidden number problem

Notation in Chapter 14

G	An algebraic group or algebraic group quotient
g	An element in an AG or AGQ G, usually of prime order r
r	The prime order of an element g
h	An element in $\langle g \rangle$
a	The discrete logarithm of h with respect to g
$\mathcal{S}$	A set
N	Size of the set $\mathcal{S}$, or an integer to be factored
$\pi(X)$	The number of primes $\leq X$
Pr	Probability
$\neg E$	Complemenent of an event E

l	The number of elements sampled from $\mathcal{S}$
n_S	Number of partitions in Pollard walk
S	Map from G to $\mathbb{Z}/n_S\mathbb{Z}$
$b(g)$	Binary representation of $g \in G$
X	Random variable
x_i	Random walk sequence
(a_i, b_i)	Representation of walk element $x_i = g^{a_i}h^{b_i}$
(u_j, v_j)	Powers of g and h in random walk steps
g_j	A jump in the random walk
walk	The random walk function
l_t	Length of tail of Pollard rho walk
l_h	Length of cycle (or head) of Pollard rho walk
ϵ	A small positive real number
$\mathcal{D}$	Set of distinguished points
n_D	Number of bits used to define distinguishing property
θ	Probability that a random $g \in G$ is a distinguished point
N_P	Number of processors
n	Number of steps made by tame kangaroo
type	Indicator 'tame' or 'wild'
s	Spacing between starting positions of kangaroos in the same herd
N_C	Size of generic equivalence class
$\overline{x}$	Equivalence class of x
$\hat{x}$	Equivalence class representative of class of x
$\mathrm{Aut}(G)$	Automorphism group of an algebraic group G
b	Start of interval; usually set to 0
w	Length of interval
m	Mean step size
$f : \mathcal{S} \to \mathcal{S}$	Function in parallel collision search
$f_i : \mathcal{S}_i \to \mathcal{R}$	Function in meet-in-the-middle attack
I	Set $\{0, 1, \ldots, N-1\}$
$\sigma_i : I \to \mathcal{S}_i$	Functions in parallel meet-in-middle-attack
$\rho : \mathcal{R} \to I \times 1, 2$	Function in parallel meet-in-middle-attack
$f(x)$	Function in Pollard rho factoring

Notation in Chapter 15

$\Psi(X, Y)$	Number of Y-smooth integers less than X
$f(n) \sim g(n)$	If $\lim_{n\to\infty} f(n)/g(n) = 1$
$\rho(u)$	Dickman-de Bruijn function
T_B	Expected number of trials until a random integer $1 \leq x < N$ is B-smooth
$L_N(a, c)$	Subexponential function
$\mathcal{B}$	Factor base
B	Bound on primes to define $\mathcal{B}$
s	Number of elements in factor base $\mathcal{B}$
$I(n)$	number of irreducible polynomials of degree n
$N(n, b)$	number of b-smooth polynomials of degree exactly equal to n
$p(n, b)$	probability that a uniformly chosen polynomial of degree at most n is b-smooth
$\mathrm{Summ}_n(x_1, \ldots, x_n)$	Summation polynomial

Notation for Part IV

$\underline{b}, \underline{v}, \underline{w}$	Row vectors (usually in $\mathbb{R}^m$)
$\underline{0}$	Zero vector in $\mathbb{R}^m$
$\underline{e}_i$	i-th unit vector in $\mathbb{R}^m$
I_n	$n \times n$ identity matrix
$\langle \underline{x}, \underline{x} \rangle$	Inner product
$\|\underline{x}\|$	Euclidean length (ℓ_2 norm)
$\|\cdot\|_a$	ℓ_a-norm for $a \in \mathbb{N}$
$\text{span}\{\underline{v}_1, \ldots, \underline{v}_n\}$	Span of a set of vectors over $\mathbb{R}$
$\text{rank}(A)$	Rank of a matrix A
$\lfloor x \rceil$	Closest integer to x, $\lfloor 1/2 \rceil = 1$
B	Basis matrix for a lattice
L	Lattice
$\underline{b}_i^*$	Gram-Schmidt vector arising from ordered basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$
$\mu_{i,j}$	Gram-Schmidt coefficient $\langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$
B_i	$\|\underline{b}_i^*\|^2$
λ_i	Successive minima of a lattice
$\det(L)$	Determinant of a lattice
γ_n	Hermite's constant
X	Bound on the size of the entries in the basis matrix L
$B_{(i)}$	$i \times m$ matrix formed by the first i rows of B
d_i	Determinant of matrix of $\langle \underline{b}_j, \underline{b}_k \rangle$ for $1 \leq j, k \leq i$
D	Product of d_i
$\mathcal{P}_{1/2}(B)$	Fundamental domain (parallelepiped) for lattice basis B
$F(x)$, $F(x, y)$	Polynomial with "small" root
$G(x), G(x, y)$	Polynomial with "small" root in common with $F(x)$ (resp., $F(x, y)$)
X, Y	Bounds on size of root in Coppersmith's method
b_F	Coefficient vector of polynomial F
$R(F, G), R_x(F(x), G(x))$	Resultant of polynomials
W	Bound in Coppersmith's method
P, R	Constants in noisy Chinese remaindering
$\text{amp}(x)$	The amplitude $\gcd(P, x - R)$ in noisy Chinese remaindering
B, B'	Basis matrices for GGH encryption
I_n	$n \times n$ identity matrix
U	Invertible matrix disguising the private key in GGH
$\underline{m}, \underline{e}, \underline{c}$	Message (respectively, error vector, ciphertext) in McEliece or GGH
σ	Entry in error vector in GGH
M	Size of coefficients in message in GGH
$\underline{s}$	GGH signature
$a_1, \ldots, a_n$	Subset sum weights
$b_1, \ldots, b_n$	Superincreasing sequence
$s = \sum_{i=1}^n x_i a_i$	The sum in a subset sum instance, with $x_i \in \{0, 1\}$
d	Density of a subset sum instance
π	Permutation of $\{1, \ldots, n\}$ used in the Merkle-Hellman cryptosystem
$\underline{\sigma}$	Vector in Nguyen attack
M	Modulus in Merkle-Hellman knapsack
W	Multiplier in Merkle-Hellman knapsack
U	$W^{-1} \pmod M$ in Merkle-Hellman
t	Number of iterations in iterated Merkle-Hellman knapsack

Notation for cryptography

κ	Security parameter
M	Message space
PK	Public key space
SK	Private key space
C	Ciphertext space
pk	Public key
sk	Private key
m	Message
c, $(\mathsf{c}_1, \mathsf{c}_2)$	Ciphertext
s, $(\mathsf{s}_1, \mathsf{s}_2)$	Signature
Enc	Symmetric encryption
Dec	Symmetric decryption
g	Element of an algebraic group G
$\perp$	Symbol for invalid ciphertext or algorithm failure
H	Cryptographic hash function
q_S	Number of signature queries in security proof
$F(s_1)$	Function used in Elgamal and DSA signatures
DLP	Discrete logarithm problem
CDH	Computational Diffie-Hellman problem
DDH	Decisional Diffie-Hellman problem
kdf	Key derivation function
Inverse-DH	Inverse Diffie-Hellman problem $(g, g^a) \mapsto g^{a^{-1}}$
Static-DH	Static Diffie-Hellman problem
Strong-DH	Strong Diffie-Hellman problem
Square-DH	Square Diffie-Hellman problem
Hash-DH	Hash Diffie-Hellman problem
Adv	Advantage of an algorithm
MAC	Message authentication code
KEM	Key encapsulation mechanism
DEM	Date encapsulation mechanism
$\mathcal{K}$	Key space (for a KEM)
$\mathcal{X}_{g_1,g_2,h}$	A set used in the security proof of the Cramer-Shoup encryption scheme
id	Identity of a user
S	The set of RSA moduli

Notation used in Part VII

E/G	Quotient elliptic curve by subgroup G
$\Phi_d(x, y)$	Modular polynomial
$\tilde{j}$	j-invariant of isogenous curve in Elkies method
$\mathfrak{a}, \mathfrak{b}, \mathfrak{l}$	$\mathcal{O}$-ideals
$X_{E,\mathbb{F}_q,S}$	Isogeny graph
$E[\mathfrak{l}]$	Kernel of isogeny corresponding to ideal $\mathfrak{l}$
$\delta_v(S)$	Vertex boundary of a set S in a graph
$\delta_e(S)$	Edge boundary of a set S in a graph
$f(D)$	Evaluation of function f at divisor D
e_n	Weil pairing
t_n	Tate-Lichtenbaum pairing
$\hat{t}_n$	Reduced Tate-Lichtenbaum pairing
$k(q, n)$	Embedding degree
G_1, G_2	Eigenspaces of Frobenius in $E[r]$
T	$t - 1$, used in the ate pairing
$a_T(Q, P)$	Ate pairing

Acknowledgements

The book grew out of my lecture notes from the Masters course "Public key cryptography" at Royal Holloway. I thank the students who took that course for asking questions and doing their homework in unexpected ways.

The staff at Cambridge University Press have been very helpful during the preparation of this book.

I also thank the following people for answering my questions, pointing out errors in drafts of the book, helping with latex, examples, proofs, exercises etc: José de Jesús Angel Angel, Olivier Bernard, Nicolas Bonifas, Nils Bruin, Ilya Chevyrev, Bart Coppens, Alex Dent, Claus Diem, Marion Duporté, Andreas Enge, Victor Flynn, David Freeman, Pierrick Gaudry, Takuya Hayashi, Nadia Heninger, Florian Hess, Mark Holmes, Everett Howe, David Jao, Jonathan Katz, Eike Kiltz, Kitae Kim, David Kohel, Cong Ling, Alexander May, Esmaeil Mehrabi, Ciaran Mullan, Mats Näslund, Francisco Monteiro, James McKee, James Nelson, Samuel Neves, Phong Nguyen, TaeHun Oh, Chris Peikert, Michael Phillips, John Pollard, Francesco Pretto, Oded Regev, Christophe Ritzenthaler, Karl Rubin, Raminder Ruprai, Takakazu Satoh, Leanne Scheepers, Davide Schipani, Michael Schneider, Peter Schwabe, Reza Sepahi, Victor Shoup, Igor Shparlinski, Andrew Shallue, Francesco Sica, Alice Silverberg, Benjamin Smith, Martijn Stam, Damien Stehlé, Anton Stolbunov, Drew Sutherland, Garry Tee, Emmanuel Thomé, Frederik Vercauteren, Timothy Vogel, Anastasia Zaytseva, Chang-An Zhao, Paul Zimmermann.

The remaining errors and omissions are the authors responsibility.

Note added October 2018: Thanks to all the people who have pointed out errors. They are thanked in the errata list on my webpage.

Chapter 1

Introduction

Cryptography is an interdisciplinary field of great practical importance. The subfield of public key cryptography has notable applications, such as digital signatures. The security of a public key cryptosystem depends on the difficulty of certain computational problems in mathematics. A deep understanding of the security and efficient implementation of public key cryptography requires significant background in algebra, number theory and geometry.

This book gives a rigorous presentation of most of the mathematics underlying public key cryptography. Our main focus is mathematics. We put mathematical precision and rigour ahead of generality, practical issues in real-world cryptography, or algorithmic optimality. It is infeasible to cover all the mathematics of public key cryptography in one book. Hence we primarily discuss the mathematics most relevant to cryptosystems that are currently in use, or that are expected to be used in the near future. More precisely, we focus on discrete logarithms (especially on elliptic curves), factoring based cryptography (e.g., RSA and Rabin), lattices and pairings. We cover many topics that have never had a detailed presentation in any textbook.

Due to lack of space, some topics are not covered in as much detail as others. For example, we do not give a complete presentation of algorithms for integer factorisation, primality testing, and discrete logarithms in finite fields, as there are several good references for these subjects. Some other topics that are not covered in the book include hardware implementation, side-channel attacks, lattice-based cryptography, cryptosystems based on coding theory, multivariate cryptosystems and cryptography in non-Abelian groups. In the future, quantum cryptography or post-quantum cryptography (see the book [50] by Bernstein, Buchmann and Dahmen) may be used in practice, but these topics are also not discussed in the book.

The reader is assumed to have at least a standard undergraduate background in groups, rings, fields and cryptography. Some experience with algorithms and complexity is also assumed. For a basic introduction to public key cryptography and the relevant mathematics the reader is recommended to consult Smart [572], Stinson [592] or Vaudenay [616].

An aim of the present book is to collect in one place all the necessary background and results for a deep understanding of public key cryptography. Ultimately, the text presents what I believe is the "core" mathematics required for current research in public key cryptography and it is what I would want my PhD students to know.

The remainder of this chapter states some fundamental definitions in public key cryptography and illustrates them using the RSA cryptosystem.

1.1 Public Key Cryptography

Two fundamental goals of cryptography are to provide privacy of communication between two entities and to provide authentication of one entity to another. Both goals can be achieved with symmetric cryptography. However, symmetric cryptography is not convenient in some applications for the following reasons. First, each pair of communicating entities needs to have a shared key. Second, these keys must be transmitted securely. Third, it is difficult to obtain signatures with non-repudiation (e.g., suitable for signing contracts).

In the mid 1970s, Merkle, Diffie and Hellman proposed the idea of **public key cryptography** (also sometimes called **asymmetric cryptography**). This idea was also proposed by Ellis at GCHQ, under the name "non-secret encryption". One of the earliest and most important public key cryptosystems is RSA, invented by Adleman, Rivest and Shamir in 1977 (essentially the same scheme was also invented by Cocks at GCHQ in 1973).

As noted above, a major application of public key cryptography is to provide authentication. An extremely important example of this in the real world is digital signatures for authenticating automatic software updates. The public key of the software developer is stored in the application or operating system and the software update is only performed if the digital signature on the update is verified for that public key (see Section 12.1 of Katz and Lindell [334] for more details). Signature schemes also provide message integrity, message authentication and non-repudiation (see Section 10.2 of Smart [572]). Other important applications of public key cryptography are key exchange and key transport for secure communication (e.g., in SSL or TLS).

1.2 The Textbook RSA Cryptosystem

We briefly describe the "textbook" RSA cryptosystem. The word "textbook" indicates that, although the RSA cryptosystem as presented below appears in many papers and books, this is definitely not how it should be used in the real world. In particular, public key encryption is most commonly used to transmit keys (the functionality is often called key transport or key encapsulation), rather than to encrypt data. Chapter 24 gives many more details about RSA including, in Section 24.7, a very brief discussion of padding schemes for use in real applications.

Alice chooses two large primes p and q of similar size and computes $N = pq$. Alice also chooses $e \in \mathbb{N}$ coprime to $\varphi(N) = (p-1)(q-1)$ and computes $d \in \mathbb{N}$ such that

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Alice's RSA **public key** is the pair of integers (N, e) and her **private key** is the integer d. To **encrypt** a message to Alice, Bob does the following:

1. Obtain an authentic copy of Alice's public key (N, e). This step may require trusted third parties and public key infrastructures, which are outside the scope of this book;

see Chapter 12 of Smart [572] or Chapter 12 of Stinson [592]. We suppress this issue in the book.

2. Encode the message as an integer $1 \leq \mathsf{m} < N$.

   Note that m does not necessarily lie in $(\mathbb{Z}/N\mathbb{Z})^*$. However, if $p, q \approx \sqrt{N}$ then the probability that $\gcd(\mathsf{m}, N) > 1$ is $(p+q-1)/(N-1) \approx 2/\sqrt{N}$. Hence, in practice one may assume that $\mathsf{m} \in (\mathbb{Z}/N\mathbb{Z})^*$.[1]

3. Compute and transmit the **ciphertext**

$$\mathsf{c} = \mathsf{m}^e \pmod{N}.$$

To **decrypt** the ciphertext, Alice computes $\mathsf{m} = \mathsf{c}^d \pmod{N}$ and decodes this to obtain the original message.

Exercise 1.2.1. Show that if $\gcd(\mathsf{m}, N) = 1$ then $(\mathsf{m}^e)^d \equiv \mathsf{m} \pmod{N}$. Show that if $\gcd(\mathsf{m}, N) \neq 1$ then $(\mathsf{m}^e)^d \equiv \mathsf{m} \pmod{N}$.

The RSA system can also be used as a digital signature algorithm. When sending a message m to Bob, Alice computes the signature $\mathsf{s} = \mathsf{m}^d \pmod{N}$. When Bob receives (m, s) he obtains an authentic copy of Alice's public key and then verifies that $\mathsf{m} \equiv \mathsf{s}^e \pmod{N}$. If the verification equation holds then Bob believes that the message m does come from Alice. The value m is not usually an actual message or document (which might be huge) but a short integer that is the output of some (non-injective) compression function (such as a hash function). We sometimes call m a **message digest**.

The idea is that exponentiation to the power e modulo N is a **one-way function**: a function that is easy to compute but such that it is hard to compute pre-images. Indeed, exponentiation modulo N is a **one-way permutation** on $(\mathbb{Z}/N\mathbb{Z})^*$ when e is co-prime to $\varphi(N)$. The private key d allows the permutation to be efficiently inverted and is known as a **trapdoor**. Therefore RSA is often described as a **trapdoor one-way permutation**.

A number of practical issues must be considered:

1. Can public keys be efficiently generated?
2. Is the cryptosystem efficient in the sense of computation time and ciphertext size?
3. How does Bob know that Alice's public key is authentic?
4. Is the scheme secure?
5. What does "security" mean anyway?

One aim of this book is to explore the above issues in depth. We will study RSA (and some other cryptosystems based on integer factorisation) as well as cryptosystems based on the discrete logarithm problem.

To indicate some of the potential problems with the "textbook" RSA cryptosystem as described above, we present a three simple attacks.

1. Suppose the RSA cryptosystem is being used for an online election to provide privacy of an individual's vote to everyone outside the electoral office.[2] Each voter encrypts

[1] If N is a product of two 150 digit primes (which is the minimum size for an RSA modulus) then the expected number of trials to find $1 \leq \mathsf{m} < N$ with $\gcd(\mathsf{m}, N) > 1$ is therefore $\approx 10^{150}$. Note that the age of the universe is believed to be less than 10^{18} seconds.

[2] Much more interesting electronic voting schemes have been invented. This unnatural example is chosen purely for pedagogical purposes.

their vote under the public key of the electoral office and then sends their vote by email. Voters don't want any other member of the public to know who they voted for.

Suppose the eavesdropper Eve is monitoring internet traffic from Alice's computer and makes a copy of the ciphertext corresponding to her vote. Since encryption is deterministic and there is only a short list of possible candidates, it is possible for Eve to compute each possible vote by encrypting each candidate's name under the public key. Hence, Eve can deduce who Alice voted for.

2. To speed up encryption it is tempting to use small encryption exponents, such as $e = 3$ (assuming that $N = pq$ where $p \equiv q \equiv 2 \pmod 3$). Now suppose Bob is only sending a very small message $0 < \mathsf{m} < N^{1/3}$ to Alice; this is quite likely, since public key cryptography is most often used to securely transmit symmetric keys. Then $\mathsf{c} = \mathsf{m}^3$ in $\mathbb{N}$, i.e., no modular reduction has taken place. An adversary can therefore compute the message m from the ciphertext c by taking cube roots in $\mathbb{N}$ (using numerical analysis techniques).

3. A good encryption scheme should allow an adversary to learn absolutely nothing about a message from the ciphertext. But with the RSA cryptosystem one can compute the Jacobi symbol $(\frac{\mathsf{m}}{N})$ of the message by computing $(\frac{\mathsf{c}}{N})$ (this can be computed efficiently without knowing the factorisation of N; see Section 2.4). The details are Exercise 24.1.11.

The above three attacks may be serious attacks for some applications, but not for others. However, a cryptosystem designer often has little control over the applications in which their system is to be used. Hence it is preferable to have systems that are not vulnerable to attacks of the above form. In Section 24.7 we will explain how to secure RSA against these sorts of attacks, by making the encryption process randomised and by using padding schemes that encode short messages as sufficiently large integers and that destroy algebraic relationships between messages.

1.3 Formal Definition of Public Key Cryptography

To study public key cryptography using mathematical techniques it is necessary to give a precise definition of an encryption scheme. The following definition uses terminology about algorithms that is recalled in Section 2.1. Note that the problem of obtaining an authentic copy of the public key is not covered by this definition; the public key is an input to the encryption function.

Definition 1.3.1. Let $\kappa \in \mathbb{N}$ be a **security parameter** (note that κ is not necessarily the same as the "key length"; see Example 1.3.2). An **encryption scheme** is defined by the following spaces (all depending on the security parameter κ) and algorithms.

M_κ	the space of all possible messages;
PK_κ	the space of all possible public keys;
SK_κ	the space of all possible private keys;
C_κ	the space of all possible ciphertexts;
KeyGen	a randomised algorithm that takes the security parameter κ, runs in expected polynomial-time (i.e., $O(\kappa^c)$ bit operations for some constant $c \in \mathbb{N}$) and outputs a public key $\mathsf{pk} \in \mathsf{PK}_\kappa$ and a private key $\mathsf{sk} \in \mathsf{SK}_\kappa$;
Encrypt	a randomised algorithm that takes as input $\mathsf{m} \in \mathsf{M}_\kappa$ and pk, runs in expected polynomial-time (i.e., $O(\kappa^c)$ bit operations for some constant

$c \in \mathbb{N}$) and outputs a ciphertext $\mathsf{c} \in \mathsf{C}_\kappa$;

Decrypt an algorithm (not usually randomised) that takes $\mathsf{c} \in \mathsf{C}_\kappa$ and sk, runs in polynomial-time and outputs either $\mathsf{m} \in \mathsf{M}_\kappa$ or the invalid ciphertext symbol $\perp$.

It is required that

$$\text{Decrypt}(\text{Encrypt}(\mathsf{m}, \mathsf{pk}), \mathsf{sk}) = \mathsf{m}$$

if $(\mathsf{pk}, \mathsf{sk})$ is a matching key pair. Typically we require that the fastest known attack on the system requires at least 2^κ bit operations.

Example 1.3.2. We sketch how to write "textbook" RSA encryption in the format of Definition 1.3.1. The KeyGen algorithm takes input κ and outputs a modulus N that is a product of two randomly chosen primes of a certain length, as well as an encryption exponent e.

Giving a precise recipe for the bit-length of the primes as a function of the security parameter is non-trivial for RSA. The complexity of the best factoring algorithms implies that we need $2^\kappa \approx L_N(1/3, c)$ for some constant c (see Chapter 15 for this notation and an explantion of factoring algorithms). This implies that $\log(N) = O(\kappa^3)$ and so the bit-length of the public key is bounded by a polynomial in κ. A typical benchmark is that if $\kappa = 128$ (i.e., so that there is no known attack on the system performing fewer than 2^{128} bit operations) then N is a product of two 1536-bit primes.

As we will discuss in Chapter 12, one can generate primes in expected polynomial-time and hence KeyGen is a randomised algorithm with expected polynomial-time complexity.

The message space M_κ depends on the randomised padding scheme being used. The ciphertext space C_κ in this case is $(\mathbb{Z}/N\mathbb{Z})^*$, which does not agree with Definition 1.3.1 as it does not depend only on κ. Instead one usually takes C_κ to be the set of $\lceil \log_2(N) \rceil$-bit strings.

The Encrypt and Decrypt algorithms are straightforward (though the details depend on the padding scheme). The correctness condition is easily checked.

1.3.1 Security of Encryption

We now give precise definitions for the security of public key encryption. An **adersary** is a randomised polynomial-time algorithm that interacts with the cryptosystem in some way. It is necessary to define the **attack model**, which specifies the way the adversary can interact with the cryptosystem. It is also necessary to define the **attack goal** of the adversary. For further details of these issues see Sections 10.2 and 10.6 of Katz and Lindell [334], Section 1.13 of Menezes, van Oorschot and Vanstone [418], or Section 15.1 of Smart [572].

We first list the **attack goals for public key encryption**. The most severe one is the **total break**, where the adversary computes a private key. There are three other commonly studied attacks, and they are usually formulated as **security properties** (the security property is the failure of an adversary to achieve its attack goal).

The word **oracle** is used below. This is just a fancy name for a magic box that takes some input and then outputs the correct answer in constant time. Precise definitions are given in Section 2.1.3.

- **One way encryption (OWE):** Given a challenge ciphertext c the adversary cannot compute the corresponding message m.
- **Semantic security:** An adversary learns no information at all about a message from its ciphertext, apart from possibly the length of the message.

This concept is made precise as follows: Assume all messages in M_κ have the same length. A **semantic security adversary** is a randomised polynomial-time algorithm A that first chooses a function $f : \mathsf{M}_\kappa \to \{0,1\}$ such that the probability, over uniformly chosen $\mathsf{m} \in \mathsf{M}_\kappa$, that $f(\mathsf{m}) = 1$ is $1/2$. The adversary A then takes as input a challenge $(\mathsf{c}, \mathsf{pk})$, where c is the encryption of a random message $\mathsf{m} \in \mathsf{M}_\kappa$, and outputs a bit b. The adversary is **successful** if $b = f(\mathsf{m})$.

Note that the standard definition of semantic security allows messages $\mathsf{m} \in \mathsf{M}_\kappa$ to be drawn according to any probability distribution. We have simplified to the case of the uniform distribution on M_κ.

- **Indistinguishability (IND):** An adversary cannot distinguish the encryption of any two messages m_0 and m_1, chosen by the adversary, of the same length.

  This concept is made precise by defining an **indistinguishability adversary** to be a randomised polynomial-time algorithm A that plays the following game with a challenger: First the challenger generates a public key and gives it to A. Then (this is the "first phase" of the attack) A performs some computations (and possibly queries to oracles) and outputs two equal length messages m_0 and m_1. The challenger computes the **challenge ciphertext** c (which is an encryption of m_b where $b \in \{0,1\}$ is randomly chosen) and gives it to A. In the "second phase" the adversary A performs more calculations (and possibly oracle queries) and outputs a bit b'. The adversary is **successful** if $b = b'$.

For a fixed value κ one can consider the probability that an adversary is successful over all public keys pk output by KeyGen, and (except when studying a total break adversary) all challenge ciphertexts c output by Encrypt, and over all random choices made by the adversary. The adversary breaks the security property if the success probability of the adversary is noticeable as a function of κ (see Definition 2.1.10 for the terms noticeable and negligible). The cryptosystem achieves the security property if every polynomial-time adversary has negligible success probability as a function of κ. An adversary that works with probability 1 is called a **perfect adversary**.

We now list the three main attack models for public key cryptography.

- **Passive attack/chosen plaintext attack (CPA):** The adversary is given the public key.
- **Lunchtime attack (CCA1):**[3] The adversary has the public key and can also ask for decryptions of ciphertexts of its choosing during the first stage of the attack (i.e., before the challenge ciphertext is received).
- **Adaptive chosen-ciphertext attack (CCA):** (Also denoted CCA2.) The adversary has the public key and is given access to a decryption oracle O that will provide decryptions of any ciphertext of its choosing, with the restriction that O outputs $\perp$ in the second phase of the attack if the challenge ciphertext is submitted to O.

One can consider an adversary against any of the above security properties in any of the above attack models. For example, the strongest security notion is indistinguishability under an adaptive chosen ciphertext attack. A cryptosystem that achieves this security level is said to have **IND-CCA security**. It has become standard in theoretical cryptography to insist that all cryptosystems have IND-CCA security. This is not because

[3]The name comes from an adversary who breaks into someone's office during their lunch break, interacts with their private key in some way, and then later in the day tries to decrypt a ciphertext.

CCA attacks occur frequently in the real world, but because a scheme that has IND-CCA security should also be secure against any real-world attacker.[4]

Exercise 1.3.3. Show that the "textbook" RSA cryptosystem does not have IND-CPA security.

Exercise 1.3.4. Show that the "textbook" RSA cryptosystem does not have OWE-CCA security.

Exercise 1.3.5. Prove that if a cryptosystem has IND security under some attack model then it has semantic security under the same attack model.

1.3.2 Security of Signatures

Definition 1.3.6. A **signature scheme** is defined, analogously to encryption, by message, signature and key spaces depending on a security parameter κ. There is a KeyGen algorithm and algorithms:

Sign	A randomised algorithm that runs in polynomial-time (i.e., $O(\kappa^c)$ bit operations for some constant $c \in \mathbb{N}$), takes as input a message m and a private key sk, and outputs a signature s.
Verify	An algorithm (usually deterministic) that runs in polynomial-time, takes as input a message m, a signature s and a public key pk, and outputs "valid" or "invalid".

We require that $\text{Verify}(\mathsf{m}, \text{Sign}(\mathsf{m}, \mathsf{sk}), \mathsf{pk}) =$ "valid". Typically, we require that all known algorithms to break the signature scheme require at least 2^κ bit operations.

The main **attack goals for signatures** are the following (for more discussion see Goldwasser, Micali and Rivest [258], Section 12.2 of Katz and Lindell [334], Section 15.4 of Smart [572], or Section 7.2 of Stinson [592]):

- **Total break:** An adversary can obtain the private key for the given public key.
- **Selective forgery:** (Also called **target message forgery**.) An adversary can generate a valid signature for the given public key on any message.
- **Existential forgery:** An adversary can generate a pair (m, s) where m is a message and s is a signature for the given public key on that message.

  The acronym **UF** stands for the security property "unforgeable". In other words, a signature scheme has UF security if every polynomial-time existential forgery algorithm succeeds with only negligible probability. Be warned that some authors use UF to denote "universal forgery", which is another name for selective forgery.

As with encryption there are various attack models.

- **Passive attack:** The adversary is given the public key only. This is also called a "public key only" attack.
- **Known message attack:** The adversary is given various sample message-signature pairs for the public key.

[4] Of course, there are attacks that lie outside the attack model we are considering, such as side-channel attacks or attacks by dishonest system administrators.

- **Adaptive chosen-message attack (CMA):** The adversary is given a signing oracle that generates signatures for the public key on messages of their choosing.

  In this case, **signature forgery** usually means producing a valid signature s for the public key pk on a message m such that m was not already queried to the signing oracle for key pk. Another notion, which we do not consider further in this book, is **strong forgery**; namely to output a valid signature s on m for public key pk such that s is not equal to any of the outputs of the signing oracle on m.

As with encryption, one says the signature scheme has the stated security property under the stated attack model if there is no polynomial-time algorithm A that solves the problem with noticeable success probability under the appropriate game. The standard notion of security for digital signatures is **UF-CMA** security.

Exercise 1.3.7. Give a precise definition for UF-CMA security.

Exercise 1.3.8. Do "textbook" RSA signatures have selective forgery security under a passive attack?

Exercise 1.3.9. Show that there is a passive existential forgery attack on "textbook" RSA signatures.

Exercise 1.3.10. Show that, under a chosen-message attack, one can selective forge "textbook" RSA signatures.

Part I

Background

Chapter 2

Basic Algorithmic Number Theory

The aim of this chapter is to give a brief summary of some fundamental algorithms for arithmetic in finite fields. The intention is not to provide an implementation guide; instead, we sketch some important concepts and state some complexity results that will be used later in the book. We do not give a consistent level of detail for all algorithms; instead we only give full details for algorithms that will play a significant role in later chapters of the book.

More details of these subjects can be found in Crandall and Pomerance [162], Shoup [556], Buhler and Stevenhagen [113], Brent and Zimmermann [100], Knuth [343], von zur Gathen and Gerhard [238], Bach and Shallit [22] and the handbooks [16, 418].

The chapter begins with some remarks about computational problems, algorithms and complexity theory. We then present methods for fast integer and modular arithmetic. Next we present some fundamental algorithms in computational number theory such as Euclid's algorithm, computing Legendre symbols, and taking square roots modulo p. Finally, we discuss polynomial arithmetic, constructing finite fields, and some computational problems in finite fields.

2.1 Algorithms and Complexity

We assume the reader is already familiar with computers, computation and algorithms. General references for this section are Chapter 1 of Cormen, Leiserson, Rivest and Stein [146], Davis and Weyuker [167], Hopcroft and Ullman [293], Section 3.1 of Shoup [556], Sipser [568] and Talbot and Welsh [600].

Rather than using a fully abstract model of computation, such as Turing machines, we consider all algorithms as running on a digital computer with a typical instruction set,

an infinite number of bits of memory and constant-time memory access. This is similar to the random access machine (or register machine) model; see Section 3.6 of [22], [139], Section 2.2 of [146], Section 7.6 of [293] or Section 3.2 of [556]. We think of an algorithm as a sequence of bit operations, though it is more realistic to consider word operations.

A **computational problem** is specified by an input (of a certain form) and an output (satisfying certain properties relative to the input). An **instance** of a computational problem is a specific input. The **input size** of an instance of a computational problem is the number of bits required to represent the instance. The **output size** of an instance of a computational problem is the number of bits necessary to represent the output. A **decision problem** is a computational problem where the output is either "yes" or "no". As an example, we give one of the most important definitions in the book.

Definition 2.1.1. Let G be a group written in multiplicative notation. The **discrete logarithm problem** (**DLP**) is: Given $g, h \in G$ to find a, if it exists, such that $h = g^a$.

In Definition 2.1.1 the input is a description of the group G together with the group elements g and h and the output is a or the failure symbol $\perp$ (to indicate that $h \notin \langle g \rangle$). Typically G is an algebraic group over a finite field and the order of g is assumed to be known. We stress that an instance of the DLP, according to Definition 2.1.1, includes the specification of G, g and h; so one must understand that they are all allowed to vary (note that, in many cryptographic applications one considers the group G and element g as being fixed; we discuss this in Exercise 21.1.2). As explained in Section 2.1.2, a computational problem should be defined with respect to an instance generator; in the absence of any further information it is usual to assume that the instances are chosen uniformly from the space of all possible inputs of a given size. In particular, for the DLP it is usual to denote the order of g by r and to assume that $h = g^a$ where a is chosen uniformly in $\mathbb{Z}/r\mathbb{Z}$. The output is the integer a (e.g., written in binary). The input size depends on the specific group G and the method used to represent it. If h can take all values in $\langle g \rangle$ then one needs at least $\log_2(r)$ bits to specify h from among the r possibilities. Hence, the input size is at least $\log_2(r)$ bits. Similarly, if the output a is uniformly distributed in $\mathbb{Z}/r\mathbb{Z}$ then the output size is at least $\log_2(r)$ bits.

An algorithm to solve a computational problem is called **deterministic** if it does not make use of any randomness. We will study the asymptotic complexity of deterministic algorithms by counting the number of bit operations performed by the algorithm expressed as a function of the input size. Upper bounds on the complexity are presented using "big O" notation. When giving complexity estimates using big O notation we implicitly assume that there is a countably infinite number of possible inputs to the algorithm.

Definition 2.1.2. Let $f, g : \mathbb{N} \to \mathbb{R}_{>0}$. Write $f = O(g)$ if there are $c \in \mathbb{R}_{>0}$ and $N \in \mathbb{N}$ such that

$$f(n) \leq cg(n)$$

for all $n \geq N$.

Similarly, if $f(n_1, \ldots, n_m)$ and $g(n_1, \ldots, n_m)$ are functions from $\mathbb{N}^m$ to $\mathbb{R}_{>0}$ then we write $f = O(g)$ if there are $c \in \mathbb{R}_{>0}$ and $N_1, \ldots, N_m \in \mathbb{N}$ such that $f(n_1, \ldots, n_m) \leq cg(n_1, \ldots, n_m)$ for all $(n_1, \ldots, n_m) \in \mathbb{N}^m$ with $n_i \geq N_i$ for all $1 \leq i \leq m$.

Example 2.1.3. $3n^2 + 2n + 1 = O(n^2)$, $n + \sin(n) = O(n)$, $n^{100} + 2^n = O(2^n)$, $\log_{10}(n) = O(\log(n))$.

Exercise 2.1.4. Show that if $f(n) = O(\log(n)^a)$ and $g(n) = O(\log(n)^b)$ then $(f+g)(n) = f(n) + g(n) = O(\log(n)^{\max\{a,b\}})$ and $(fg)(n) = f(n)g(n) = O(\log(n)^{a+b})$. Show that $O(n^c) = O(2^{c\log(n)})$.

We also present the "little o", "soft O", "big Omega" and "big Theta" notation . These will only ever be used in this book for functions of a single argument.

Definition 2.1.5. Let $f, g : \mathbb{N} \to \mathbb{R}_{>0}$. Write $f(n) = o(g(n))$ if

$$\lim_{n\to\infty} f(n)/g(n) = 0.$$

Write $f(n) = \tilde{O}(g(n))$ if there is some $m \in \mathbb{N}$ such that $f(n) = O(g(n)\log(g(n))^m)$. Write $f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$. Write $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$ and $g(n) = O(f(n))$.

Exercise 2.1.6. Show that if $g(n) = O(n)$ and $f(n) = \tilde{O}(g(n))$ then there is some $m \in \mathbb{N}$ such that $f(n) = O(n\log(n)^m)$.

Definition 2.1.7. (Worst-case asymptotic complexity.) Let A be a deterministic algorithm and let $t(n)$ be a bound on the running time of A on every problem of input size n bits.

- A is **polynomial-time** if there is an integer $k \in \mathbb{N}$ such that $t(n) = O(n^k)$.
- A is **superpolynomial-time** if $t(n) = \Omega(n^c)$ for all $c \in \mathbb{R}_{>1}$.
- A is **exponential-time** if there is a constant $c_2 > 1$ such that $t(n) = O(c_2^n)$.
- A is **subexponential-time** if $t(n) = O(c^n)$ for all $c \in \mathbb{R}_{>1}$.

Exercise 2.1.8. Show that $n^{a\log(\log(n))}$ and $n^{a\log(n)}$, for some $a \in \mathbb{R}_{>0}$, are functions that are $\Omega(n^c)$ and $O(c^n)$ for all $c \in \mathbb{R}_{>1}$.

For more information about computational complexity, including the definitions of complexity classes such as P and NP, see Chapters 2 to 4 of [600], Chapter 13 of [293], Chapter 15 of [167], Chapter 7 of [568] or Chapter 34 of [146]. Definition 2.1.7 is for **uniform** complexity, as a single algorithm A solves all problem instances. One can also consider **non-uniform complexity**, where one has an algorithm A and, for each $n \in \mathbb{N}$, polynomially sized auxiliary input $h(n)$ (the hint) such that if x is an n-bit instance of the computational problem then $A(x, h(n))$ solves the instance. An alternative definition is a sequence A_n of algorithms, one for each input size $n \in \mathbb{N}$, and such that the description of the algorithm is polynomially bounded. We stress that the hint is not required to be efficiently computable. We refer to Section 4.6 of Talbot and Welsh [600] for details.

Complexity theory is an excellent tool for comparing algorithms, but one should always be aware that the results can be misleading. For example, it can happen that there are several algorithms to solve a computational problem and that the one with the best complexity is slower than the others for the specific problem instance one is interested in (for example, see Remark 2.2.5).

2.1.1 Randomised Algorithms

All our algorithms may be **randomised**, in the sense that they have access to a random number generator. A deterministic algorithm should terminate after a finite number of steps but a randomised algorithm can run forever if an infinite sequence of "unlucky" random choices is made.[1] Also, a randomised algorithm may output an incorrect answer for

[1] In algorithmic number theory it is traditional to allow algorithms that do not necessarily terminate, whereas in cryptography it is traditional to consider algorithms whose running time is bounded (typically by a polynomial in the input size). Indeed, in security reductions it is crucial that an adversary (i.e., randomised algorithm) always terminates. Hence, some of the definitions in this section (e.g., Las Vegas algorithms) mainly arise in the algorithmic number theory literature.

some choices of randomness. A **Las Vegas algorithm** is a randomised algorithm which, if it terminates[2], outputs a correct solution to the problem. A randomised algorithm for a decision problem is a **Monte Carlo algorithm** if it always terminates and if the output is "yes" then it is correct and if the output is "no" then it is correct with "noticeable" probability (see the next section for a formal definition of noticeable success probability).

An example of a Las Vegas algorithm is choosing a random quadratic non-residue modulo p by choosing random integers modulo p and computing the Legendre symbol (see Exercise 2.4.6 in Section 2.4); the algorithm could be extremely unlucky forever. Of course, there is a deterministic algorithm for this problem, but its complexity is worse than the randomised algorithm. An example of a Monte Carlo algorithm is testing primality of an integer N using the Miller-Rabin test (see Section 12.1.2). Many of the algorithms in the book are randomised Monte Carlo or Las Vegas algorithms. We will often omit the words "Las Vegas" or "Monte Carlo".

Deterministic algorithms have a well-defined running time on any given problem instance. For a randomised algorithm the running time for a fixed instance of the problem is not necessarily well-defined. Instead, one considers the expected value of the running time over all choices of the randomness. We usually consider **worst-case complexity**. For a randomised algorithm, the worst-case complexity for input size n is the maximum, over all problem instances of size n, of the expected running time of the algorithm. As always, when considering asymptotic complexity it is necessary that the computational problem have a countably infinite number of problem instances.

A randomised algorithm is **expected polynomial-time** if the worst-case over all problem instances of size n bits of the expected value of the running time is $O(n^c)$ for some $c \in \mathbb{R}_{>0}$. (An expected polynomial-time algorithm can run longer than polynomial-time if it makes many "unlucky" choices.) A randomised algorithm is **expected exponential-time** (respectively, **expected subexponential-time**) if there exists $c \in \mathbb{R}_{>1}$ (respectively, for all $c \in \mathbb{R}_{>1}$) such that the expected value of the running time on problem instances of size n bits is $O(c^n)$.

One can also consider **average-case complexity**, which is the average, over all problem instances of size n, of the expected running time of the algorithm. Equivalently, the average-case complexity is the expected number of bit operations of the algorithm where the expectation is taken over all problem instances of size n as well as all choices of the randomness. For more details see Section 4.2 of Talbot and Welsh [600].

2.1.2 Success Probability of a Randomised Algorithm

Throughout the book we give very simple definitions (like Definition 2.1.1) for computational problems. However, it is more subtle to define what it means for a randomised algorithm A to solve a computational problem. A **perfect algorithm** is one whose output is always correct (i.e., it always succeeds). We also consider algorithms that give the correct answer only for some subset of the problem instances, or for all instances but only with a certain probability.

The issue of whether an algorithm is successful is handled somewhat differently by the two communities whose work is surveyed in this book. In the computational number theory community, algorithms are expected to solve all problem instances with probability of success close to 1. In the cryptography community it is usual to consider algorithms that only solve some noticeable (see Definition 2.1.10) proportion of problem instances, and even then only with some noticeable probability. The motivation for the latter community

[2] An alternative definition is that a Las Vegas algorithm has finite expected running time, and outputs either a correct result or the failure symbol $\perp$.

is that an algorithm to break a cryptosystem is considered devastating even if only a relatively small proportion of ciphertexts are vulnerable to the attack. Two examples of attacks that only apply to a small proportion of ciphertexts are the attack by Boneh, Joux and Nguyen on textbook Elgamal (see Exercise 20.4.9) and the Desmedt-Odlyzko signature forgery method (see Section 24.4.3).

We give general definitions for the success probability of an algorithm in this section, but rarely use the formalism in our later discussion. Instead, for most of the book, we focus on the case of algorithms that always succeed (or, at least, that succeed with probability extremely close to 1). This choice allows shorter and simpler proofs of many facts. In any case, for most computational problems the success probability can be increased by running the algorithm repeatedly, see Section 2.1.4.

The success of an algorithm to solve a computational problem is defined with respect to an **instance generator**, which is a randomised algorithm that takes as input $\kappa \in \mathbb{N}$ (often κ is called the **security parameter**), runs in polynomial-time in the output size, and outputs an instance of the computational problem (or fails to generate an instance with some negligible probability). The output is usually assumed to be $\Theta(\kappa)$ bits,[3] so "polynomial-time" in the previous sentence means $O(\kappa^m)$ bit operations for some $m \in \mathbb{N}$. We give an example of an instance generator for the DLP in Example 2.1.9.

Let A be a randomised algorithm that takes an input $\kappa \in \mathbb{N}$. Write $\mathcal{S}_\kappa$ for the set of possible outputs of $A(\kappa)$. The **output distribution** of A on input κ is the distribution on $\mathcal{S}_\kappa$ such that $\Pr(x)$ for $x \in \mathcal{S}_\kappa$ is the probability, over the random choices made by A, that the output of $A(\kappa)$ is x.

Example 2.1.9. Let a security parameter $\kappa \in \mathbb{N}$ be given. First, generate a random prime number r such that $2^{2\kappa} < r < 2^{2\kappa+1}$ (by choosing uniformly at random $(2\kappa+1)$-bit integers and testing each for primality). Next, try consecutive small[4] integers k until $p = kr + 1$ is prime. Then, choose a random integer $1 < u < p$ and set $g = u^{(p-1)/r}$ and repeat if $g = 1$. It follows that g is a generator of a cyclic subgroup of $G = \mathbb{F}_p^*$ of order r. Finally, choose uniformly at random an integer $0 < a < r$ and set $h = g^a$. Output (p, r, g, h), which can be achieved using $3\lceil \log_2(p) \rceil + \lceil \log_2(r) \rceil$ bits.

One sees that there are finitely many problem instances for a given value of the security parameter κ, but infinitely many instances in total. The output distribution has r uniform among $(2\kappa+1)$-bit primes, p is not at all random (it is essentially determined by r), while the pair (g, h) is uniformly distributed in the set of pairs of elements of order r in $\mathbb{F}_p^*$, but not necessarily well-distributed in $(\mathbb{F}_p^*)^2$.

When considering an algorithm A to solve a computational problem we assume that A has been customised for a particular instance generator. Hence, a problem might be easy with respect to some instance generators and hard for others. Thus it makes no sense to claim that "DLP is a hard problem"; instead, one should conjecture that DLP is hard for certain instance generators.

We now define what is meant by the word negligible.

Definition 2.1.10. A function $\epsilon : \mathbb{N} \to \mathbb{R}_{>0}$ is **negligible** if for every polynomial $p(x) \in \mathbb{R}[x]$ there is some $K \in \mathbb{N}$ such that for all $\kappa > K$ with $p(\kappa) \neq 0$ we have $\epsilon(\kappa) < 1/|p(\kappa)|$.

A function $\epsilon : \mathbb{N} \to \mathbb{R}_{>0}$ is **noticeable** if there exists a polynomial $p(x) \in \mathbb{R}[x]$ and an integer K such that $\epsilon(\kappa) > 1/|p(\kappa)|$ for all $\kappa > K$ with $p(\kappa) \neq 0$.

[3] For problems related to RSA or factoring, we may either take κ to be the bit-length of the modulus, or assume the output is $O(\kappa^3)$ bits.

[4] In practice, to ensure the discrete logarithm problem can't be solved in 2^κ bit operations using index calculus algorithms, one would choose k large enough that $L_p(1/3, 1.5) > 2^{kappa}$.

Let $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. A function $p : \mathbb{N} \to [0,1]$ is **overwhelming** if $1 - p(\kappa)$ is negligible.

Note that noticeable is not the logical negation of negligible. There are functions that are neither negligible nor noticeable.

Example 2.1.11. The function $\epsilon(\kappa) = 1/2^\kappa$ is negligible.

Exercise 2.1.12. Let $f_1(\kappa)$ and $f_2(\kappa)$ be negligible functions. Prove that $f_1 + f_2$ is a negligible function and that $p(\kappa)f_1(\kappa)$ is a negligible function for any polynomial $p(x) \in \mathbb{R}[x]$ such that $p(x) > 0$ for all sufficiently large x.

Definition 2.1.13. Let A be a randomised algorithm to solve instances of a computational problem generated by a specific instance generator. The **success probability** of the algorithm A is the function $f : \mathbb{N} \to [0,1]$ such that, for $\kappa \in \mathbb{N}$, $f(\kappa)$ is the probability that A outputs the correct answer, where the probability is taken over the randomness used by A and according to the output distribution of the instance generator on input κ. An algorithm A with respect to an instance generator **succeeds** if its success probability is a noticeable function.

Note that the success probability is taken over both the random choices made by A and the distribution of problem instances. In particular, an algorithm that succeeds does not necessarily solve a specific problem instance even when run repeatedly with different random choices.

Example 2.1.14. Consider an algorithm A for the DLP with respect to the instance generator of Example 2.1.9. Suppose A simply outputs an integer a chosen uniformly at random in the range $0 < a < r$. Since $r > 2^{2\kappa}$ the probability that A is correct is $1/(r-1) \leq 1/2^{2\kappa}$. For any polynomial $p(x)$ there are $X, c \in \mathbb{R}_{>0}$ and $n \in \mathbb{N}$ such that $|p(x)| \leq cx^n$ for $x \geq X$. Similarly, there is some $K \geq X$ such that $cK^n \leq 2^{2K}$. Hence, the success probability of A is negligible.

Certain decision problems (for example, decision Diffie-Hellman) require an algorithm to behave differently when given inputs drawn from different distributions on the same underlying set. In this case, the success probability is not the right concept and one instead uses the **advantage**. We refer to Definition 20.2.4 for an example.

Chapter 7 of Shoup [556] gives further discussion of randomised algorithms and success probabilities.

2.1.3 Reductions

An **oracle** for a computational problem takes one unit of running time, independent of the size of the instance, and returns an output. An oracle that always outputs a correct answer is called a **perfect oracle**. One can consider oracles that only output a correct answer with a certain noticeable probability (or advantage). For simplicity we usually assume that oracles are perfect and leave the details in the general case as an exercise for the reader. We sometimes use the word **reliable** for an oracle whose success probability is overwhelming (i.e., success probability $1 - \epsilon$ where ϵ is negligible) and **unreliable** for an oracle whose success probability is small (but still noticeable).

Note that the behaviour of an oracle is only defined if its input is a valid instance of the computational problem it solves. Similarly, the oracle performs with the stated success probability only if it is given problem instances drawn with the correct distribution from the set of all problem instances.

Definition 2.1.15. A **reduction** from problem A to problem B is a randomised algorithm to solve problem A (running in expected polynomial-time and having noticeable success probability) by making queries to an oracle (which succeeds with noticeable probability) to solve problem B.

If there is a reduction from problem A to problem B then we write[5]

$$\text{A} \leq_R \text{B}.$$

Theorem 2.1.16. *Let A and B be computational problems such that $A \leq_R B$. If there is a polynomial-time randomised algorithm to solve B then there is a polynomial-time randomised algorithm to solve A.*

A reduction between problems A and B therefore explains that "if you can solve B then you can solve A". This means that solving A has been "reduced" to solving problem B and we can infer that problem B is "at least as hard as" problem A or that problem A is "no harder than" problem B.

Since oracle queries take one unit of running time and reductions are polynomial-time algorithms, a reduction makes only polynomially many oracle queries.

Definition 2.1.17. If there is a reduction from A to B and a reduction from B to A then we say that problems A and B are **equivalent** and write $A \equiv_R B$.

Some authors use the phrases **polynomial-time reduction** and **polynomial-time equivalent** in place of reduction and equivalence. However, these terms have a technical meaning in complexity theory that is different from reduction (see Section 34.3 of [146]). Definition 2.1.15 is closer to the notion of Turing reduction, except that we allow randomised algorithms whereas a Turing reduction is a deterministic algorithm. We abuse terminology and define the terms **subexponential-time reduction** and **exponential-time reduction** by relaxing the condition in Definition 2.1.15 that the algorithm be polynomial-time (these terms are used in Section 21.4.3).

2.1.4 Random Self-Reducibility

There are two different ways that an algorithm or oracle can be unreliable: First, it may be randomised and only output the correct answer with some probability; such a situation is relatively easy to deal with by repeatedly running the algorithm/oracle on the same input. The second situation, which is more difficult to handle, is when there is a subset of problem instances for which the algorithm or oracle extremely rarely or never outputs the correct solution; for this situation random self-reducibility is essential. We give a definition only for the special case of computational problems in groups.

Definition 2.1.18. Let P be a computational problem for which every instance of the problem is an n_1-tuple of elements of some cyclic group G of order r and such that the solution is an n_2-tuple of elements of G together with an n_3-tuple of elements of $\mathbb{Z}/r\mathbb{Z}$ (where n_2 or n_3 may be zero).

The computational problem P is **random self-reducible** if there is a polynomial-time algorithm that transforms an instance of the problem (with elements in a group G) into a uniformly random instance of the problem (with elements in the *same* group G) such that the solution to the original problem can be obtained in polynomial-time from the solution to the new instance.

[5]The subscript R denotes the word "reduction" and should also remind the reader that our reductions are randomised algorithms.

We stress that a random self-reduction of a computational problem in a group G gives instances of the same computational problem in the same group. In general there is no way to use information about instances of a computational problem in a group G' to solve computational problems in G if $G' \neq G$ (unless perhaps G' is a subgroup of G or vice versa).

Lemma 2.1.19. *Let G be a group and let $g \in G$ have prime order r. Then the DLP in $\langle g \rangle$ is random self-reducible.*

Proof: First, note that the DLP fits the framework of computational problems in Definition 2.1.18. Denote by $\mathcal{X}$ the set $(\langle g \rangle - \{1\}) \times \langle g \rangle$. Let $(g, h) \in \mathcal{X}$ be an instance of the DLP.

Choose $1 \leq x < r$ and $0 \leq y < r$ uniformly at random and consider the pair $(g^x, h^x g^{xy}) \in \mathcal{X}$. Every pair $(g_1, g_2) \in \mathcal{X}$ arises in this way for exactly one pair (x, y). Hence we have produced a DLP instance uniformly at random.

If a is the solution to the new DLP instance, i.e., $h^x g^{xy} = (g^x)^a$ then the solution to the original instance is

$$a - y \pmod{r}.$$

This completes the proof. □

A useful feature of random self-reducible problems is that if A is an algorithm that solves an instance of the problem in a group G with probability (or advantage) ϵ then one can obtain an algorithm A' that repeatedly calls A and solves any instance in G of the problem with overwhelming probability. This is called **amplifying** the success probability (or advantage). An algorithm to transform an unreliable oracle into a reliable one is sometimes called a **self-corrector**.

Lemma 2.1.20. *Let g have prime order r and let $G = \langle g \rangle$. Let A be an algorithm that solves the DLP in G with probability at least $\epsilon > 0$. Let $\epsilon' > 0$ and define $n = \lceil \log(1/\epsilon')/\epsilon \rceil$ (where* log *denotes the natural logarithm). Then there is an algorithm A' that solves the DLP in G with probability at least $1 - \epsilon'$. The running time of A' is $O(n \log(r))$ group operations plus n times the running time of A.*

Proof: Run A on n random self-reduced versions of the original DLP. One convenient feature of the DLP is that one can check whether a solution is correct (this takes $O(\log(r))$ group operations for each guess for the DLP).

The probability that all n trials are incorrect is at most $(1-\epsilon)^n < (e^{-\epsilon})^{\log(1/\epsilon')/\epsilon} = e^{\log(\epsilon')} = \epsilon'$. Hence A' outputs the correct answer with probability at least $1 - \epsilon'$. □

2.2 Integer Operations

We now begin our survey of efficient computer arithmetic. General references for this topic are Section 9.1 of Crandall and Pomerance [162], Section 3.3 of Shoup [556], Section 4.3.1 of Knuth [343], Chapter 1 of Brent-Zimmermann [100] and von zur Gathen and Gerhard [238].

Integers are represented as a sequence of binary words. Operations like add or multiply may correspond to many bit or word operations. The **length** of an unsigned integer a represented in binary is

$$\text{len}(a) = \begin{cases} \lfloor \log_2(a) \rfloor + 1 & \text{if } a \neq 0, \\ 1 & \text{if } a = 0. \end{cases}$$

For a signed integer we define $\text{len}(a) = \text{len}(|a|) + 1$.

The complexity of algorithms manipulating integers depends on the length of the integers, hence one should express the complexity in terms of the function len. However, it is traditional to just use $\log_2$ or the natural logarithm log.

Exercise 2.2.1. Show that, for $a \in \mathbb{N}$, $\text{len}(a) = O(\log(a))$ and $\log(a) = O(\text{len}(a))$.

Lemma 2.2.2. *Let $a, b \in \mathbb{Z}$ be represented as a sequence of binary words.*

1. *It requires $O(\log(a))$ bit operations to write a out in binary.*
2. *One can compute $a \pm b$ in $O(\max\{\log(a), \log(b)\})$ bit operations.*
3. *One can compute ab in $O(\log(a)\log(b))$ bit operations.*
4. *Suppose $|a| > |b|$. One can compute q and r such that $a = bq + r$ and $0 \leq r < |b|$ in $O(\log(b)\log(q)) = O(\log(b)(\log(a) - \log(b) + 1))$ bit operations.*

Proof: Only the final statement is non-trivial. The school method of long division computes q and r simultaneously and requires $O(\log(q)\log(a))$ bit operations. It is more efficient to compute q first by considering only the most significant $\log_2(q)$ bits of a, and then to compute r as $a - bq$. For more details see Section 4.3.1 of [343], Section 2.4 of [238] or Section 3.3.4 of [556]. □

2.2.1 Faster Integer Multiplication

An important discovery is that it is possible to multiply integers more quickly than the "school method". General references for this subject include Section 9.5 of [162], Section 4.3.3 of [343], Section 3.5 of [556] and Section 1.3 of [100].

Karatsuba multiplication is based on the observation that one can compute $(a_0 + 2^n a_1)(b_0 + 2^n b_1)$, where a_0, a_1, b_0 and b_1 are n-bit integers, in three multiplications of n-bit integers rather than four.

Exercise 2.2.3. Prove that the complexity of Karatsuba multiplication of n bit integers is $O(n^{\log_2(3)}) = O(n^{1.585})$ bit operations.
[Hint: Assume n is a power of 2.]

Toom-Cook multiplication is a generalisation of Karatsuba. Fix a value k and suppose $a = a_0 + a_1 2^n + a_2 2^{2n} + \cdots a_k 2^{kn}$ and similarly for b. One can think of a and b as being polynomials in x of degree k evaluated at 2^n and we want to compute the product $c = ab$, which is a polynomial of degree $2k$ in x evaluated at $x = 2^n$. The idea is to compute the coefficients of the polynomial c using polynomial interpolation and therefore to recover c. The arithmetic is fast if the polynomials are evaluated at small integer values. Hence, we compute $c(1) = a(1)b(1)$, $c(-1) = a(-1)b(-1)$, $c(2) = a(2)b(2)$ etc. The complexity of Toom-Cook multiplication for n-bit integers is $O(n^{\log_{k+1}(2k+1)})$ (e.g., when $k = 3$ the complexity is $O(n^{1.465})$). For more details see Section 9.5.1 of [162].

Exercise 2.2.4.★ Give an algorithm for Toom-Cook multiplication with $k = 3$.

Schönhage-Strassen multiplication multiplies n-bit integers in nearly linear time, namely $O(n\log(n)\log(\log(n)))$ bit operations, using the fast Fourier transform (FFT). The Fürer algorithm is slightly better. These algorithms are not currently used in the implementation of RSA or discrete logarithm cryptosystems so we do not describe them in this book. We refer to Sections 9.5.2 to 9.5.7 of Crandall and Pomerance [162], Chapter 8 of von zur Gathen and Gerhard [238], Chapter 2 of Brent and Zimmermann [100], Turk [611] and Chapter 4 of Borodin and Munro [88] for details.

Another alternative is residue number arithmetic which is based on the Chinese remainder theorem. It reduces large integer operations to modular computations for some set of moduli. This idea may be useful if one can exploit parallel computation (though for any given application there may be more effective uses for parallelism). These methods are not used frequently for cryptography so interested readers are referred to Section II.1.2 of [64], Section 14.5.1 of [418], Remark 10.53(ii) of [16], and Section 4.3.2 of [343].

Remark 2.2.5. In practice, the "school" method is fastest for small numbers. The crossover point (i.e., when Karatsuba becomes faster than the school method) depends on the word size of the processor and many other issues, but seems to be for numbers of around 300-1000 bits (i.e., 90-300 digits) for most computing platforms. For a popular 32 bit processor Zimmermann [642] reports reports that Karatsuba beats the school method for integers of 20 words (640 bits) and Toom-Cook with $k = 3$ beats Karatsuba at 77 words (2464 bits). Bentahar [43] reports crossovers of 23 words (i.e., about 700 bits) and 133 words (approximately 4200 bits) respectively. The crossover point for the FFT methods is much larger. Hence, for elliptic curve cryptography at current security levels the "school" method is usually used, while for RSA cryptography the Karatsuba method is usually used.

Definition 2.2.6. Denote by $M(n)$ the number of bit operations to perform a multiplication of n bit integers.

For the remainder of the book we assume that $M(n) = c_1 n^2$ for some constant c_1 when talking about elliptic curve arithmetic, and that $M(n) = c_2 n^{1.585}$ for some constant c_2 when talking about RSA .

Applications of Newton's Method

Recall that if $F : \mathbb{R} \to \mathbb{R}$ is differentiable and if x_0 is an approximation to a zero of $F(x)$ then one can efficiently get a very close approximation to the zero by running Newton's iteration

$$x_{n+1} = x_n - F(x_n)/F'(x_n).$$

Newton's method has quadratic convergence, in general, so the precision of the approximation roughly doubles at each iteration.

Integer Division

There are a number of fast algorithms to compute $\lfloor a/b \rfloor$ for $a, b \in \mathbb{N}$. This operation has important applications to efficient modular arithmetic (see Section 2.5). Section 10.5 of [16] gives an excellent survey.

We now present an application of Newton's method to this problem. The idea is to to compute a good rational approximation to $1/a$ by finding a root of $F(x) = x^{-1} - a$.

Exercise 2.2.7. Show that the Newton iteration for $F(x) = x^{-1} - a$ is $x_{n+1} = 2x_n - ax_n^2$.

First we recall that a real number α can be represented by a rational approximation $b/2^e$ where $b, e \in \mathbb{Z}$. A key feature of this representation (based on the fact that division by powers of 2 is easy) is that if we know that $|\alpha - b/2^e| < 1/2^k$ (i.e., the result is correct to precision k) then we can renormalise the representation by replacing the approximation $b/2^e$ by $\lfloor b/2^{e-k} \rceil / 2^k$.

Suppose $2^m \leq a < 2^{m+1}$. Then we take $x_0 = b_0/2^{e_0} = 1/2^m$ as the first approximation to $1/a$. In other words, $b_0 = 1$ and $e_0 = m$. The Newton iteration in this case is

$e_{n+1} = 2e_n$ and $b_{n+1} = b_n(2^{e_n+1} - ab_n)$ which requires two integer multiplications. To prevent exponential growth of the numbers b_n one can renormalise the representation according to the expected precision of that step. One can show that the total complexity of getting an approximation to $1/a$ of precision m is $O(M(m))$ bit operations. For details see Section 3.5 of [556] (especially Exercise 3.35), Chapter 9 of [238] or, for a slightly different formulation, Section 9.2.2 of [162]. Applications of this idea to modular arithmetic will be given in Section 2.5.

Integer Approximations to Real Roots of Polynomials

Let $F(x) \in \mathbb{Z}[x]$. Approximations to roots of $F(x)$ in $\mathbb{R}$ can be computed using Newton's method. As a special case, integer square roots of m-bit numbers can be computed in time proportional to the cost of a multiplication of two m-bit numbers. Similarly, other roots (such as cube roots) can be computed in polynomial-time.

Exercise 2.2.8. Show that the Newton iteration for computing a square root of a is $x_{n+1} = (x_n + a/x_n)/2$. Hence, write down an algorithm to compute an integer approximation to the square root of a.

Exercise 2.2.8 can be used to test whether an integer a is a square. An alternative is to compute the Legendre symbol $(\frac{a}{p})$ for some random small primes p. For details see Exercise 2.4.9.

Exercise 2.2.9. Show that if $N = p^e$ where p is prime and $e \geq 1$ then one can factor N in polynomial-time.

2.3 Euclid's Algorithm

For $a, b \in \mathbb{N}$, Euclid's algorithm computes $d = \gcd(a, b)$. A simple way to express Euclid's algorithm is by the recursive formula

$$\gcd(a,b) = \begin{cases} \gcd(a,0) = a \\ \gcd(b, a \pmod b) & \text{if } b \neq 0. \end{cases}$$

The traditional approach is to work with positive integers a and b throughout the algorithm and to choose $a \pmod b$ to be in the set $\{0, 1, \ldots, b-1\}$. In practice, the algorithm can be used with $a, b \in \mathbb{Z}$ and it runs faster if we choose remainders in the range $\{-\lceil |b|/2 \rceil + 1, \ldots, -1, 0, 1, \ldots, \lceil |b|/2 \rceil\}$. However, for some applications (especially, those related to Diophantine approximation) the version with positive remainders is the desired choice.

In practice we often want to compute integers (s, t) such that $d = as + bt$, in which case we use the extended Euclidean algorithm. This is presented in Algorithm 1, where the integers r_i, s_i, t_i always satisfy $r_i = s_i a + t_i b$.

Theorem 2.3.1. *The complexity of Euclid's algorithm is $O(\log(a)\log(b))$ bit operations.*

Proof: Each iteration of Euclid's algorithm involves computing the quotient and remainder of division of r_{i-2} by r_{i-1} where we may assume $|r_{i-2}| > |r_{i-1}|$ (except maybe for $i = 1$). By Lemma 2.2.2 this requires $\leq c \log(r_{i-1})(\log(r_{i-2}) - \log(r_{i-1}) + 1)$ bit operations for some constant $c \in \mathbb{R}_{>0}$. Hence the total running time is at most

$$c \sum_{i \geq 1} \log(r_{i-1})(\log(r_{i-2}) - \log(r_{i-1}) + 1).$$

Algorithm 1 Extended Euclidean algorithm

INPUT: $a, b \in \mathbb{Z}$
OUTPUT: $d = \gcd(a, b)$ and $s, t \in \mathbb{Z}$ such that $d = sa + tb$
1: $r_{-1} = a,\ s_{-1} = 1,\ t_{-1} = 0$
2: $r_0 = b,\ s_0 = 0,\ t_0 = 1$
3: $i = 0$
4: **while** $(r_i \neq 0)$ **do**
5: $\quad i = i + 1$
6: $\quad$ find $q_i, r_i \in \mathbb{Z}$ such that $-|r_{i-1}|/2 < r_i \leq |r_{i-1}|/2$ and $r_{i-2} = q_i r_{i-1} + r_i$
7: $\quad s_i = s_{i-2} - q_i s_{i-1}$
8: $\quad t_i = t_{i-2} - q_i t_{i-1}$
9: **end while**
10: **return** $r_{i-1},\ s_{i-1},\ t_{i-1}$

Re-arranging terms gives

$$c \log(r_{-1}) \log(r_0) + c \sum_{i \geq 1} \log(r_{i-1})(1 + \log(r_i) - \log(r_{i-1})).$$

Now, $2|r_i| \leq |r_{i-1}|$ so $1 + \log(r_i) \leq \log(r_{i-1})$ hence all the terms in the above sum are ≤ 0. It follows that the algorithm performs $O(\log(a) \log(b))$ bit operations. □

Exercise 2.3.2. Show that the complexity of Algorithm 1 is still $O(\log(a) \log(b))$ bit operations even when the remainders in line 6 are chosen in the range $0 \leq r_i < r_{i-1}$.

A more convenient method for fast computer implementation is the binary Euclidean algorithm (originally due to Stein). This uses bit operations such as division by 2 rather than taking general quotients; see Section 4.5.2 of [343], Section 4.7 of [22], Chapter 3 of [238], Section 9.4.1 of [162] or Section 14.4.3 of [418].

There are subquadratic versions of Euclid's algorithm. One can compute the extended gcd of two n-bit integers in $O(M(n) \log(n))$ bit operations. We refer to Section 9.4 of [162], [583] or Section 11.1 of [238].

The rest of the section gives some results about Diophantine approximation that are used later (for example, in the Wiener attack on RSA, see Section 24.5.1). We assume that $a, b > 0$ and that the extended Euclidean algorithm with positive remainders is used to generate the sequence of values (r_i, s_i, t_i).

The integers s_i and t_i arising from the extended Euclidean algorithm are equal, up to sign, to the convergents of the continued fraction expansion of a/b. To be precise, if the convergents of a/b are denoted h_i/k_i for $i = 0, 1, \ldots$ then, for $i \geq 1$, $s_i = (-1)^{i-1} k_{i-1}$ and $t_i = (-1)^i h_{i-1}$. Therefore, the values (s_i, t_i) satisfy various equations, summarised below, that will be used later in the book. We refer to Chapter 10 of [276] or Chapter 7 of [468] for details on continued fractions.

Lemma 2.3.3. *Let $a, b \in \mathbb{N}$ and let $r_i, s_i, t_i \in \mathbb{Z}$ be the triples generated by running Algorithm 1 in the case of positive remainders $0 \leq r_i < r_{i-1}$.*

1. *For $i \geq 1$, $|s_i| < |s_{i+1}|$ and $|t_i| < |t_{i+1}|$.*
2. *If $a, b > 0$ then $t_i > 0$ when $i \geq 1$ is even and $t_i < 0$ when i is odd (and vice versa for s_i).*
3. $t_{i+1} s_i - t_i s_{i+1} = (-1)^{i+1}$.

4. $r_i s_{i-1} - r_{i-1} s_i = (-1)^i b$ *and* $r_i t_{i-1} - r_{i-1} t_i = (-1)^{i-1} a$. *In other words,* $r_i|s_{i-1}| + r_{i-1}|s_i| = b$ *and* $r_i|t_{i-1}| + r_{i-1}|t_i| = a$.
5. $|a/b + t_i/s_i| \leq 1/|s_i s_{i+1}|$.
6. $|r_i s_i| < |r_i s_{i+1}| \leq |b|$ *and* $|r_i t_i| < |r_i t_{i+1}| \leq |a|$.
7. *If* $s, t \in \mathbb{Z}$ *are such that* $|a/b + t/s| < 1/(2s^2)$ *then* (s, t) *is (up to sign) one of the pairs* (s_i, t_i) *computed by Euclid's algorithm.*
8. *If* $r, s, t \in \mathbb{Z}$ *satisfy* $r = as + bt$ *and* $|rs| < |b|/2$ *then* (r, s, t) *is (up to sign) one of the triples* (r_i, s_i, t_i) *computed by Euclid's algorithm.*

Proof: Statements 1, 2 and 3 are proved using the relation $s_i = (-1)^{i-1} k_{i-1}$ and $t_i = (-1)^i h_{i-1}$ where h_i/k_i are the continued fraction convergents to a/b. From Chapter 10 of [276] and Chapter 7 of [468] one knows that $h_m = q_{m+1} h_{m-1} + h_{m-2}$ and $k_m = q_{m+1} k_{m-1} + k_{m-2}$ where q_{m+1} is the quotient in iteration $m + 1$ of Euclid's algorithm. The first statement follows immediately and the third statement follows from the fact that $h_m k_{m-1} - h_{m-1} k_m = (-1)^{m-1}$. The second statement follows since $a, b > 0$ implies $h_i, k_i > 0$.

Statement 4 can be proved by induction, using the fact that $r_{i+1} s_i - r_i s_{i+1} = (r_{i-1} - q_i r_i) s_i - r_i (s_{i-1} - q_i s_i) = -(r_i s_{i-1} - r_{i-1} s_i)$. Statement 5 is the standard result (equation (10.7.7) of [276], Theorem 7.11 of [468]) that the convergents of a/b satisfy $|a/b - h_m/k_m| < 1/|k_m k_{m+1}|$. Statement 6 follows directly from statements 2 and 4. For example, $a = r_i (-1)^{i-1} t_{i-1} + r_{i-1} (-1)^i t_i$ and both terms on the right hand side are positive.

Statement 7 is also a standard result in Diophantine approximation; see Theorem 184 of [276] or Theorem 7.14 of [468].

Finally, to prove statement 8, suppose $r, s, t \in \mathbb{Z}$ are such that $r = as + bt$ and $|rs| < |b|/2$. Then

$$|a/b + t/s| = |(as + bt)/bs| = |r|/|bs| = |rs|/|bs^2| < 1/(2s^2).$$

The result follows from statement 7. □

Example 2.3.4. The first few terms of Euclid's algorithm on $a = 513$ and $b = 311$ give

i	r_i	q_i	s_i	t_i	$\lvert r_i s_i \rvert$	$\lvert r_i t_i \rvert$
-1	513	–	1	0	513	0
0	311	–	0	1	0	311
1	202	1	1	–1	202	202
2	109	1	–1	2	109	218
3	93	1	2	–3	186	279
4	16	1	–3	5	48	80
5	13	5	17	-28	221	364

One can verify that $|r_i s_i| \leq |b|$ and $|r_i t_i| \leq |a|$. Indeed, $|r_i s_{i+1}| \leq |b|$ and $|r_i t_{i+1}| \leq |a|$ as stated in part 6 of Lemma 2.3.3.

Diophantine approximation is the study of approximating real numbers by rationals. Statement 7 in Lemma 2.3.3 is a special case of one of the famous results; namely that the "best" rational approximations to real numbers are given by the convergents in their continued fraction expansion. Lemma 2.3.5 shows how the result can be relaxed slightly, giving "less good" rational approximations in terms of convergents to continued fractions.

Lemma 2.3.5. *Let* $\alpha \in \mathbb{R}$, $c \in \mathbb{R}_{>0}$ *and let* $s, t \in \mathbb{N}$ *be such that* $|\alpha - t/s| < c/s^2$. *Then* $(t, s) = (uh_{n+1} \pm vh_n, uk_{n+1} \pm vk_n)$ *for some* $n, u, v \in \mathbb{Z}_{\geq 0}$ *such that* $uv < 2c$.

Proof: See Theorem 1 and Remark 2 of Dujella [184]. □

We now remark that continued fractions allow one to compute solutions to Pell's equation.

Theorem 2.3.6. *Let $d \in \mathbb{N}$ be square-free. Then the continued fraction expansion of $\sqrt{d}$ is periodic; denote by r the period. Let h_n/k_n be the convergents in the continued fraction expansion of $\sqrt{d}$. Then $h_{nr-1}^2 - dk_{nr-1}^2 = (-1)^{nr}$ for $n \in \mathbb{N}$. Furthermore, every solution of the equation $x^2 - dy^2 = \pm 1$ arises in this way.*

Proof: See Corollary 7.23 of [468]. □

2.4 Computing Legendre and Jacobi Symbols

The Legendre symbol tells us when an integer is a square modulo p. It is a non-trivial group homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ to the multiplicative group $\{-1, 1\}$.

Definition 2.4.1. Let p be an odd prime and $a \in \mathbb{Z}$. The **Legendre symbol** $(\frac{a}{p})$ is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution.} \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise} \end{cases}$$

If p is prime and $a \in \mathbb{Z}$ satisfies $(\frac{a}{p}) = 1$ then a is a **quadratic residue**, while if $(\frac{a}{p}) = -1$ then a is a **quadratic non-residue**.

Let $n = \prod_i p_i^{e_i}$ be odd. The **Jacobi symbol** is

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i}.$$

A further generalisation is the **Kronecker symbol** $(\frac{a}{n})$ which allows n to be even. This is defined in equation (25.4), which is the only place in the book that it is used.

Exercise 2.4.2. Show that if p is an odd prime then $(\frac{a}{p}) = 1$ for exactly half the integers $1 \leq a \leq p-1$.

Theorem 2.4.3. *Let $n \in \mathbb{N}$ be odd and $a \in \mathbb{Z}$. The Legendre and Jacobi symbols satisfy the following properties.*

- $(\frac{a}{n}) = (\frac{a \pmod n}{n})$ *and* $(\frac{1}{n}) = 1$.
- *(Euler's criterion) If n is prime then* $(\frac{a}{n}) = a^{(n-1)/2} \pmod n$.
- *(Multiplicative)* $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$ *for all* $a, b \in \mathbb{Z}$.
- $(\frac{-1}{n}) = (-1)^{(n-1)/2}$. *In other words*

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4, \\ -1 & \text{otherwise} \end{cases}$$

- $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$. *In other words*

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \pmod 8, \\ -1 & \text{otherwise} \end{cases}$$

- *(Quadratic reciprocity) Let n and m be odd integers with* $\gcd(m,n)=1$. *Then*

$$\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{m}{n}\right).$$

In other words, $(\frac{n}{m}) = (\frac{m}{n})$ *unless* $m \equiv n \equiv 3 \pmod 4$.

Proof: See Section II.2 of [348], Sections 3.1, 3.2 and 3.3 of [468] or Chapter 6 of [276]. □

An important fact is that it is not necessary to factor integers to compute the Jacobi symbol.

Exercise 2.4.4. Write down an algorithm to compute Legendre and Jacobi symbols using quadratic reciprocity.

Exercise 2.4.5. Prove that the complexity of computing $(\frac{m}{n})$ is $O(\log(m)\log(n))$ bit operations.

Exercise 2.4.6. Give a randomised algorithm to compute a quadratic non-residue modulo p. What is the expected complexity of this algorithm?

Exercise 2.4.7. Several applications require knowing a quadratic non-residue modulo a prime p. Prove that the values a in the following table satisfy $(\frac{a}{p}) = -1$.

p	a
$p \equiv 3 \pmod 4$	-1
$p \equiv 1 \pmod 4$, $p \equiv 2 \pmod 3$	3
$p \equiv 1 \pmod 4$, $p \not\equiv 1 \pmod 8$	$\sqrt{-1}$
$p \equiv 1 \pmod 8$, $p \not\equiv 1 \pmod{16}$	$(1+\sqrt{-1})/\sqrt{2}$

Remark 2.4.8. The problem of computing quadratic non-residues has several algorithmic implications. One conjectures that the least quadratic non-residue modulo p is $O(\log(p)\log(\log(p)))$. Burgess proved that the least quadratic non-residue modulo p is at most $p^{1/(4\sqrt{e})+o(1)} \approx p^{0.151633+o(1)}$ while Ankeny showed, assuming the extended Riemann hypothesis, that it is $O(\log(p)^2)$. We refer to Section 8.5 of Bach and Shallit [22] for details and references. It follows that one can compute a quadratic non-residue in $O(\log(p)^4)$ bit operations assuming the extended Riemann hypothesis.

Exercise 2.4.9. Give a Las Vegas algorithm to test whether $a \in \mathbb{N}$ is a square by computing $(\frac{a}{p})$ for some random small primes p. What is the complexity of this algorithm?

Exercise 2.4.10. Let p be prime. In Section 2.8 we give algorithms to compute modular exponentiation quickly. Compare the cost of computing $(\frac{a}{p})$ using quadratic reciprocity versus using Euler's criterion.

Remark 2.4.11. An interesting computational problem (considered, for example, by Damgård [164]) is: given a prime p an integer k and the sequence $(\frac{a}{p}), (\frac{a+1}{p}), \ldots, (\frac{a+k-1}{p})$ to output $(\frac{a+k}{p})$. A potentially harder problem is to determine a given the sequence of values. It is known that if k is a little larger than $\log_2(p)$ then a is usually uniquely determined modulo p and so both problems make sense. No efficient algorithms are known to solve either of these problems. One can also consider the natural analogue for Jacobi symbols. We refer to [164] for further details. This is also discussed as Conjecture 2.1 of Boneh and Lipton [83]. The pseudorandomness of the sequence is discussed by Mauduit and Sárközy [401] and Sárközy and Stewart [510].

Finally, we remark that one can compute the Legendre or Jacobi symbol of n-bit integers in $O(M(n)\log(n))$ operations using an analogue of fast algorithms for computing gcds. We refer to Exercise 5.52 (also see pages 343-344) of Bach and Shallit [22] or Brent and Zimmermann [101] for the details.

2.5 Modular Arithmetic

In cryptography, modular arithmetic (i.e., arithmetic modulo $n \in \mathbb{N}$) is a fundamental building block. We represent elements of $\mathbb{Z}/n\mathbb{Z}$ as integers from the set $\{0, 1, \ldots, n-1\}$. We first summarise the complexity of standard "school" methods for modular arithmetic.

Lemma 2.5.1. *Let $a, b \in \mathbb{Z}/n\mathbb{Z}$.*

1. *Computing $a \pm b \pmod n$ can be done in $O(\log(n))$ bit operations.*
2. *Computing $ab \pmod n$ can be done in $O(\log(n)^2)$ bit operations.*
3. *Computing $a^{-1} \pmod n$ can be done in $O(\log(n)^2)$ bit operations.*
4. *For $a \in \mathbb{Z}$ computing $a \pmod n$ can be done in $O(\log(n)(\log(a) - \log(n) + 1))$ bit operations.*

Montgomery Multiplication

This method[6] is useful when one needs to perform an operation such as $a^m \pmod n$ when n is odd. It is based on the fact that arithmetic modulo 2^s is easier than arithmetic modulo n. Let $R = 2^s > n$ (where s is typically a multiple of the word size).

Definition 2.5.2. Let $n \in \mathbb{N}$ be odd and $R = 2^s > n$. The **Montgomery representation** of $a \in (\mathbb{Z}/n\mathbb{Z})$ is $\overline{a} = aR \pmod n$ such that $0 \leq \overline{a} < n$.

To transform a into Montgomery representation requires a standard modular multiplication. However, Lemma 2.5.3 shows that transforming back from Montgomery representation to standard representation may be performed more efficiently.

Lemma 2.5.3. *(Montgomery reduction) Let $n \in \mathbb{N}$ be odd and $R = 2^s > n$. Let $n' = -n^{-1} \pmod R$ be such that $1 \leq n' < R$. Let $\overline{a}$ be an element of $(\mathbb{Z}/n\mathbb{Z})$ in Montgomery representation. Let $u = \overline{a}n' \pmod R$. Then $w = (\overline{a} + un)/R$ lies in $\mathbb{Z}$ and satisfies $w \equiv \overline{a}R^{-1} \pmod n$.*

Proof: Write $w' = \overline{a} + un$. Clearly $w' \equiv 0 \pmod R$ so $w \in \mathbb{Z}$. Further, $0 \leq w' \leq (n-1) + (R-1)n = Rn - 1$ and so $w < n$. Finally, it is clear that $w \equiv \overline{a}R^{-1} \pmod n$. □

The reason why this is efficient is that division by R is easy. The computation of n' is also easier than a general modular inversion (see Algorithm II.5 of [64]) and, in many applications, it can be precomputed.

We now sketch the **Montgomery multiplication** algorithm. If $\overline{a}$ and $\overline{b}$ are in Montgomery representation then we want to compute the Montgomery representation of ab, which is $\overline{a}\overline{b}R^{-1} \pmod n$. Compute $x = \overline{a}\overline{b} \in \mathbb{Z}$ so that $0 \leq x < n^2 < nR$, then compute $u = xn' \pmod R$ and $w' = x + nu \in \mathbb{Z}$. As in Lemma 2.5.3 we have $w' \equiv 0 \pmod R$ and can compute $w = w'/R$. It follows that $w \equiv \overline{a}\overline{b}R^{-1} \pmod n$ and $0 \leq w < 2n$ so $\overline{ab}$ is either w or $w - n$.

Lemma 2.5.4. *The complexity of Montgomery multiplication modulo n is $O(M(\log(n)))$ bit operations.*

[6] Credited to Montgomery [435], but apparently a similar idea was used by Hensel.

For further details see Section 9.2.1 of [162], Section II.1.4 of [64], Section 11.1.2.b of [16] or Section 2.2.4 of [274].

Faster Modular Reduction

Using Newton's method to compute $\lfloor a/n \rfloor$ one can compute $a \pmod n$ using only multiplication of integers. If $a = O(n^2)$ then the complexity is $O(M(\log(n)))$. The basic idea is to use Newton's method to compute a rational approximation to $1/a$ of the form $b/2^e$ (see Section 2.2.1) and then compute $q = \lfloor n/a \rfloor = \lfloor nb/2^e \rfloor$ and thus $r = a - nq$ is the remainder. See Exercises 3.35, 3.36 of [556] and Section 9.1 of [238] for details. For large a the cost of computing $a \pmod n$ remains $O(\log(a)\log(n))$ as before. This idea gives rise to Barret reduction; see Section 9.2.2 of [162], Section 2.3.1 of [100], Section 14.3.3 of [418], Section II.1.3 of [64], or Section 10.4.1 of [16].

Special Moduli

For cryptography based on discrete logarithms, especially elliptic curve cryptography, it is recommended to use primes of a special form to speed up arithmetic modulo p. Commonly used primes are of the form $p = 2^k - c$ for some small $c \in \mathbb{N}$ or the **NIST primes** $p = 2^{n_k w} \pm 2^{n_{k-1} w} \pm \cdots \pm 2^{n_1 w} \pm 1$ where $w = 16, 32$ or 64. In these cases it is possible to compute reduction modulo p much more quickly than for general p. See Section 2.2.6 of [274], Section 14.3.4 of [418] or Section 10.4.3 of [16] for examples and details.

Modular Inversion

Suppose that $a, n \in \mathbb{N}$ are such that $\gcd(a, n) = 1$. One can compute $a^{-1} \pmod n$ using the extended Euclidean algorithm: computing integers $s, t \in \mathbb{Z}$ such that $as + nt = 1$ gives $a^{-1} \equiv s \pmod n$. Hence, if $0 < a < n$ then one can compute $a^{-1} \pmod n$ in $O(\log(n)^2)$ bit operations, or faster using subquadratic versions of the extended Euclidean algorithm.

In practice, modular inversion is significantly slower than modular multiplication. For example, when implementing elliptic curve cryptography it is usual to assume that the cost of an inversion in $\mathbb{F}_p$ is between 8 and 50 times slower than the cost of a multiplication in $\mathbb{F}_p$ (the actual figure depends on the platform and algorithms used).

Simultaneous Modular Inversion

One can compute $a_1^{-1} \pmod n, \ldots, a_m^{-1} \pmod n$ with a single inversion modulo n and a number of multiplications modulo n using a trick due to Montgomery. Namely, one computes $b = a_1 \cdots a_m \pmod n$, computes $b^{-1} \pmod n$, and then recovers the individual a_i^{-1}.

Exercise 2.5.5. Give pseudocode for simultaneous modular inversion and show that it requires one inversion and $3(m-1)$ modular multiplications.

2.6 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) states that if $\gcd(m_1, m_2) = 1$ then there is a unique solution $0 \leq x < m_1 m_2$ to $x \equiv c_i \pmod{m_i}$ for $i = 1, 2$. Computing x can be done in polynomial-time in various ways. One method is to use the formula

$$x = c_1 + (c_2 - c_1)(m_1^{-1} \pmod{m_2}) m_1.$$

This is a special case of Garner's algorithm (see Section 14.5.2 of [418] or Section 10.6.4 of [16]).

Exercise 2.6.1. Suppose $m_1 < m_2$ and $0 \leq c_i < m_i$. What is the input size of the instance of the CRT? What is the complexity of computing the solution?

Exercise 2.6.2. Let $n > 2$ and suppose coprime integers $2 \leq m_1 < \cdots < m_n$ and integers $c_1, \ldots, c_n$ such that $0 \leq c_i < m_i$ for $1 \leq i \leq n$ are given. Let $N = \prod_{i=1}^{n} m_i$. For $1 \leq i \leq n$ define $N_i = N/m_i$ and $u_i = N_i^{-1} \pmod{m_i}$. Show that

$$x = \sum_{i=1}^{n} c_i u_i N_i \tag{2.1}$$

satisfies $x \equiv c_i \pmod{m_i}$ for all $1 \leq i \leq n$.

Show that one can compute the integer x in equation (2.1) in $O(n^2 \log(m_n)^2)$ bit operations.

Exercise 2.6.3. Show that a special case of Exercise 2.6.2 (which is recommended when many computations are required for the same pair of moduli) is to pre-compute the integers $A = u_1 N_1$ and $B = u_2 N_2$ so that $x = c_1 A + c_2 B \pmod{N}$.

Algorithm 10.22 of [238] gives an asymptotically fast CRT algorithm.

Exercise 2.6.4 gives a variant of the Chinese remainder theorem, which seems to originate in work of Montgomery and Silverman, called the **explicit Chinese remainder theorem**. This variant is useful when one wants to compute the large integer x modulo a smaller integer p and one wants to minimise the overall storage. For a more careful complexity analysis see Section 6 of Sutherland [597]; for small p he shows that the explicit CRT can be computed in $O(nM(\log(p)) + M(\log(N) + n\log(n)))$ bit operations.

Exercise 2.6.4. Let the notation be as in Exercise 2.6.2 and let p be coprime to N. The goal is to compute $x \pmod{p}$ where x is an integer such that $x \equiv c_i \pmod{m_i}$ for $1 \leq i \leq n$ and $|x| < N/2$.

Let $z = \sum_{i=1}^{n} c_i u_i / m_i \in \mathbb{Q}$. Show that $2z \notin \mathbb{Z}$ and that $0 \leq z < nm_n$. Show that the solution x to the congruences satisfying $|x| < N/2$ is equal to $Nz - N\lfloor z \rceil$.

Hence, show that

$$x \equiv \sum_{i=1}^{n} (c_i u_i (N_i \pmod{p}) \pmod{p}) - (N \pmod{p})(\lfloor z \rceil \pmod{p}) \pmod{p}. \tag{2.2}$$

Show that one can therefore compute x using equation (2.2) and representing z as a floating point number in a way that does not require knowing more than one of the values c_i at a time. Show that one can precompute $N \pmod{p}$ and $N_i \pmod{p}$ for $1 \leq i \leq n$ in $O(n(\log(m_n)\log(p) + M(\log(p)))$ bit operations. Hence show that the complexity of solving the explicit CRT is (assuming the floating point operations can be ignored) at most $O(n(\log(m_n)\log(p) + M(\log(p))))$ bit operations.

2.7 Linear Algebra

Let A be an $n \times n$ matrix over a field $\Bbbk$. One can perform Gaussian elimination to solve the linear system $A\underline{x} = \underline{b}$ (or determine there are no solutions), to compute $\det(A)$, or to compute A^{-1} in $O(n^3)$ field operations. When working over $\mathbb{R}$ a number of issues arise

due to rounding errors, but no such problems arise when working over finite fields. We refer to Section 3.3 of Joux [317] for details.

A matrix is called **sparse** if almost all entries of each row are zero. To make this precise one usually considers the asymptotic complexity of an algorithm on $m \times n$ matrices, as m and/or n tends to infinity, and where the number of non-zero entries in each row is bounded by $O(\log(n))$ or $O(\log(m))$.

One can compute the kernel (i.e., a vector $\underline{x}$ such that $A\underline{x} = \underline{0}$) of an $n \times n$ sparse matrix A over a field in $O(n^2)$ field operations using the algorithms of Wiedemann [629] or Lanczos [363]. We refer to Section 3.4 of [317] or Section 12.4 of [238] for details.

Hermite Normal Form

When working over a ring the Hermite normal form (HNF) is an important tool for solving or simplifying systems of equations. Some properties of the Hermite normal form are mentioned in Section A.11.

Algorithms to compute the HNF of a matrix are given in Section 2.4.2 of Cohen [136], Hafner and McCurley [273], Section 3.3.3 of Joux [317], Algorithm 16.26 of von zur Gathen and Gerhard [238], Section 5.3 of Schrijver [531], Kannan and Bachem [331], Storjohann and Labahn [593], and Micciancio and Warinschi [425]. Naive algorithms to compute the HNF suffer from coefficient explosion, so computing the HNF efficiently in practice, and determining the complexity of the algorithm, is non-trivial. One solution is to work modulo the determinant (or a sub-determinant) of the matrix A (see Section 2.4.2 of [136], [273] or [593] for further details). Let $A = (A_{i,j})$ be an $n \times m$ matrix over $\mathbb{Z}$ and define $\|A\|_\infty = \max_{i,j}\{|A_{i,j}|\}$. The complexity of the HNF algorithm of Storjohann and Labahn on A (using naive integer and matrix multiplication) is $O(nm^4 \log(\|A\|_\infty)^2)$ bit operations.

One can also use lattice reduction to compute the HNF of a matrix. For details see page 74 of [531], Havas, Majewski and Matthews [280], or van der Kallen [328].

2.8 Modular Exponentiation

Exponentiation modulo n can be performed in polynomial-time by the "square-and-multiply" method.[7] This method is presented in Algorithm 2; it is called a "left-to-right" algorithm as it processes the bits of the exponent m starting with the most significant bits. Algorithm 2 can be applied in any group, in which case the complexity is $O(\log(m))$ times the complexity of the group operation. In this section we give some basic techniques to speed-up the algorithm; further tricks are described in Chapter 11.

Lemma 2.8.1. *The complexity of Algorithm 2 using naive modular arithmetic is* $O(\log(m)\log(n)^2)$ *bit operations.*

Exercise 2.8.2. Prove Lemma 2.8.1.

Lemma 2.8.3. *If Montgomery multiplication (see Section 2.5) is used then the complexity of Algorithm 2.5 is* $O(\log(n)^2 + \log(m)M(\log(n)))$.

Proof: Convert g to Montgomery representation $\overline{g}$ in $O(\log(n)^2)$ bit operations. Algorithm 2 then proceeds using Montgomery multiplication in lines 5 and 7, which requires $O(\log(m)M(\log(n)))$ bit operations. Finally Montgomery reduction is used to convert the output to standard form. □

[7] This algorithm already appears in the *chandah-sūtra* by Pingala.

Algorithm 2 Square-and-multiply algorithm for modular exponentiation

INPUT: $g, n, m \in \mathbb{N}$
OUTPUT: $b \equiv g^m \pmod{n}$
1: $i = \lfloor \log_2(m) \rfloor - 1$
2: Write m in binary as $(1m_i \dots m_1 m_0)_2$
3: $b = g$
4: **while** $(i \geq 0)$ **do**
5: $\quad b = b^2 \pmod{n}$
6: $\quad$ **if** $m_i = 1$ **then**
7: $\quad\quad b = bg \pmod{n}$
8: $\quad$ **end if**
9: $\quad i = i - 1$
10: **end while**
11: **return** b

The algorithm using Montgomery multiplication is usually better than the naive version, especially when fast multiplication is available. An application of the above algorithm, where Karatsuba multiplication would be appropriate, is RSA decryption (either the standard method, or using the CRT). Since $\log(m) = \Omega(\log(n))$ in this case, decryption requires $O(\log(n)^{2.585})$ bit operations.

Corollary 2.8.4. *One can compute the Legendre symbol* $(\frac{a}{p})$ *using Euler's criterion in* $O(\log(p)M(\log(p)))$ *bit operations.*

When storage for precomputed group elements is available there are many ways to speed up exponentiation. These methods are particularly appropriate when many exponentiations of a fixed element g are required. The methods fall naturally into two types: those that reduce the number of squarings in Algorithm 2 and those that reduce the number of multiplications. An extreme example of the first type is to precompute and store $u_i = g^{2^i} \pmod{n}$ for $2 \leq i \leq \log(n)$. Given $2^l \leq m < 2^{l+1}$ with binary expansion $(1m_{l-1} \dots m_1 m_0)_2$ one computes $\prod_{i=0:m_i=1}^{l} u_i \pmod{n}$. Obviously this method is not more efficient than Algorithm 2 if g varies. An example of the second type is **sliding window methods** that we now briefly describe. Note that there is a simpler but less efficient "non-sliding" window method, also called the 2^k-ary method, which can be found in many books. Sliding window methods can be useful even in the case where g varies (e.g., Algorithm 3 below).

Given a **window length** w one precomputes $u_i = g^i \pmod{n}$ for all odd integers $1 \leq i < 2^w$. Then one runs a variant of Algorithm 2 where w (or more) squarings are performed followed by one multiplication corresponding to a w-bit sub-string of the binary expansion of m that corresponds to an odd integer. One subtlety is that algorithms based on the "square-and-multiply" idea and which use pre-computation must parse the exponent starting with the most significant bits (i.e., from left to right) whereas to work out sliding windows one needs to parse the exponent from the least significant bits (i.e., right to left).

Example 2.8.5. Let $w = 2$ so that one precomputes $u_1 = g$ and $u_3 = g^3$. Suppose m has binary expansion $(10011011)_2$. By parsing the binary expansion starting with the least significant bits one obtains the representation 10003003 (we stress that this is still a representation in base 2). One then performs the usual square-and-multiply algorithm by parsing the exponent from left to right; the steps of the sliding window algorithm are

(omitting the (mod n) notation)

$$b = u_1,\ b = b^2;\ b = b^2,\ b = b^2,\ b = b^2,\ b = bu_3,\ b = b^2,\ b = b^2,\ b = b^2,\ b = bu_3.$$

Exercise 2.8.6. Write pseudocode for the sliding window method. Show that the precomputation stage requires one squaring and $2^{w-1} - 1$ multiplications.

Exercise 2.8.7. Show that the expected number of squarings between each multiply in the sliding window algorithm is $w + 1$. Hence show that (ignoring the precomputation) exponentiation using sliding windows requires $\log(m)$ squarings and, on average, $\log(m)/(w + 1)$ multiplications.

Exercise 2.8.8. Consider running the sliding window method in a group, with varying g and m (so the powers of g must be computed for every exponentiation) but with unlimited storage. For a given bound on $\text{len}(m)$ one can compute the value for w that minimises the total cost. Verify that the choices in the following table are optimal.

$\text{len}(m)$	80	160	300	800	2000
w	3	4	5	6	7

Exercise 2.8.9. Algorithm 2 processes the bits of the exponent m from left to right. Give pseudocode for a modular exponentiation algorithm that processes the bits of the exponent m from right to left.
[Hint: Have two variables in the main loop; one that stores g^{2^i} in the i-th iteration, and the other that stores the value $g^{\sum_{j=0}^{i} a_j 2^j}$.]

Exercise 2.8.10. Write pseudocode for a right to left sliding window algorithm for computing $g^m \pmod n$, extending Exercise 2.8.9. Explain why this variant is not appropriate when using precomputation (hence, it is not so effective when computing $g^m \pmod n$ for many random m but when g is fixed).

One can also consider the opposite scenario where one is computing $g^m \pmod n$ for a fixed value m and varying g. Again, with some precomputation, and if there is sufficient storage available, one can get an improvement over the naive algorithm. The idea is to determine an efficient **addition chain** for m. This is a sequence of squarings and multiplications, depending on m, that minimises the number of group operations. More precisely, an addition chain of length l for m is a sequence $m_1, m_2, \ldots, m_l$ of integers such that $m_1 = 1$, $m_l = m$ and, for each $2 \leq i \leq l$ we have $m_i = m_j + m_k$ for some $1 \leq j \leq k < i$. One computes each of the intermediate values g^{m_i} for $2 \leq i \leq l$ with one group operation. Note that *all* these intermediate values are stored. The algorithm requires l group operations and l group elements of storage.

It is conjectured by Stolarsky that every integer m has an addition chain of length $\log_2(m) + \log_2(\text{wt}(m))$ where $\text{wt}(m)$ is the **Hamming weight** of m (i.e., the number of ones in the binary expansion of m). There is a vast literature on addition chains, we refer to Section C6 of [272], Section 4.6.3 of [343] and Section 9.2 of [16] for discussion and references.

Exercise 2.8.11. Prove that an addition chain has length at least $\log_2(m)$.

2.9 Square Roots Modulo p

There are a number of situations in this book that require computing square roots modulo a prime. Let p be an odd prime and let $a \in \mathbb{N}$. We have already shown that Legendre

symbols can be computed in polynomial-time. Hence, the decision problem "Is a a square modulo p?" is soluble in polynomial-time. But this fact does not imply that the computational problem "Find a square root of a modulo p" is easy.

We present two methods in this section. The Tonelli-Shanks algorithm [549] is the best method in practice. The Cipolla algorithm actually has better asymptotic complexity, but is usually slower than Tonelli-Shanks.

Recall that half the integers $1 \leq a < p$ are squares modulo p and, when a is square, there are two solutions $\pm x$ to the equation $x^2 \equiv a \pmod{p}$.

Lemma 2.9.1. *Let $p \equiv 3 \pmod 4$ be prime and $a \in \mathbb{N}$. If $(\frac{a}{p}) = 1$ then $x = a^{(p+1)/4} \pmod p$ satisfies $x^2 \equiv a \pmod p$.*

This result can be verified directly by computing x^2, but we give a more group-theoretic proof that helps to motivate the general algorithm.

Proof: Since $p \equiv 3 \pmod 4$ it follows that $q = (p-1)/2$ is odd. The assumption $(\frac{a}{p}) = 1$ implies that $a^q = a^{(p-1)/2} \equiv 1 \pmod p$ and so the order of a is odd. Therefore a square root of a is given by

$$x = a^{2^{-1} \pmod q} \pmod p.$$

Now, $2^{-1} \pmod q$ is just $(q+1)/2 = (p+1)/4$. □

Lemma 2.9.2. *Let p be a prime and suppose that a is a square modulo p. Write $p-1 = 2^e q$ where q is odd. Let $w = a^{(q+1)/2} \pmod p$. Then $w^2 \equiv ab \pmod p$ where b has order dividing 2^{e-1}.*

Proof: We have

$$w^2 \equiv a^{q+1} \equiv aa^q \pmod p$$

so $b \equiv a^q \pmod p$. Now a has order dividing $(p-1)/2 = 2^{e-1}q$ so b has order dividing 2^{e-1}. □

The value w is like a "first approximation" to the square root of a modulo p. To complete the computation it is therefore sufficient to compute a square root of b.

Lemma 2.9.3. *Suppose $1 < n < p$ is such that $(\frac{n}{p}) = -1$. Then $y \equiv n^q \pmod p$ has order 2^e.*

Proof: The order of y is a divisor of 2^e. The fact $n^{(p-1)/2} \equiv -1 \pmod p$ implies that y satisfies $y^{2^{e-1}} \equiv -1 \pmod p$. Hence the order of y is equal to 2^e. □

Since $\mathbb{Z}_p^*$ is a cyclic group, it follows that y generates the full subgroup of elements of order dividing 2^e. Hence, $b = y^i \pmod p$ for some $1 \leq i \leq 2^e$. Furthermore, since the order of b divides 2^{e-1} it follows that i is even.

Writing $i = 2j$ and $x = w/y^j \pmod p$ then

$$x^2 \equiv w^2/y^{2j} \equiv ab/b \equiv a \pmod p.$$

Hence, if one can compute i then one can compute the square root of a.

If e is small then the value i can be found by a brute-force search. A more advanced method is to use the Pohlig-Hellman method to solve the discrete logarithm of b to the base y (see Section 13.2 for an explanation of these terms). This idea leads to the Tonelli-Shanks algorithm for computing square roots modulo p (see Section 1.3.3 of [64] or Section 1.5 of [136]).

Exercise 2.9.4. Compute $\sqrt{3}$ modulo 61 using the Tonelli-Shanks algorithm.

Algorithm 3 Tonelli-Shanks algorithm

INPUT: a, p such that $(\frac{a}{p}) = 1$
OUTPUT: x such that $x^2 \equiv a \pmod{p}$
1: Write $p - 1 = 2^e q$ where q is odd
2: Choose random integers $1 < n < p$ until $(\frac{n}{p}) = -1$
3: Set $y = n^q \pmod{p}$
4: Set $w = a^{(q+1)/2} \pmod{p}$ and $b = a^q \pmod{p}$
5: Compute an integer j such that $b \equiv y^{2j} \pmod{p}$
6: **return** $w/y^j \pmod{p}$

Lemma 2.9.5. *The Tonelli-Shanks method is a Las Vegas algorithm with expected running time $O(\log(p)^2 M(\log(p)))$ bit operations.*

Proof: The first step of the algorithm is the requirement to find an integer n such that $(\frac{n}{p}) = -1$. This is Exercise 2.4.6 and it is the only part of the algorithm that is randomised and Las Vegas. The expected number of trials is 2. Since one can compute the Legendre symbol in $O(\log(p)^2)$ bit operations, this gives $O(\log(p)^2)$ expected bit operations, which is less than $O(\log(p)M(\log(p)))$.

The remaining parts of the algorithm amount to exponentiation modulo p, requiring $O(\log(p)M(\log(p)))$ bit operations, and the computation of the index j. Naively, this could require as many as $p - 1$ operations, but using the Pohlig-Hellman method (see Exercise 13.2.6 in Section 13.2) brings the complexity of this stage to $O(\log(p)^2 M(\log(p)))$ bit operations. □

As we will see in Exercise 2.12.6, the worst-case complexity $O(\log(p)^2 M(\log(p)))$ of the Tonelli-Shanks algorithm is actually worse than the cost of factoring quadratic polynomials using general polynomial-factorisation algorithms. But, in most practical situations, the Tonelli-Shanks algorithm is faster than using polynomial factorisation.

Exercise 2.9.6. If one precomputes y for a given prime p then the square root algorithm becomes deterministic. Show that the complexity remains the same.

Exercise 2.9.7. Show, using Remark 2.4.8, that under the extended Riemann hypothesis one can compute square roots modulo p in deterministic $O(\log(p)^4)$ bit operations.

Exercise 2.9.8. Let $r \in \mathbb{N}$. Generalise the Tonelli-Shanks algorithm so that it computes r-th roots in $\mathbb{F}_p$ (the only non-trivial case being when $p \equiv 1 \pmod{r}$).

Exercise 2.9.9. (Atkin) Let $p \equiv 5 \pmod{8}$ be prime and $a \in \mathbb{Z}$ such that $(\frac{a}{p}) = 1$. Let $z = (2a)^{(p-5)/8} \pmod{p}$ and $i = 2az^2 \pmod{p}$. Show that $i^2 = -1 \pmod{p}$ and that $w = az(i - 1)$ satisfies $w^2 \equiv a \pmod{p}$.

If $p - 1$ is highly divisible by 2 then an algorithm due to Cipolla, sketched in Exercise 2.9.10 below, is more suitable (see Section 7.2 of [22] or Section 3.5 of [418]). See Bernstein [44] for further discussion. There is a completely different algorithm due to Schoof that is deterministic and has polynomial-time complexity for fixed a as p tends to infinity.

Exercise 2.9.10. (Cipolla) Let p be prime and $a \in \mathbb{Z}$. Show that if $t \in \mathbb{Z}$ is such that $(\frac{t^2-4a}{p}) = -1$ then $x^{(p+1)/2}$ in $\mathbb{F}_p[x]/(x^2 - tx + a)$ is a square root of a modulo p. Hence write down an algorithm to compute square roots modulo p and show that it has expected running time $O(\log(p)M(\log(p)))$ bit operations.

We remark that, in some applications, one wants to compute a Legendre symbol to test whether an element is a square and, if so, compute the square root. If one computes the Legendre symbol using Euler's criterion as $a^{(p-1)/2} \pmod p$ then one will have already computed $a^q \pmod p$ and so this value can be recycled. This is not usually faster than using quadratic reciprocity for large p, but it is relevant for applications such as Lemma 21.4.9.

A related topic is, given a prime p and an integer $d > 0$, to find integer solutions (x, y), if they exist, to the equation $x^2 + dy^2 = p$. The **Cornacchia algorithm** achieves this. The algorithm is given in Section 2.3.4 of Crandall and Pomerance [162], and a proof of correctness is given in Section 4 of Schoof [530] or Morain and Nicolas [437]. In brief, the algorithm computes $p/2 < x_0 < p$ such that $x_0^2 \equiv -d \pmod p$, then runs the Euclidean algorithm on $2p$ and x_0 stopping at the first remainder $r < \sqrt{p}$, then computes $s = \sqrt{(p - r^2)/d}$ if this is an integer. The output is $(x, y) = (r, s)$. The complexity is dominated by computing the square root modulo p, and so is an expected $O(\log(p)^2 M(\log(p)))$ bit operations. A closely related algorithm finds solutions to $x^2 + dy^2 = 4p$.

2.10 Polynomial Arithmetic

Let R be a commutative ring. A polynomial in $R[x]$ of degree d is represented[8] as a $(d+1)$-tuple over R. A polynomial of degree d over $\mathbb{F}_q$ therefore requires $(d+1)\lceil \log_2(q) \rceil$ bits for its representation. An algorithm on polynomials will be polynomial-time if the number of bit operations is bounded above by a polynomial in $d \log(q)$.

Arithmetic on polynomials is analogous to integer arithmetic (indeed, it is simpler as there are no carries to deal with). We refer to Chapter 2 of [238], Chapter 18 of [556], Section 4.6 of [343] or Section 9.6 of [162] for details.

Lemma 2.10.1. *Let R be a commutative ring and $F_1(x), F_2(x) \in R[x]$.*

1. *One can compute $F_1(x) + F_2(x)$ in $O(\max\{\deg(F_1), \deg(F_2)\})$ additions in R.*
2. *One can compute $F_1(x)F_2(x)$ in $O(\deg(F_1)\deg(F_2))$ additions and multiplications in R.*
3. *If R is a field one can compute the quotient and remainder of division of $F_1(x)$ by $F_2(x)$ in $O(\deg(F_2)(\deg(F_1) - \deg(F_2) + 1))$ operations (i.e., additions, multiplications and inversions) in R.*
4. *If R is a field one can compute $F(x) = \gcd(F_1(x), F_2(x))$ and polynomials $s(x), t(x) \in R[x]$ such that $F(x) = s(x)F_1(x) + t(x)F_2(x)$, using the extended Euclidean algorithm in $O(\deg(F_1)\deg(F_2))$ operations in R.*

Exercise 2.10.2. Prove Lemma 2.10.1.

Exercise 2.10.3. ★ Describe the Karatsuba and 3-Toom-Cook algorithms for multiplication of polynomials of degree d in $\mathbb{F}_q[x]$. Show that these algorithms have complexity $O(d^{1.585})$ and $O(d^{1.404})$ multiplications in $\mathbb{F}_q$.

Asymptotically fast multiplication of polynomials, analogous to the algorithms mentioned in Section 2.2, are given in Chapter 8 of [238] or Section 18.6 of [556]. Multiplication of polynomials in $\Bbbk[x]$ of degree bounded by d can be done in $O(M(d))$ multiplications in $\Bbbk$. The methods mentioned in Section 2.5 for efficiently computing remainders

[8] We restrict attention in this and the following section to univariate polynomials. There are alternative representations for sparse and/or multivariate polynomials, but we do not consider this issue further.

$F(x) \pmod{G(x)}$ in $\Bbbk[x]$ can also be used with polynomials; see Section 9.6.2 of [162] or Section 11.1 of [238] for details. Fast variants of algorithms for the extended Euclidean algorithm for polynomials in $\Bbbk[x]$ of degree bounded by d require $O(M(d)\log(d))$ multiplications in $\Bbbk$ and $O(d)$ inversions in $\Bbbk$ (Corollary 11.6 of [238]).

Kronecker substitution is a general technique which transforms polynomial multiplication into integer multiplication. It allows multiplication of two degree d polynomials in $\mathbb{F}_q[x]$ (where q is prime) in $O(M(d(\log(q)+\log(d)))) = O(M(d\log(dq)))$ bit operations; see Section 1.3 of [100], Section 8.4 of [238] or Section 18.6 of [556]. Kronecker substitution can be generalised to bivariate polynomials and hence to polynomials over $\mathbb{F}_q$ where q is a prime power. We write $M(d,q) = M(d\log(dq))$ for the number of bit operations to multiply two degree d polynomials over $\mathbb{F}_q$.

Exercise 2.10.4. Show that Montgomery reduction and multiplication can be implemented for arithmetic modulo a polynomial $F(x) \in \mathbb{F}_q[x]$ of degree d.

Exercise 2.10.5. One can evaluate a polynomial $F(x) \in R[x]$ at a value $a \in R$ efficiently using **Horner's rule**. More precisely, if $F(x) = \sum_{i=0}^{d} F_i x^i$ then one computes $F(a)$ as $(\cdots((F_d a)a + F_{d-1})a + \cdots + F_1)a + F_0$. Write pseudocode for Horner's rule and show that the method requires d additions and d multiplications if $\deg(F(x)) = d$.

2.11 Arithmetic in Finite Fields

Efficient algorithms for arithmetic modulo p have been presented, but we now consider arithmetic in finite fields $\mathbb{F}_{p^m}$ when $m > 1$. We assume $\mathbb{F}_{p^m}$ is represented using either a polynomial basis (i.e., as $\mathbb{F}_p[x]/(F(x))$) or a normal basis. Our main focus is when either p is large and m is small, or vice versa. Optimal asymptotic complexities for the case when both p and m grow large require some care.

Exercise 2.11.1. Show that addition and subtraction of elements in $\mathbb{F}_{p^m}$ requires $O(m)$ additions in $\mathbb{F}_p$. Show that multiplication in $\mathbb{F}_{p^m}$, represented by a polynomial basis and using naive methods, requires $O(m^2)$ multiplications modulo p and $O(m)$ reductions modulo p.

If p is constant and m grows then multiplication in $\mathbb{F}_{p^m}$ requires $O(m^2)$ bit operations or, using fast polynomial arithmetic, $O(M(m))$ bit operations. If m is fixed and p goes to infinity then the complexity is $O(M(\log(p)))$ bit operations.

Inversion of elements in $\mathbb{F}_{p^m} = \mathbb{F}_p[x]/(F(x))$ can be done using the extended Euclidean algorithm in $O(m^2)$ operations in $\mathbb{F}_p$. If p is fixed and m grows then one can invert elements in $\mathbb{F}_{p^m}$ in $O(M(m)\log(m))$ bit operations.

Alternatively, for any vector space basis $\{\theta_1, \ldots, \theta_m\}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ there is an $m \times m$ matrix M over $\mathbb{F}_q$ such that the product ab for $a, b \in \mathbb{F}_{q^m}$ is given by

$$(a_1, \ldots, a_m)M(b_1, \ldots, b_m)^t = \sum_{i=1}^{m}\sum_{j=1}^{m} M_{i,j}a_i b_j$$

where $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$ are the coefficient vectors for the representation of a and b with respect to the basis.

In particular, if $\mathbb{F}_{q^m}$ is represented by a normal basis $\{\theta, \theta^q, \ldots, \theta^{q^{m-1}}\}$ then multiplication of elements in normal basis representation is given by

$$\left(\sum_{i=0}^{m-1} a_i\theta^{q^i}\right)\left(\sum_{j=0}^{m-1} b_j\theta^{q^j}\right) = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \theta^{q^i+q^j}$$

so it is necessary to precompute the representation of each term $M_{i,j} = \theta^{q^i+q^j}$ over the normal basis. Multiplication in $\mathbb{F}_{p^m}$ using a normal basis representation is typically slower than multiplication with a polynomial basis; indeed, the complexity can be as bad as $O(m^3)$ operations in $\mathbb{F}_p$. An **optimal normal basis** is a normal basis for which the number of non-zero coefficients in the product is minimal (see Section II.2.2 of [64] for the case of $\mathbb{F}_{2^m}$). Much work has been done on speeding up multiplication with optimal normal bases; for example see Bernstein and Lange [54] for discussion and references.

Raising an element of $\mathbb{F}_{q^m}$ to the q-th power is always fast since it is a linear operation. Taking q-th powers (respectively, q-th roots) is especially fast for normal bases as it is a rotation; this is the main motivation for considering normal bases. This fact has a number of important applications, see for example, Exercise 14.4.7.

The **Itoh-Tsujii inversion algorithm** [307] is appropriate when using a normal basis representation, though it can be used to compute inverses in any finite field. First we present a simple inversion algorithm for any field and later we sketch the actual Itoh-Tsujii algorithm. Let $g \in \mathbb{F}_{q^m}^*$. The idea is to exploit the fact that the norm $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(g) = g^{1+q+q^2+\cdots+q^{m-1}}$ lies in $\mathbb{F}_q$ and is therefore easier to invert than an element of $\mathbb{F}_{q^m}$.

Lemma 2.11.2. *Let $g \in \mathbb{F}_{q^m}^*$. Then*

$$g^{-1} = \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(g)^{-1} \prod_{i=1}^{m-1} g^{q^i}.$$

Exercise 2.11.3. Prove Lemma 2.11.2.

A simple inversion algorithm is to compute $h_1 = \prod_{i=1}^{m-1} g^{q^i}$ and $h_2 = gh$ using m multiplications in $\mathbb{F}_{q^m}$, then h_2^{-1} using one inversion in $\mathbb{F}_q$ and finally $g^{-1} = h_2^{-1}h_1$ with an $\mathbb{F}_q \times \mathbb{F}_{q^m}$ multiplication. The complexity of the algorithm is $O(m^3 \log(q)^2)$ bit operations using naive arithmetic, or $O(mM(m)\log(q)^2)$ using fast arithmetic when m is large and q is small. This is worse than the complexity $O(m^2 \log(q)^2)$ of the extended Euclidean algorithm.

In the case where $q = 2$ we know that $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(g) = 1$ and the algorithm simply computes g^{-1} as

$$g^{2+2^2+\cdots+2^{m-1}} = \prod_{i=1}^{m-1} g^{2^i}.$$

This formula can be derived directly using the fact $g^{2^m-1} = 1$ as

$$g^{-1} = g^{2^m-1-1} = g^{2(2^{m-1}-1)} = g^{2(1+2+2^2+\cdots+2^{m-2})}.$$

The Itoh-Tsujii algorithm then follows from a further idea, which is that one can compute $g^{2^{m-1}-1}$ in fewer than m multiplications using an appropriate addition chain. We give the details only in the special case where $m = 2^k + 1$. Since $2^{m-1} - 1 = 2^{2^k} - 1 = (2^{2^{k-1}} - 1)2^{2^{k-1}} + (2^{2^{k-1}} - 1)$ it is sufficient to compute the sequence $g^{2^{2^i}-1}$ iteratively for $i = 0, 1, \ldots, k$, each step taking some shifts and one multiplication in the field. In other words, the complexity in this case is $O(km^2 \log(q)^2) = O(\log(m)m^2 \log(q)^2)$ field operations. For details of the general case, and further discussion we refer to [307, 270].

See, for example, Fong, Hankerson, Lopez and Menezes [207] for more discussion about inversion for the fields relevant for elliptic curve cryptography.

Finally we remark that, for some computational devices, it is convenient to use finite fields $\mathbb{F}_{p^m}$ where $p \approx 2^{32}$ or $p \approx 2^{64}$. These are called **optimal extension fields** and we refer to Section 2.4 of [274] for details.

2.12 Factoring Polynomials over Finite Fields

There is a large literature on polynomial factorisation and we only give a very brief sketch of the main concepts. The basic ideas go back to Berlekamp and others. For full discussion, historical background, and extensive references see Chapter 7 of Bach and Shallit [22] or Chapter 14 of von zur Gathen and Gerhard [238]. One should be aware that for polynomials over fields of small characteristic the algorithm by Niederreiter [466] can be useful.

Let $F(x) \in \mathbb{F}_q[x]$ have degree d. If there exists $G(x) \in \mathbb{F}_q[x]$ such that $G(x)^2 \mid F(x)$ then $G(x) \mid F'(x)$ where $F'(x)$ is the derivative of $F(x)$. A polynomial is **square-free** if it has no repeated factor. It follows that $F(x)$ is square-free if $F'(x) \neq 0$ and $\gcd(F(x), F'(x)) = 1$. If $F(x) \in \mathbb{F}_q[x]$ and $S(x) = \gcd(F(x), F'(x))$ then $F(x)/S(x)$ is square-free.

Exercise 2.12.1. Determine the complexity of testing whether a polynomial $F(x) \in \mathbb{F}_q[x]$ is square-free.

Exercise 2.12.2. Show that one can reduce polynomial factorisation over finite fields to the case of factoring square-free polynomials.

Finding Roots of Polynomials in Finite Fields

Let $F(x) \in \mathbb{F}_q[x]$ have degree d. The roots of $F(x)$ in $\mathbb{F}_q$ are precisely the roots of

$$R_1(x) = \gcd(F(x), x^q - x). \tag{2.3}$$

If q is much larger than d then the efficient way to compute $R_1(x)$ is to compute $x^q \pmod{F(x)}$ using a square-and-multiply algorithm and then run Euclid's algorithm.

Exercise 2.12.3. Determine the complexity of computing $R_1(x)$ in equation (2.3). Hence explain why the decision problem "Does $F(x)$ have a root in $\mathbb{F}_q$?" has a polynomial-time solution.

The basic idea of root-finding algorithms is to note that, if q is odd, $x^q - x = x(x^{(q-1)/2} + 1)(x^{(q-1)/2} - 1)$. Hence, one can try to split[9] $R_1(x)$ by computing

$$\gcd(R_1(x), x^{(q-1)/2} - 1). \tag{2.4}$$

Similar ideas can be used when q is even (see Section 2.14.2).

Exercise 2.12.4. Show that the roots of the polynomial in equation (2.4) are precisely the $\alpha \in \mathbb{F}_q$ such that $F(\alpha) = 0$ and α is a square in $\mathbb{F}_q^*$.

To obtain a randomised (Las Vegas) algorithm to factor $R_1(x)$ completely when q is odd one simply chooses a random polynomial $u(x) \in \mathbb{F}_q[x]$ of degree $< d$ and computes

$$\gcd(R_1(x), u(x)^{(q-1)/2} - 1).$$

This computation selects those roots α of $R_1(x)$ such that $u(\alpha)$ is a square in $\mathbb{F}_q$. In practice it suffices to choose $u(x)$ to be linear. Performing this computation sufficiently many times on the resulting factors of $R_1(x)$ and taking gcds eventually leads to the complete factorisation of $R_1(x)$.

[9] We reserve the word "factor" for giving the full decomposition into irreducibles, whereas we use the word "split" to mean breaking into two pieces.

Exercise 2.12.5. Write down pseudocode for the above root finding algorithm and show that its expected complexity (without using a fast Euclidean algorithm) is bounded by $O(\log(d)(\log(q)M(d) + d^2)) = O(\log(q)\log(d)d^2)$ field operations.

Exercise 2.12.6. Let q be an odd prime power and $R(x) = x^2 + ax + b \in \mathbb{F}_q[x]$. Show that the expected complexity of finding roots of $R(x)$ using polynomial factorisation is $O(\log(q)M(\log(q)))$ bit operations.

Exercise 2.12.7. ★ Show, using Kronecker substitution, fast versions of Euclid's algorithm and other tricks, that one can compute one root in $\mathbb{F}_q$ (if any exist) of a degree d polynomial in $\mathbb{F}_q[x]$ in an expected $O(\log(qd)M(d, q))$ bit operations.

When q is even (i.e., $q = 2^m$) then, instead of $x^{(q-1)/2}$, one considers the **trace polynomial** $T(x) = \sum_{i=0}^{m-1} x^{2^i}$. (A similar idea can be used over any field of small characteristic.)

Exercise 2.12.8. Show that the roots of the polynomial $\gcd(R_1(x), T(x))$ are precisely the $\alpha \in \mathbb{F}_q$ such that $R_1(\alpha) = 0$ and $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\alpha) = 0$.

Taking random $u(x) \in \mathbb{F}_{2^m}[x]$ of degree $< d$ and then computing $\gcd(R_1(x), T(u(x)))$ gives a Las Vegas root finding algorithm as before. See Section 21.3.2 of [556] for details.

Higher Degree Factors

Having found the roots in $\mathbb{F}_q$ one can try to find factors of larger degree. The same ideas can be used. Let

$$R_2(x) = \gcd(F(x)/R_1(x), x^{q^2} - x),\ R_3(x) = \gcd(F(x)/(R_1(x)R_2(x)), x^{q^3} - x),\ \ldots.$$

Exercise 2.12.9. Show that all irreducible factors of $R_i(x)$ over $\mathbb{F}_q[x]$ have degree i.

Exercise 2.12.10. Give an algorithm to test whether a polynomial $F(x) \in \mathbb{F}_q[x]$ of degree d is irreducible. What is the complexity?

When q is odd one can factor $R_i(x)$ using similar ideas to the above, i.e., by computing

$$\gcd(R_i(x), u(x)^{(q^i-1)/2} - 1).$$

These techniques lead to the **Cantor-Zassenhaus algorithm**. It factors polynomials of degree d over $\mathbb{F}_q$ in an expected $O(d\log(d)\log(q)M(d))$ field operations. For many more details about polynomial factorisation see Section 7.4 of [22], Sections 21.3 and 21.4 of [556], Chapter 14 of [238], [370], Chapter 4 of [388, 389] or Section 4.6.2 of [343].

Exercise 2.12.11. Let $d \in \mathbb{N}$ and $F(x) \in \mathbb{F}_q[x]$ of degree d. Given $1 < b < n$ suppose we wish to output all irreducible factors of $F(x)$ of degree at most b. Show that the expected complexity is $O(b\log(d)\log(q)M(d))$ operations in $\mathbb{F}_q$. Hence, one can factor $F(x)$ completely in $O(d\log(d)\log(q)M(d))$ operations in $\mathbb{F}_q$.

Exercise 2.12.12. ★ Using the same methods as Exercise 2.12.7, show that one can find an irreducible factor of degree $1 < b < d$ of a degree d polynomial in $\mathbb{F}_q[x]$ in an expected $O(b\log(dq)M(d, q))$ bit operations.

2.13 Hensel Lifting

Hensel lifting is a tool for solving polynomial equations of the form $F(x) \equiv 0 \pmod{p^e}$ where p is prime and $e \in \mathbb{N}_{>1}$. One application of Hensel lifting is the Takagi variant of RSA, see Example 24.1.6. The key idea is given in the following Lemma.

Lemma 2.13.1. *Let $F(x) \in \mathbb{Z}[x]$ be a polynomial and p a prime. Let $x_k \in \mathbb{Z}$ satisfy $F(x_k) \equiv 0 \pmod{p^k}$ where $k \in \mathbb{N}$. Suppose $F'(x_k) \not\equiv 0 \pmod{p}$. Then one can compute $x_{k+1} \in \mathbb{Z}$ in polynomial-time such that $F(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$.*

Proof: Write $x_{k+1} = x_k + p^k z$ where z is a variable. Note that $F(x_{k+1}) \equiv 0 \pmod{p^k}$. One has

$$F(x_{k+1}) \equiv F(x_k) + p^k F'(x_k) z \pmod{p^{k+1}}.$$

Setting $z = -(F(x_k)/p^k)F'(x_k)^{-1} \pmod{p}$ gives $F(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$. □

Example 2.13.2. We solve the equation

$$x^2 \equiv 7 \pmod{3^3}.$$

Let $f(x) = x^2 - 7$. First, the equation $f(x) \equiv x^2 - 1 \pmod{3}$ has solutions $x \equiv 1, 2 \pmod{3}$. We take $x_1 = 1$. Since $f'(1) = 2 \not\equiv 0 \pmod{3}$ we can "lift" this to a solution modulo 3^2. Write $x_2 = 1 + 3z$. Then

$$f(x_2) = x_2^2 - 7 \equiv -6 + 6z \pmod{3^2}$$

or, in other words, $1 - z \equiv 0 \pmod{3}$. This has the solution $z = 1$ giving $x_2 = 4$.

Now lift to a solution modulo 3^3. Write $x_3 = 4 + 9z$. Then $f(x_3) \equiv 9 + 72z \pmod{3^3}$ and dividing by 9 yields $1 - z \equiv 0 \pmod{3}$. This has solution $z = 1$ giving $x_3 = 13$ as one solution to the original equation.

Exercise 2.13.3. The equation $x^3 \equiv 3 \pmod{5}$ has the solution $x \equiv 2 \pmod{5}$. Use Hensel lifting to find a solution to the equation $x^3 \equiv 3 \pmod{5^3}$.

Exercise 2.13.4. Let $F(x) \in \mathbb{Z}[x]$ be a polynomial and p a prime. Let $x_k \in \mathbb{Z}$ satisfy $F(x_k) \equiv 0 \pmod{p^k}$ and $F'(x_k) \not\equiv 0 \pmod{p}$. Show that the Hensel iteration can be written in the form

$$x_{k+1} = x_k - \frac{F(x_k)}{F'(x_k)}$$

just like Newton iteration. Show that Hensel lifting has quadratic convergence in this case (i.e., if $F(x_k) \equiv 0 \pmod{p^k}$ then $F(x_{k+1}) \equiv 0 \pmod{p^{2k}}$).

2.14 Algorithms in Finite Fields

We present some algorithms for constructing finite fields $\mathbb{F}_{p^m}$ when $m > 1$, solving equations in them, and transforming between different representations of them.

2.14.1 Constructing Finite Fields

Lemma A.5.1 implies a randomly chosen monic polynomial in $\mathbb{F}_q[x]$ of degree m is irreducible with probability $\geq 1/(2m)$. Hence, using the algorithm of Exercise 2.12.10 one can generate a random irreducible polynomial $F(x) \in \mathbb{F}_q[x]$ of degree m, using naive arithmetic, in $O(m^4 \log(q))$ operations in $\mathbb{F}_q$. In other words, one can construct a polynomial basis for $\mathbb{F}_{q^m}$ in $O(m^4 \log(q))$ operations in $\mathbb{F}_q$. This complexity is not the best known.

Constructing a Normal Basis

We briefly survey the literature on constructing normal bases for finite fields. We assume that a polynomial basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ has already been computed.

The simplest randomised algorithm is to choose $\theta \in \mathbb{F}_{q^m}$ at random and test whether the set $\{\theta, \theta^q, \ldots, \theta^{q^{m-1}}\}$ is linearly independent over $\mathbb{F}_q$. Corollary 3.6 of von zur Gathen and Giesbrecht [239] (also see Theorem 3.73 and Exercise 3.76 of [388, 389]) shows that a randomly chosen θ is normal with probability at least $1/34$ if $m < q^4$ and probability at least $1/(16\log_q(m))$ if $m \geq q^4$.

Exercise 2.14.1. Determine the complexity of constructing a normal basis by randomly choosing θ.

When $q > m(m-1)$ there is a better randomised algorithm based on the following result.

Theorem 2.14.2. *Let $F(x) \in \mathbb{F}_q[x]$ be irreducible of degree m and let $\alpha \in \mathbb{F}_{q^m}$ be any root of $F(x)$. Define $G(x) = F(x)/((x-\alpha)F'(\alpha)) \in \mathbb{F}_{q^m}[x]$. Then there are $q - m(m-1)$ elements $u \in \mathbb{F}_q$ such that $\theta = G(u)$ generates a normal basis.*

Proof: See Theorem 28 of Section II.N of Artin [14] or Section 3.1 of Gao [236]. □

Deterministic algorithms for constructing a normal basis have been given by Lüneburg [399] and Lenstra [379] (also see Gao [236]).

2.14.2 Solving Quadratic Equations in Finite Fields

This section is about solving quadratic equations $x^2 + ax + b = 0$ over $\mathbb{F}_q$. One can apply any of the algorithms for polynomial factorisation mentioned earlier. As we saw in Exercise 2.12.6, when q is odd, the basic method computes roots in $O(\log(q)M(\log(q)))$ bit operations. When q is odd it is also natural to use the quadratic formula and a square-roots algorithm (see Section 2.9).

Exercise 2.14.3. Generalise the Tonelli-Shanks algorithm from Section 2.9 to work for any finite field $\mathbb{F}_q$ where q is odd. Show that the complexity remains an expected $O(\log(q)^2 M(\log(q)))$ bit operations.

Exercise 2.14.4. Suppose $\mathbb{F}_{q^2}$ is represented as $\mathbb{F}_q(\theta)$ where $\theta^2 \in \mathbb{F}_q$. Show that one can compute square roots in $\mathbb{F}_{q^2}$ using two square roots in $\mathbb{F}_q$ and a small number of multiplications in $\mathbb{F}_q$.

Since squaring in $\mathbb{F}_{2^m}$ is a linear operation one can take square roots in $\mathbb{F}_{2^m}$ using linear algebra in $O(m^3)$ bit operations. The following exercise gives a method that is more efficient.

Exercise 2.14.5. Suppose one represents $\mathbb{F}_{2^m}$ using a polynomial basis $\mathbb{F}_2[x]/(F(x))$. Precompute $\sqrt{x}$ as a polynomial in x. Let $g = \sum_{i=0}^{m-1} a_i x^i$. To compute $\sqrt{g}$ write (assuming m is odd; the case of m even is similar)

$$g = \left(a_0 + a_2x^2 + \cdots + a_{m-1}x^{m-1}\right) + x\left(a_1 + a_3x^2 + \cdots + a_{m-2}x^{m-3}\right).$$

Show that

$$\sqrt{g} = \left(a_0 + a_2x + \cdots x_{m-1}x^{(m-1)/2}\right) + \sqrt{x}\left(a_1 + a_3x + \cdots + a_{m-2}x^{(m-3)/2}\right).$$

Show that this computation takes roughly half the cost of one field multiplication, and hence $O(m^2)$ bit operations.

Exercise 2.14.6. Generalise Exercise 2.14.5 to computing p-th roots in $\mathbb{F}_{p^m}$. Show that the method requires $(p-1)$ multiplications in $\mathbb{F}_{p^m}$.

We now consider how to solve quadratic equations of the form

$$x^2 + x = \alpha \tag{2.5}$$

where $\alpha \in \mathbb{F}_{2^m}$.

Exercise 2.14.7.★ Prove that the equation $x^2 + x = \alpha$ has a solution $x \in \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\alpha) = 0$.

Lemma 2.14.8. *If m is odd (we refer to Section II.2.4 of [64] for the case where m is even) then a solution to equation (2.5) is given by the* ***half trace***

$$x = \sum_{i=0}^{(m-1)/2} \alpha^{2^{2i}}. \tag{2.6}$$

Exercise 2.14.9. Prove Lemma 2.14.8. Show that the complexity of solving quadratic equations in $\mathbb{F}_q$ when $q = 2^m$ and m is odd is an expected $O(m^3)$ bit operations (or $O(m^2)$ bit operations when a normal basis is being used).

The expected complexity of solving quadratic equations in $\mathbb{F}_{2^m}$ when m is even is $O(m^4)$ bit operations, or $O(m^3)$ when a normal basis is being used. Hence, we can make the statement that the complexity of solving a quadratic equation over any field $\mathbb{F}_q$ is an expected $O(\log(q)^4)$ bit operations.

2.14.3 Isomorphisms Between Finite Fields

Computing the Minimal Polynomial of an Element

Given $g \in \mathbb{F}_{q^m}$ one can compute the minimal polynomial $F(x)$ of g over $\mathbb{F}_q$ using linear algebra. To do this one considers the set $S_n = \{1, g, g^2, \ldots, g^n\}$ for $n = 1, \ldots, m$. Let n be the smallest integer such that S_n is linearly dependent over $\mathbb{F}_q$. Then there are $a_0, \ldots, a_n \in \mathbb{F}_q$ such that $\sum_{i=0}^{n} a_i g^i = 0$. Since S_{n-1} is linearly independent it follows that $F(x) = \sum_{i=0}^{n} a_i x^i$ is the minimal polynomial for g.

Exercise 2.14.10. Show that the above algorithm requires $O(m^3)$ operations in $\mathbb{F}_q$.

Computing a Polynomial Basis for a Finite Field

Suppose $\mathbb{F}_{q^m}$ is given by some basis that is not a polynomial basis. We now give a method to compute a polynomial basis for $\mathbb{F}_{q^m}$.

If $g \in \mathbb{F}_{q^m}$ is chosen uniformly at random then, by Lemma A.8.4, with probability at least $1/q$ the element g does not lie in a subfield of $\mathbb{F}_{q^m}$ that contains $\mathbb{F}_q$. Hence the minimal polynomal $F(x)$ of g over $\mathbb{F}_q$ has degree m and the algorithm of the previous subsection computes $F(x)$. One therefore has a polynomial basis $\{1, x, \ldots, x^{m-1}\}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Exercise 2.14.11. Determine the complexity of this algorithm.

Computing Isomorphisms Between Finite Fields

Suppose one has two representations for $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$ and wants to compute an isomorphism between them. We do this in two stages: first we compute an isomorphism from any representation to a polynomial basis, and second we compute isomorphisms between any two polynomial bases. We assume that one already has an isomorphism between the corresponding representations of the subfield $\mathbb{F}_q$.

Let $\{\theta_1, \ldots, \theta_m\}$ be the vector space basis over $\mathbb{F}_q$ for one of the representations of $\mathbb{F}_{q^m}$. The first task is to compute an isomorphism from this representation to a polynomial representation. To do this one computes a polynomial basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ using the method above. One now has a monic irreducible polynomial $F(x) \in \mathbb{F}_q[x]$ of degree m and a representation $x = \sum_{i=1}^m a_i\theta_i$ for a root of $F(x)$ in $\mathbb{F}_{q^m}$. Determine the representations of $x^2, x^3, \ldots, x^m$ over the basis $\{\theta_1, \ldots, \theta_m\}$. This gives an isomorphism from $\mathbb{F}_q[x]/(F(x))$ to the original representation of $\mathbb{F}_{q^m}$. By solving a system of linear equations, one can express each of $\theta_1, \ldots, \theta_m$ with respect to the polynomial basis; this gives the isomorphism from the original representation to $\mathbb{F}_q[x]/(F(x))$. The above ideas appear in a special case in the work of Zierler [641].

Exercise 2.14.12. Determine the complexity of the above algorithm to give an isomorphism between an arbitrary vector space representation of $\mathbb{F}_{q^m}$ and a polynomial basis for $\mathbb{F}_{q^m}$.

Finally, it remains to compute an isomorphism between any two polynomial representations $\mathbb{F}_q[x]/(F_1(x))$ and $\mathbb{F}_q[y]/(F_2(y))$ for $\mathbb{F}_{q^m}$. This is done by finding a root $a(y) \in \mathbb{F}_q[y]/(F_2(y))$ of the polynomial $F_1(x)$. The function $x \mapsto a(y)$ extends to a field isomorphism from $\mathbb{F}_q[x]/(F_1(x))$ to $\mathbb{F}_q[y]/(F_2(y))$. The inverse to this isomorphism is computed by linear algebra.

Exercise 2.14.13. Determine the complexity of the above algorithm to give an isomorphism between an arbitrary vector space representation of $\mathbb{F}_{q^m}$ and a polynomial basis for $\mathbb{F}_{q^m}$.

See Lenstra [379] for deterministic algorithms to solve this problem.

Random Sampling of Finite Fields

Let $\mathbb{F}_{p^m}$ be represented as a vector space over $\mathbb{F}_p$ with basis $\{\theta_1, \ldots, \theta_m\}$. Generating an element $g \in \mathbb{F}_{p^m}$ uniformly at random can be done by selecting m integers $a_1, \ldots, a_m$ uniformly at random in the range $0 \leq a_i < p$ and taking $g = \sum_{i=1}^m a_i\theta_i$. Section 11.4 mentions some methods to get random integers modulo p from random bits.

To sample uniformly from $\mathbb{F}_{p^m}^*$ one can use the above method, repeating the process if $a_i = 0$ for all $1 \leq i \leq m$. This is much more efficient than choosing $0 \leq a < p^m - 1$ uniformly at random and computing $g = \gamma^a$ where γ is a primitive root.

2.15 Computing Orders of Elements and Primitive Roots

We first consider how to determine the order of an element $g \in \mathbb{F}_q^*$. Assume the factorisation $q - 1 = \prod_{i=1}^m l_i^{e_i}$ is known.[10] Then it is sufficient to determine, for each i, the

[10] As far as I am aware, it has not been proved that computing the order of an element in $\mathbb{F}_q^*$ is equivalent to factoring $q-1$; or even that computing the order of an element in $\mathbb{Z}_N^*$ is equivalent to factoring $\varphi(N)$. Yet it seems to be impossible to correctly determine the order of every $g \in \mathbb{F}_q^*$ without knowing the factorisation of $q-1$.

smallest $0 \leq f \leq e_i$ such that

$$g^{(q-1)/l_i^f} = 1.$$

This leads to a simple algorithm for computing the order of g that requires $O(\log(q)^4)$ bit operations.

Exercise 2.15.1. Write pseudocode for the basic algorithm for determining the order of g and determine the complexity.

The next subsection gives an algorithm (also used in other parts of the book) that leads to an improvement of the basic algorithm.

2.15.1 Sets of Exponentials of Products

We now explain how to compute sets of the form $\{g^{(q-1)/l} : l \mid (q-1)\}$ efficiently. We generalise the problem as follows. Let $N_1, \ldots, N_m \in \mathbb{N}$ and $N = \prod_{i=1}^m N_i$ (typically the integers N_i will be coprime, but it is not necessary to assume this). Let $k = \lceil \log_2(m) \rceil$ and, for $m < i \leq 2^k$ set $N_i = 1$. Let G be a group and $g \in G$ (where g typically has order $\geq N$). The goal is to efficiently compute

$$\{g^{N/N_i} : 1 \leq i \leq m\}.$$

The naive approach (computing each term separately and not using any window methods etc) requires at least

$$\sum_{i=1}^{m} \log(N/N_i) = m\log(N) - \sum_{i=1}^{m} \log(N_i) = (m-1)\log(N)$$

operations in G and at most $2m\log(N)$ operations in G.

For the improved solution one re-uses intermediate values. The basic idea can be seen in the following example. Computing products in such a way is often called using a **product tree**.

Example 2.15.2. Let $N = N_1N_2N_3N_4$ and suppose one needs to compute

$$g^{N_1N_2N_3}, g^{N_1N_2N_4}, g^{N_1N_3N_4}, g^{N_2N_3N_4}.$$

We first compute

$$h_{1,1} = g^{N_3N_4} \qquad \text{and} \qquad h_{1,2} = g^{N_1N_2}$$

in $\leq 2(\log_2(N_1N_2) + \log_2(N_3N_4)) = 2\log_2(N)$ operations. One can then compute the result

$$g^{N_1N_2N_3} = h_{1,2}^{N_3},\ g^{N_1N_2N_4} = h_{1,2}^{N_4},\ g^{N_1N_3N_4} = h_{1,1}^{N_1},\ g^{N_2N_3N_4} = h_{1,1}^{N_2}.$$

This final step requires at most $2(\log_2(N_3)+\log_2(N_4)+\log_2(N_1)+\log_2(N_2)) = 2\log_2(N)$ operations. The total complexity is at most $4\log_2(N)$ operations in the group.

The algorithm has a compact recursive description. Let F be the function that on input $(g, m, N_1, \ldots, N_m)$ outputs the list of m values g^{N/N_i} for $1 \leq i \leq m$ where $N = N_1 \cdots N_m$. Then $F(g, 1, N_1) = g$. For $m > 1$ one computes $F(g, m, N_1, \ldots, N_m)$ as follows: Let $l = \lfloor m/2 \rfloor$ and let $h_1 = g^{N_1 \cdots N_l}$ and $h_2 = g^{N_{l+1} \cdots N_m}$. Then $F(g, m, N_1, \ldots, N_m)$ is equal to the concatenation of $F(h_1, (m-l), N_{l+1}, \ldots, N_m)$ and $F(h_2, l, N_1, \ldots, N_l)$.

We introduce some notation to express the algorithm in a non-recursive format.

Definition 2.15.3. Define $S = \{1, 2, 3, \ldots, 2^k\}$. For $1 \leq l \leq k$ and $1 \leq j \leq 2^l$ define

$$S_{l,j} = \{i \in S : (j-1)2^{k-l} + 1 \leq i \leq j2^{k-l}\}$$

Lemma 2.15.4. *Let $1 \leq l \leq k$ and $1 \leq j \leq 2^l$. The sets $S_{l,j}$ satisfy:*

1. $\#S_{l,j} = 2^{k-l}$;
2. $S_{l,j} \cap S_{l,j'} = \varnothing$ *if* $j \neq j'$;
3. $\cup_{j=1}^{2^l} S_{l,j} = S$ *for all* $1 \leq l \leq k$;
4. *If* $l \geq 2$ *and* $1 \leq j \leq 2^{l-1}$ *then* $S_{l-1,j} = S_{l,2j-1} \cup S_{l,2j}$;
5. $S_{k,j} = \{j\}$ *for* $1 \leq j \leq 2^k$.

Exercise 2.15.5. Prove Lemma 2.15.4.

Definition 2.15.6. For $1 \leq l \leq k$ and $1 \leq j \leq 2^l$ define

$$h_{l,j} = g^{\prod_{j \in S - S_{l,j}} N_i}.$$

To compute $\{h_{k,j} : 1 \leq j \leq m\}$ efficiently one notes that if $l \geq 2$ and $1 \leq j \leq 2^l$ then, writing $j_1 = \lceil j/2 \rceil$,

$$h_{l,j} = h_{l-1,j_1}^{\prod_{i \in S_{l-1,j_1} - S_{l,j}} N_i}.$$

This leads to Algorithm 4.

Algorithm 4 Computing Set of Exponentials of Products

INPUT: $N_1, \ldots, N_m$
OUTPUT: $\{g^{N/N_i} : 1 \leq i \leq m\}$
1: $k = \lceil \log_2(m) \rceil$
2: $h_{1,1} = g^{N_{2^{k-1}+1} \cdots N_{2^k}}$, $h_{1,2} = g^{N_1 \cdots N_{2^{k-1}}}$
3: **for** $l = 2$ to k **do**
4: **for** $j = 1$ to 2^l **do**
5: $j_1 = \lceil j/2 \rceil$
6: $h_{l,j} = h_{l-1,j_1}^{\prod_{i \in S_{l-1,j_1} - S_{l,j}} N_i}$
7: **end for**
8: **end for**
9: **return** $\{h_{k,1}, \ldots, h_{k,m}\}$

Lemma 2.15.7. *Algorithm 4 is correct and requires $\leq 2\lceil \log_2(m) \rceil \log(N)$ group operations.*

Proof: Almost everything is left as an exercise. The important observation is that lines 4 to 7 involve raising to the power N_i for all $i \in S$. Hence the cost for each iteration of the loop in line 3 is at most $2\sum_{i=1}^{2^k} \log_2(N_i) = 2\log_2(N)$. □

This method works efficiently in all cases (i.e., it doesn't require m to be large). However, Exercise 2.15.8 shows that for small values of m there may be more efficient solutions.

Exercise 2.15.8. Let $N = N_1N_2N_3$ where $N_i \approx N^{1/3}$ for $1 \leq i \leq 3$. One can compute g^{N/N_i} for $1 \leq i \leq 3$ using Algorithm 4 or in the "naive" way. Suppose one uses the

standard square-and-multiply method for exponentiation and assume that each of N_1, N_2 and N_3 has Hamming weight about half their bit-length.

Note that the exponentiations in the naive solution are all with respect to the fixed base g. A simple optimisation is therefore to precompute all g^{2^j} for $1 \leq j \leq \log_2(N^{2/3})$. Determine the number of group operations for each algorithm if this optimisation is performed. Which is better?

Remark 2.15.9. Sutherland gives an improved algorithm (which he calls the **snowball algorithm**) as Algorithm 7.4 of [596]. Proposition 7.3 of [596] states that the complexity is

$$O(\log(N)\log(m)/\log(\log(m))) \tag{2.7}$$

group operations.

2.15.2 Computing the Order of a Group Element

We can now return to the original problem of computing the order of an element in a finite field.

Theorem 2.15.10. *Let $g \in \mathbb{F}_q^*$ and assume that the factorisation $q-1 = \prod_{i=1}^m l_i^{e_i}$ is known. Then one can determine the order of g in $O(\log(q)\log\log(q))$ multiplications in $\mathbb{F}_q$.*

Proof: The idea is to use Algorithm 4 to compute all $h_i = g^{(q-1)/l_i^{e_i}}$. Since $m = O(\log(q))$ this requires $O(\log(q)\log\log(q))$ multiplications in $\mathbb{F}_q$. One can then compute all $h_i^{l_i^f}$ for $1 \leq f < e_i$ and, since $\prod_{i=1}^m l_i^{e_i} = q-1$ this requires a further $O(\log(q))$ multiplications. □

The complexity in Theorem 2.15.10 cannot be improved to $O(\log(q)\log\log(q)/\log(\log(\log(q))))$ using the result of equation (2.7) because the value m is not always $\Theta(\log(q))$.

2.15.3 Computing Primitive Roots

Recall that $\mathbb{F}_q^*$ is a cyclic group and that a primitive root in $\mathbb{F}_q^*$ is an element of order $q-1$. We assume in this section that the factorisation of $q-1$ is known.

One algorithm to generate primitive roots is to choose $g \in \mathbb{F}_q^*$ uniformly at random and to compute the order of g using the method of Theorem 2.15.10 until an element of order $q-1$ is found. The probability that a random $g \in \mathbb{F}_q^*$ is a primitive root is $\varphi(q-1)/(q-1)$. Using Theorem A.3.1 this probability is at least $1/(6\log(\log(q)))$. Hence this gives an algorithm that requires $O(\log(q)(\log(\log(q)))^2)$ field multiplications in $\mathbb{F}_q$.

We now present a better algorithm for this problem, which works by considering the prime powers dividing $q-1$ individually. See Exercise 11.2 of Section 11.1 of [556] for further details.

Theorem 2.15.11. *Algorithm 5 outputs a primitive root. The complexity of the algorithm is $O(\log(q)\log\log(q))$ multiplications in $\mathbb{F}_q$.*

Proof: The values g_i are elements of order dividing $l_i^{e_i}$. If $g_i^{l_i^{e_i-1}} \neq 1$ then g_i has order exactly $l_i^{e_i}$. One completion of the while loop the value t is the product of m elements of maximal coprime orders $l_i^{e_i}$. Hence t is a primitive root.

Each iteration of the while loop requires $O(\log(q)\log\log(q))$ multiplications in $\mathbb{F}_q$. It remains to bound the number of iterations of the loop. First note that, by the Chinese remainder theorem, the g_i are independent and uniformly at random in subgroups of

Algorithm 5 Computing a primitive root in $\mathbb{F}_q^*$

INPUT: $q, m, \{(l_i, e_i)\}$ such that $q-1 = \prod_{i=1}^{m} l_i^{e_i}$ and the l_i are distinct primes
OUTPUT: primitive root g

```
1: Let S = {1, ..., m}
2: t = 1
3: while S ≠ ∅ do
4:     Choose g ∈ F_q^* uniformly at random
5:     Compute g_i = g^{(q-1)/l_i^{e_i}} for 1 ≤ i ≤ m using Algorithm 4
6:     for i ∈ S do
7:         if g_i^{l_i^{e_i - 1}} ≠ 1 then
8:             t = t g_i
9:             Remove i from S
10:        end if
11:    end for
12: end while
13: return t
```

order $l_i^{e_i}$. Hence, the probability that $g_i^{l_i^{e_i-1}} = 1$ is $1/l_i \leq 1/2$ and the expected number of trials for any given value g_i less than or equal to 2. Hence, the expected number of iterations of the while loop is less than or equal to 2. This completes the proof. □

2.16 Fast Evaluation of Polynomials at Multiple Points

We have seen that one can evaluate a univariate polynomial at a field element efficiently using Horner's rule. For some applications, for example the attack on small CRT exponents for RSA in Section 24.5.2, one must evaluate a fixed polynomial repeatedly at lots of field elements. Naively repeating Horner's rule n times would give a total cost of n^2 multiplications. This section shows one can solve this problem more efficiently than the naive method.

Theorem 2.16.1. *Let $F(x) \in \Bbbk[x]$ have degree n and let $x_1, \ldots, x_n \in \Bbbk$. Then one can compute $\{F(x_1), \ldots, F(x_n)\}$ in $O(M(n)\log(n))$ field operations. The storage requirement is $O(n\log(n))$ elements of $\Bbbk$.*

Proof: (Sketch) Let $t = \lceil \log_2(n) \rceil$ and set $x_i = 0$ for $n < i \leq 2^t$. For $0 \leq i \leq t$ and $1 \leq j \leq 2^{t-i}$ define

$$G_{i,j}(x) = \prod_{k=(j-1)2^i+1}^{j2^i} (x - x_k).$$

One computes the $G_{i,j}(x)$ for $i = 0, 1, \ldots, t$ using the formula $G_{i,j}(x) = G_{i-1,2j-1}(x)G_{i-1,2j}(x)$. (This is essentially the same trick as Section 2.15.1.) For each i one needs to store n elements of $\Bbbk$ to represent all the polynomials $G_{i,j}(x)$. Hence, the total storage is $n\log(n)$ elements of $\Bbbk$.

Once all the $G_{i,j}(x)$ have been computed one defines, for $0 \leq i \leq t$, $1 \leq j \leq 2^{t-i}$ the polynomials $F_{i,j}(x) = F(x) \pmod{G_{i,j}(x)}$. One computes $F_{t,0}(x) = F(x) \pmod{G_{t,0}(x)}$ and then computes $F_{i,j}(x)$ efficiently as $F_{i+1,\lfloor (j+1)/2 \rfloor}(x) \pmod{G_{i,j}(x)}$ for $i = t-1$ downto 0. Note that $F_{0,j}(x) = F(x) \pmod{(x - x_j)} = F(x_j)$ as required.

One can show that the complexity is $O(M(n)\log(n))$ operations in $\Bbbk$. For details see Theorem 4 of [611], Section 10.1 of [238] or Corollary 4.5.4 of [88]. □

Exercise 2.16.2. Show that Theorem 2.16.1 also holds when the field $\Bbbk$ is replaced by a ring.

The inverse problem (namely, determining $F(x)$ from the n pairs $(x_j, F(x_j))$) can also be solved in $O(M(n)\log(n))$ field operations; see Section 10.2 of [238].

2.17 Pseudorandom Generation

Many of the above algorithms, and also many cryptographic systems, require generation of random or pseudorandom numbers. The precise definitions for random and pseudorandom are out of the scope of this book, as is a full discussion of methods to extract almost perfect randomness from the environment and methods to generate pseudorandom sequences from a short random seed.

There are pseudorandom number generators related to RSA (the Blum-Blum-Shub generator) and discrete logarithms. Readers interest to learn more about this topic should consult Chapter 5 of [418], Chapter 3 of [343], Chapter 30 of [16], or [398].

2.18 Summary

Table 2.18 gives a brief summary of the complexities for the algorithms discussed in this chapter. The notation used in the table is $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, p is a prime, q is a prime power and $\Bbbk$ is a field. Recall that $M(m)$ is the number of bit operations to multiply two m-bit integers (which is also the number of operations in $\Bbbk$ to multiply two degree-m polynomials over a field $\Bbbk$). Similarly, $M(d, q)$ is the number of bit operations to multiply two degree-d polynomials in $\mathbb{F}_q[x]$.

Table 2.18 gives the asymptotic complexity for the algorithms that are used in cryptographic applications (i.e., for integers of, say, at most 10,000 bits). Many of the algorithms are randomised and so the complexity in those cases is the expected complexity. The reader is warned that the best possible asymptotic complexity may be different: sometimes it is sufficient to replace $M(m)$ by $m\log(m)\log(\log(m))$ to get the best complexity, but in other cases (such as constructing a polynomial basis for $\mathbb{F}_{q^m}$) there are totally different methods that have better asymptotic complexity. In cryptographic applications $M(m)$ typically behaves as $M(m) = O(m^2)$ or $M(m) = O(m^{1.585})$.

The words "$\Bbbk$-operations" includes additions, multiplications and inversions in $\Bbbk$. If inversions in $\Bbbk$ are not required in the algorithm then we say "$\Bbbk$ multiplications".

Table 2.1: Expected complexity of basic algorithms for numbers of size relevant for cryptography and related applications. The symbol $*$ indicates that better asymptotic complexities are known.

Computational problem	Expected complexity for cryptography
Multiplication of m-bit integers, $M(m)$	$O(m^2)$ or $O(m^{1.585})$ bit operations
Compute $\lfloor a/n \rfloor, a \pmod n$	$O((\log(\lvert a\rvert) - \log(n))\log(n))$ or $O(M(\log(\lvert a\rvert))$ bit operations
Compute $\lfloor \sqrt{\lvert a\rvert} \rfloor$	$O(M(\log(\lvert a\rvert)))$ bit operations
Extended $\gcd(a, b)$ where a and b are m-bit integers	$O(m^2)$ or $O(M(m)\log(m))$ bit operations
Legendre/Jacobi symbol $(\frac{a}{n})$, $\lvert a\rvert < n$	$O(\log(n)^2)$ or $O(M(\log(n))\log(\log(n)))$ bit operations
Multiplication modulo n	$O(M(\log(n)))$ bit operations
Inversion modulo n	$O(\log(n)^2)$ or $O(M(\log(n))\log(n))$ bit operations
Compute $g^m \pmod n$	$O(\log(m)M(\log(n)))$ bit operations
Compute square roots in $\mathbb{F}_q^*$ (q odd)	$O(\log(q)M(\log(q)))$ bit operations
Multiplication of two degree d polys in $\Bbbk[x]$	$O(M(d))$ $\Bbbk$-multiplications
Multiplication of two degree d polys in $\mathbb{F}_q[x]$, $M(d, q)$	$O(M(d\log(dq)))$ bit operations
Inversion in $\Bbbk[x]/(F(x))$ where $\deg(F(x)) = d$	$O(d^2)$ or $O(M(d)\log(d))$ $\Bbbk$-operations
Multiplication in $\mathbb{F}_{q^m}$	$O(M(m))$ operations in $\mathbb{F}_q$ $*$
Evaluate degree d polynomial at $\alpha \in \Bbbk$	$O(d)$ $\Bbbk$-operations
Find all roots in $\mathbb{F}_q$ of a degree d polynomial in $\mathbb{F}_q[x]$	$O(\log(d)\log(q)d^2)$ $\mathbb{F}_q$-operations $*$
Find one root in $\mathbb{F}_q$ of a degree d polynomial in $\mathbb{F}_q[x]$	$O(\log(dq)M(d, q))$ bit operations
Determine if degree d poly over $\mathbb{F}_q$ is irreducible	$O(d^3\log(q))$ $\mathbb{F}_q$-operations $*$
Factor degree d polynomial over $\mathbb{F}_q$	$O(d^3\log(q))$ $\mathbb{F}_q$-operations $*$
Construct polynomial basis for $\mathbb{F}_{q^m}$	$O(m^4\log(q))$ $\mathbb{F}_q$-operations $*$
Construct normal basis for $\mathbb{F}_{q^m}$ given a poly basis	$O(m^3\log_q(m))$ $\mathbb{F}_q$-operations $*$
Solve quadratic equations in $\mathbb{F}_q$	$O(\log(q)^4)$ bit operations $*$
Compute the minimal poly over $\mathbb{F}_q$ of $\alpha \in \mathbb{F}_{q^m}$	$O(m^3)$ $\mathbb{F}_q$-operations
Compute an isomorphism between repns of $\mathbb{F}_{q^m}$	$O(m^3)$ $\mathbb{F}_q$-operations
Compute order of $\alpha \in \mathbb{F}_q^*$ given factorisation of $q-1$	$O(\log(q)\log(\log(q)))$ $\mathbb{F}_q$-multiplications
Compute primitive root in $\mathbb{F}_q^*$ given factorisation of $q-1$	$O(\log(q)\log(\log(q)))$ $\mathbb{F}_q$-multiplications
Compute $f(\alpha_j) \in \Bbbk$ for $f \in \Bbbk[x]$ of degree n and $\alpha_1, \ldots, \alpha_n \in \Bbbk$	$O(M(n)\log(n))$ $\Bbbk$-multiplications

Chapter 3

Hash Functions and MACs

Hash functions are important tools in cryptography. In public key cryptography, they are used in key derivation functions, digital signatures and message authentication codes. We are unable to give a thorough presentation of hash functions. Instead, we refer to Chapter 4 of Katz and Lindell [334], Chapter 9 of Menezes, van Oorschot and Vanstone [418], Chapter 4 of Stinson [592] or Chapter 3 of Vaudenay [616].

3.1 Security Properties of Hash Functions

Definition 3.1.1. A **cryptographic hash function** is a deterministic algorithm H that maps bitstrings of arbitrary finite length (we denote the set of arbitrary finite length bitstrings by $\{0,1\}^*$) to bitstrings of a fixed length l (e.g., $l = 160$ or $l = 256$). A **cryptographic hash family** is a set of functions $\{H_k : k \in \mathbb{K}\}$, for some finite set $\mathbb{K}$, such that each function in the family is of the form $H_k : \{0,1\}^* \rightarrow \{0,1\}^l$.

The value k that specifies a hash function H_k from a hash family is called a key, but in many applications the key is not kept secret (an exception is message authentication codes). We now give an informal description of the typical security properties for hash functions.

1. **Preimage-resistance**: Given an l-bit string y it should be computationally infeasible to compute a bitstring x such that $H(x) = y$.
2. **Second-preimage-resistance**: Given a bitstring x and a bitstring $y = H(x)$ it should be computationally infeasible to compute a bitstring $x' \neq x$ such that $H(x') = y$.
3. **Collision-resistance**: It should be computationally infeasible to compute bitstrings $x \neq x'$ such that $H(x) = H(x')$.

In general one expects that for any $y \in \{0,1\}^l$ there are infinitely many bitstrings x such that $H(x) = y$. Hence, all the above problems will have many solutions.

To obtain a meaningful definition for collision-resistance it is necessary to consider hash families rather than hash functions. The problem is that an efficient adversary for collision-resistance against a fixed hash function H is only required to output a pair $\{x, x'\}$ of messages. As long as such a collision exists then there exists an efficient algorithm that outputs one (namely, an algorithm that has the values x and x' hard-coded into it). Note that there is an important distinction here between the running time of the algorithm and the running time of the programmer (who is obliged to compute the collision as part of their task). A full discussion of this issue is given by Rogaway [500]; also see Section 4.6.1 of Katz and Lindell [334].

Intuitively, if one can compute preimages then one can compute second-preimages (though some care is needed here to be certain that the value x' output by a pre-image oracle is not just x again; Note 9.20 of Menezes, van Oorschot and Vanstone [418] gives an artificial hash function that is second-preimage-resistant but not preimage-resistant). Similarly, if one can compute second-preimages then one can find collisions. Hence, in practice we prefer to study hash families that offer collision-resistance. For more details about these relations see Section 4.6.2 of [334], Section 4.2 of [592] or Section 10.3 of [572].

Another requirement of hash families is that they be **entropy smoothing**: If G is a "sufficiently large" finite set (i.e., $\#G \gg 2^l$) with a "sufficiently nice" distribution on it (but not necessarily uniform) then the distribution on $\{0,1\}^l$ given by $\Pr(y) = \sum_{x \in G : H(x) = y} \Pr(x)$ is "close" to uniform. We do not make this notion precise, but refer to Section 6.9 of Shoup [556].

In Section 23.2 we will need the following security notion for hash families (which is just a re-statement of second-preimage resistance).

Definition 3.1.2. Let X and Y be finite sets. A hash family $\{H_k : X \to Y : k \in \mathbb{K}\}$ is called **target-collision-resistant** if there is no polynomial-time adversary A with non-negligible advantage in the following game: A receives $x \in X$ and a key $k \in \mathbb{K}$, both chosen uniformly at random, then outputs an $x' \in X$ such that $x' \neq x$ and $H_k(x') = H_k(x)$.

For more details about target-collision-resistant hash families we refer to Section 5 of Cramer and Shoup [161].

3.2 Birthday Attack

Computing pre-images for a general hash function with l-bit output is expected to take approximately 2^l computations of the hash algorithm, but one can find collisions much more efficiently. Indeed, one can find collisions in roughly $\sqrt{\pi 2^{l-1}}$ applications of the hash function using a randomised algorithm as follows: Choose a subset $\mathcal{D} \subset \{0,1\}^l$ of distinguished points (e.g., those whose κ least significant bits are all zero, for some $0 < \kappa < l/4$). Choose random starting values $x_0 \in \{0,1\}^l$ (Joux [317] suggests that these should be distinguished points) and compute the sequence $x_n = H(x_{n-1})$ for $n = 1, 2, \ldots$ until $x_n \in \mathcal{D}$. Store (x_0, x_n) (i.e., the starting point and the ending distinguished point) and repeat. When the same distinguished point x is found twice then, assuming the starting points x_0 and x'_0 are distinct, one can find a collision in the hash function by computing the full sequences x_i and x'_j and determining the smallest integers i and j such that $x_i = x'_j$ and hence the collision is $H(x_{i-1}) = H(x'_{j-1})$.

If we assume that values x_i are close to uniformly distributed in $\{0,1\}^l$ then, by the birthday paradox, one expects to have a collision after $\sqrt{\pi 2^l / 2}$ strings have been

encountered (i.e., that many evaluations of the hash function). The storage required is expected to be

$$\sqrt{\pi 2^{l-1}}\frac{\#\mathcal{D}}{2^l}$$

pairs (x_0, x_n). For the choice of $\mathcal{D}$ as above, this would be about $2^{l/2-\kappa}$ bitstrings of storage. For many more details on this topic see Section 7.5 of Joux [317], Section 9.7.1 of Menezes, van Oorschot and Vanstone [418] or Section 3.2 of Vaudenay [616].

This approach also works if one wants to find collisions under some constraint on the messages (for example, all messages have a fixed prefix or suffix).

3.3 Message Authentication Codes

Message authentication codes are a form of symmetric cryptography. The main purpose is for a sender and receiver who share a secret key k to determine whether a communication between them has been tampered with.

A **message authentication code** (**MAC**) is a set of functions $\{\mathsf{MAC}_k(x) : k \in \mathbb{K}\}$ such that $\mathsf{MAC}_k : \{0,1\}^* \to \{0,1\}^l$. Note that this is exactly the same definition as a hash family. The difference between MACs and hash families lies in the security requirement; in particular the security model for MACs assumes the adversary does not know the key k. Informally, a MAC is secure against forgery if there is no efficient adversary that, given pairs $(x_i, y_i) \in \{0,1\}^* \times \{0,1\}^l$ such that $y_i = \mathsf{MAC}_k(x_i)$ (for some fixed, but secret, key k) for $1 \leq i \leq n$, can output a pair $(x, y) \in \{0,1\}^* \times \{0,1\}^l$ such that $y = \mathsf{MAC}_k(x)$ but $(x, y) \neq (x_i, y_i)$ for all $1 \leq i \leq n$. For precise definitions and further details of MACs see Section 4.3 of Katz and Lindell [334], Section 9.5 of Menezes, van Oorschot and Vanstone [418], Section 6.7.2 of Shoup [556], Section 4.4 of Stinson [592] or Section 3.4 of Vaudenay [616].

There are well-known constructions of MACs from hash functions (such as HMAC, see Section 4.7 of [334], Section 4.4.1 of [592] or Section 3.4.6 of [616]) and from block ciphers (such as CBC-MAC, see Section 4.5 of [334], Section 4.4.2 of [592] or Section 3.4.4 of [616]).

3.4 Constructions of Hash Functions

There is a large literature on constructions of hash functions and it is beyond the scope of this book to give the details. The basic process is to first define a **compression function** (namely a function that takes bitstrings of a fixed length to bitstrings of some shorter fixed length) and then to build a hash function on arbitrary length bitstrings by iterating the compression function (e.g., using the Merkle-Damgård construction). We refer to Chapter 4 of Katz and Lindell [334], Sections 9.3 and 9.4 of Menezes, van Oorschot and Vanstone [418], Chapter 10 of Smart [572], Chapter 4 of Stinson [592] or Chapter 3 of Vaudenay [616] for the details.

3.5 Number-Theoretic Hash Functions

We briefly mention some compression functions and hash functions that are based on algebraic groups and number theory. These schemes are not usually used in practice as the computational overhead is usually much too high.

An early proposal for hashing based on number theory, due to Davies and Price, was to use the function $H(x) = x^2 \pmod N$ where N is an RSA modulus whose factorisation is not known. Inverting such a function or finding collisions (apart from the trivial collisions $H(x) = H(\pm x + yN)$ for $y \in \mathbb{Z}$) is as hard as factoring N. There are a number of papers that build on this idea.

Another approach to hash functions based on factoring is to let N be an RSA modulus whose factorisation is unknown and let $g \in (\mathbb{Z}/N\mathbb{Z})^*$ be fixed. One can define the compression function $H : \mathbb{N} \to (\mathbb{Z}/N\mathbb{Z})^*$ by

$$H(x) = g^x \pmod N.$$

Finding a collision $H(x) = H(x')$ is equivalent to finding a multiple of the order of g. This is hard if factoring is hard, by Exercise 24.1.20. Finding pre-images is the discrete logarithm problem modulo N, which is also as hard as factoring. Hence, we have a collision-resistant compression function. More generally, fix $g, h \in (\mathbb{Z}/N\mathbb{Z})^*$ and consider the compression function $H : \mathbb{N} \times \mathbb{N} \to (\mathbb{Z}/N\mathbb{Z})^*$ defined by $H(x, y) = g^x h^y \pmod N$. A collision leads to either finding the order of g or h, or essentially finding the discrete logarithm of h with respect to g, and all these problems are as hard as factoring.

One can also base hash functions on the discrete logarithm problem in any group G. Let $g, h \in G$ have order r. One can now consider the compression function $H : \{0, \ldots, r-1\}^2 \to G$ by $H(x, y) = g^x h^y \pmod p$. It is necessary to fix the domain of the function since $H(x, y) = H(x + r, y) = H(x, y + r)$. If one can find collisions in this function then one can compute the discrete logarithm of h to the base g. A reference for this scheme is Chaum, van Heijst and Pfitzmann [130].

3.6 Full Domain Hash

Hash functions usually output binary strings of some fixed length l. Some cryptosystems, such as full domain hash RSA signatures, require hashing uniformly (or, at least, very close to uniformly) to $\mathbb{Z}/N\mathbb{Z}$, where N is large.

Bellare and Rogaway gave two methods to do this (one in Section 6 of [38] and another in Appendix A of [41]). We briefly recall the latter. The idea is to take some hash function H with fixed length output and define a new function $h(x)$ using a constant bitstring c and a counter i as

$$h(x) = H(c\|0\|x) \,\|\, H(c\|1\|x) \,\|\, \cdots \,\|\, H(c\|i\|x).$$

For the RSA application one can construct a bitstring that is a small amount larger than N and then reduce the resulting integer modulo N (as in Example 11.4.2).

These approaches have been critically analysed by Leurent and Nguyen [385]. They give a number of results that demonstrate that care is needed in assessing the security level of a hash function with "full domain" output.

3.7 Random Oracle Model

The random oracle model is a tool for the security analysis of cryptographic systems. It is a computational model that includes the **standard model** (i.e., the computational model mentioned in Section 2.1) together with an oracle that computes a "random" function from the set $\{0,1\}^*$ (i.e., binary strings of arbitrary finite length) to $\{0,1\}^\infty$ (i.e., bitstrings of countably infinite length). Since the number of such functions is uncountable, care must

be taken when defining the word "random". In any given application, one has a fixed bit-length l in mind for the output, and one also can bound the length of the inputs. Hence, one is considering functions $H : \{0,1\}^n \to \{0,1\}^l$ and, since there are $l2^n$ such functions we can define "random" to mean uniformly chosen from the set of all possible functions. We stress that a random oracle is a function: if it is queried twice on the same input then the output is the same.

A **cryptosystem in the random oracle model** is a cryptosystem where one or more hash functions are replaced by oracle queries to the random function. A cryptosystem is **secure in the random oracle model** if the cryptosystem in the random oracle model is secure. This does not imply that the cryptosystem in the standard model is secure, since there may be an attack that exploits some feature of the hash function. Indeed, there are "artificial" cryptosystems that are proven secure in the random oracle model, but that are insecure for any instantiation of the hash function (see Canetti, Goldreich and Halevi [115]).

The random oracle model enables security proofs in several ways. We list three of these ways, in increasing order of power.

1. It ensures that the output of H is truly random (rather than merely pseudorandom).
2. It allows the security proof to "look inside" the working of the adversary by learning the values that are inputs to the hash function.
3. It allows the security proof to "programme" the hash function so that it outputs a specific value at a crucial stage in the security game.

A classic example of a proof in the random oracle model is Theorem 20.4.11. An extensive discussion of the random oracle model is given in Section 13.1 of Katz and Lindell [334].

Since a general function from $\{0,1\}^n$ to $\{0,1\}^l$ cannot be represented more compactly than by a table of values, a random oracle requires $l2^n$ bits to describe. It follows that a random oracle cannot be implemented in polynomial space. However, the crucial observation that is used in security proofs is that a random oracle can be simulated in polynomial-time and space (assuming only polynomially many queries to the oracle are made) by creating, on-the-fly, a table giving the pairs (x, y) such that $H(x) = y$.

Part II

Algebraic Groups

Chapter 4

Preliminary Remarks on Algebraic Groups

For efficient public key cryptography based on discrete logarithms one would like to have groups for which computing g^n is as fast as possible, the representation of group elements is as small as possible, and for which the DLP (see Definition 2.1.1 or 13.0.1) is (at least conjecturally) as hard as possible.

If g is a group element of order r then one needs at least $\log_2(r)$ bits to represent an arbitrary element of $\langle g \rangle$. This optimal size can be achieved by using the **exponent representation**, i.e., represent g^a as $a \in \mathbb{Z}/r\mathbb{Z}$. However, the DLP is not hard when this representation is used.

Ideally, for any cyclic group G of order r, one would like to be able to represent arbitrary group elements (in a manner which does not then render the DLP trivial) using roughly $\log_2(r)$ bits. This can be done in some cases (e.g., elliptic curves over finite fields with a prime number of points) but it is unlikely that it can always be done. Using algebraic groups over finite fields is a good way to achieve these conflicting objectives.

4.1 Informal Definition of an Algebraic Group

The subject of algebraic groups is large and has an extensive literature. Instead of presenting the full theory, in this book we present only the algebraic groups that are currently believed to be useful in public key cryptography. Informally[1], an **algebraic group** over a field $\Bbbk$ is a group such that:

- Group elements are specified as n-tuples of elements in a field $\Bbbk$;

[1] We refrain from giving a formal definition of algebraic groups; mainly as it requires defining products of projective varieties.

- The group operations (multiplication and inversion) can be performed using only polynomial equations (or ratios of polynomials) defined over $\mathbb{k}$. In other words, we have polynomial or rational maps mult : $\mathbb{k}^{2n} \to \mathbb{k}^n$ and inverse : $\mathbb{k}^n \to \mathbb{k}^n$. There is not necessarily a single n-tuple of polynomial equations that defines mult for all possible pairs of group elements.

An algebraic group quotient is the set of equivalence classes of an algebraic group under some equivalence relation (see Section 4.3 for an example). Note that, in general, an algebraic group quotient is not a group.

We stress that being an algebraic group is not a group-theoretic property; it is a property of a particular description of the group. Perhaps it helps to give an example of a group whose usual representation is not an algebraic group.

Example 4.1.1. Let $n \in \mathbb{N}$ and let S_n be the group of permutations on n symbols. Permutations can be represented as an n-tuple of distinct integers from the set $\{1, 2, \ldots, n\}$. The composition $(x_1, \ldots, x_n) \circ (y_1, \ldots, y_n)$ of two permutations is $(x_{y_1}, x_{y_2}, \ldots, x_{y_n})$. Since x_{y_1} is not a polynomial, the usual representation of S_n is not an algebraic group. However, S_n can be represented as a subgroup of the matrix group $GL_n(\mathbb{k})$ (for any field $\mathbb{k}$), which is an algebraic group.

Our main interest is algebraic groups over finite fields $\mathbb{F}_q$. For each example of an algebraic group (or quotient) G we will explain how to achieve the following basic functionalities:

- Efficient group operations in G (typically requiring $O(\log(q)^2)$ bit operations);
- Compact representation of elements of G (typically $O(\log(q))$ bits);
- Generating cryptographically suitable G in polynomial-time (i.e., $O(\log(q)^c)$ for some (small) $c \in \mathbb{N}$);
- Generating random elements in G in polynomial-time;
- Hashing from $\{0,1\}^l$ to G or from G to $\{0,1\}^l$ in polynomial-time.

In order to be able to use an algebraic group (or quotient) G for cryptographic applications we need some or all of these functionalities, as well as requiring the discrete logarithm problem (and possibly other computational problems) to be hard.

We sometimes use the notation AG to mean "algebraic group in the context of this book"; similarly AGQ means "algebraic group quotient in the context of this book". The aim of this part of the book is to describe the algebraic groups of relevance for public key cryptography (namely, multiplicative groups, algebraic tori, elliptic curves and divisor class groups). As is traditional, we will use multiplicative notation for the group operation in multiplicative groups and tori, and additive notation for the group operation on elliptic curves and divisor class groups of hyperelliptic curves. In Parts III and V, when we discuss cryptographic applications, we will always use multiplicative notation for algebraic groups.

The purpose of this chapter is to give the simplest examples of algebraic groups and quotients. The later chapters introduce enough algebraic geometry to be able to define the algebraic groups of interest in this book and prove some important facts about them.

4.2 Examples of Algebraic Groups

The simplest examples of algebraic groups are the **additive group** G_a and **multiplicative group** G_m of a field $\mathbb{k}$. For $G_a(\mathbb{k})$ the set of points is $\mathbb{k}$ and the group operation is given by the polynomial $\text{mult}(x, y) = x + y$ (for computing the group operation) and $\text{inverse}(x) = -x$ (for computing inverses). For $G_m(\mathbb{k})$ the set of points is $\mathbb{k}^* = \mathbb{k} - \{0\}$ and the group operation is given by the polynomial $\text{mult}(x, y) = xy$ and the rational function $\text{inverse}(x) = 1/x$ (Example 5.1.5 shows how to express $G_m(\mathbb{k})$ as an algebraic set).

The additive group is useless for cryptography since the discrete logarithm problem is easy. The discrete logarithm problem is also easy for the multiplicative group over certain fields (e.g., if $g \in \mathbb{R}^*$ then the discrete logarithm problem in $\langle g \rangle \subseteq \mathbb{R}^*$ is easy due to algorithms that compute approximations to the natural logarithm function). However, $G_m(\mathbb{F}_q)$ is useful for cryptography and will be one of the main examples used in this book.

The other main examples of algebraic groups in public key cryptography are algebraic tori (see Chapter 6), elliptic curves and divisor class groups of hyperelliptic curves.

4.3 Algebraic Group Quotients

Quotients of algebraic groups are used to reduce the storage and communication requirements of public key cryptosystems. Let G be a group with an automorphism ψ such that $\psi^n = 1$ (where $1 : G \to G$ is the identity map and ψ^n is the n-fold composition $\psi \circ \cdots \circ \psi$). We define $\psi^0 = 1$. Define the **orbit** or **equivalence class** of $g \in G$ under ψ to be $[g] = \{\psi^i(g) : 0 \leq i < n\}$. Define the **quotient** as the set of orbits under ψ. In other words

$$G/\psi = \{[g] : g \in G\}.$$

We call G the **covering group** of a quotient G/ψ. In general, the group structure of G does not induce a group structure on the quotient G/ψ. Nevertheless, we can define exponentiation on the quotient by $[g]^n = [g^n]$ for $n \in \mathbb{Z}$. Since exponentiation is the fundamental operation for many cryptographic applications it follows that quotients of algebraic groups are sufficient for many cryptographic applications.

Lemma 4.3.1. *Let $n \in \mathbb{Z}$ and $[g] \in G/\psi$, then $[g]^n$ is well-defined.*

Proof: Since ψ is a group homomorphism we have $\psi^i(g)^n = \psi^i(g^n)$ and so for each $g_1 \in [g]$ we have $g_1^n \in [g^n]$. □

The advantage of algebraic group quotients G/ψ is that they can require less storage than the original algebraic group G. We now give an example of this.

Example 4.3.2. Let p be an odd prime. Consider the subgroup $G \subset \mathbb{F}_{p^2}^*$ of order $p + 1$. Note that $\gcd(p - 1, p + 1) = 2$ so $G \cap \mathbb{F}_p^* = \{1, -1\}$. If $g \in G$ then we have $g^{p+1} = 1$, which is equivalent to $g^p = g^{-1}$. Let ψ be the automorphism $\psi(g) = g^p$. Then $\psi^2 = 1$ in $\mathbb{F}_{p^2}$ and the orbits $[g]$ in G/ψ all have size 2 except for $[1]$ and $[-1]$.

The natural representation for elements of $G \subseteq \mathbb{F}_{p^2}$ is a pair of elements of $\mathbb{F}_p$. However, since $\#(G/\psi) = 2 + (p - 1)/2$ one might expect to be able to represent elements of G/ψ using just one element of $\mathbb{F}_p$.

Let $g \in G$. Then the elements of $[g] = \{g, g^p\}$ are the roots of the equation $x^2 - tx + 1$ in $\mathbb{F}_{p^2}$ where $t = g + g^p \in \mathbb{F}_p$. Conversely, each $t \in \mathbb{F}_p$ such that the roots of $x^2 - tx + 1$ are Galois conjugates corresponds to a class $[g]$ (the values $t = \pm 2$ correspond to $[1]$ and $[-1]$). Hence, one can represent an element of G/ψ by the trace t. We therefore require half the storage compared with the standard representation of $G \subset \mathbb{F}_{p^2}$.

In Section 6.3.2 we show that, given the trace t of g, one can compute the trace t_n of g^n efficiently using Lucas sequences (though there is a slight catch, namely that we have to work with a pair (t_n, t_{n-1}) of traces).

Another important example of an algebraic group quotient is elliptic curve arithmetic using x-coordinates only. This is the quotient of an elliptic curve by the equivalence relation $P \equiv -P$.

4.4 Algebraic Groups over Rings

Algebraic geometry is traditionally studied over fields. However, several applications (both algorithmic and cryptographic) will exploit algebraic groups or algebraic group quotients over $\mathbb{Z}/N\mathbb{Z}$ (we do not consider general rings).

Let $N = \prod_{i=1}^{k} p_i$ be square-free (the non-square-free case is often more subtle). By the Chinese remainder theorem, $\mathbb{Z}/N\mathbb{Z}$ is isomorphic as a ring to $\oplus_{i=1}^{k} \mathbb{F}_{p_i}$ (where $\oplus$ denotes the direct sum of rings). Hence, if G is an algebraic group then it is natural to define

$$G(\mathbb{Z}/N\mathbb{Z}) = \bigoplus_{i=1}^{k} G(\mathbb{F}_{p_i}) \tag{4.1}$$

(where $\oplus$ now denotes the direct sum of groups). A problem is that this representation for $G(\mathbb{Z}/N\mathbb{Z})$ does not satisfy the natural generalisation to rings of our informal definition of an algebraic group. For example, group elements are not n-tuples over the ring, but over a collection of different fields. Also the value n is no longer bounded.

The challenge is to find a representation for $G(\mathbb{Z}/N\mathbb{Z})$ that uses n-tuples over $\mathbb{Z}/N\mathbb{Z}$ and satisfies the other properties of the informal definition. Example 4.4.1 shows that this holds for the additive and multiplicative groups.

Example 4.4.1. Let $N = \prod_i p_i$ where the p_i are distinct primes. Then, using the definition in equation (4.1),

$$G_a(\mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_i G_a(\mathbb{F}_{p_i}) \cong \bigoplus_i \mathbb{F}_{p_i} \cong \mathbb{Z}/N\mathbb{Z}.$$

Similarly,

$$G_m(\mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_i G_m(\mathbb{F}_{p_i}) \cong \bigoplus_i \mathbb{F}_{p_i}^* \cong (\mathbb{Z}/N\mathbb{Z})^*.$$

Hence, both groups can naturally be considered as algebraic groups over $\mathbb{Z}/N\mathbb{Z}$.

Note that $G_m(\mathbb{Z}/N\mathbb{Z})$ is not cyclic when N is square-free but not prime.

To deal with non-square-free N it is necessary to define $G(\mathbb{Z}/p^n\mathbb{Z})$. The details of this depend on the algebraic group. For G_a and G_m it is straightforward and we still have $G_a(\mathbb{Z}/N\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z}$ and $G_m(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^*$. For other groups it can be more complicated.

Chapter 5

Varieties

The purpose of this chapter is to state some basic definitions and results from algebraic geometry that are required for the main part of the book. In particular, we define algebraic sets, irreducibility, function fields, rational maps and dimension. The chapter is not intended as a self-contained introduction to algebraic geometry. We make the following recommendations to the reader:

1. Readers who want a very elementary introduction to elliptic curves are advised to consult one or more of Koblitz [348], Silverman-Tate [567], Washington [626], Smart [572] or Stinson [592].

2. Readers who wish to learn algebraic geometry properly should first read a basic text such as Reid [497] or Fulton [216]. They can then skim this chapter and consult Stichtenoth [589], Moreno [439], Hartshorne [278], Lorenzini [394] or Shafarevich [543] for detailed proofs and discussion.

5.1 Affine algebraic sets

Let $\mathbb{k}$ be a perfect field contained in a fixed algebraic closure $\overline{\mathbb{k}}$. All algebraic extensions $\mathbb{k}'/\mathbb{k}$ are implicitly assumed to be subfields of $\overline{\mathbb{k}}$. We use the notation $\mathbb{k}[\underline{x}] = \mathbb{k}[x_1, \ldots, x_n]$ (in later sections we also use $\mathbb{k}[\underline{x}] = \mathbb{k}[x_0, \ldots, x_n]$). When $n = 2$ or 3 we often write $\mathbb{k}[x, y]$ or $\mathbb{k}[x, y, z]$.

Define **affine n-space over** $\mathbb{k}$ as $\mathbb{A}^n(\mathbb{k}) = \mathbb{k}^n$. We call $\mathbb{A}^1(\mathbb{k})$ the **affine line** and $\mathbb{A}^2(\mathbb{k})$ the **affine plane** over $\mathbb{k}$. If $\mathbb{k} \subseteq \mathbb{k}'$ then we have the natural inclusion $\mathbb{A}^n(\mathbb{k}) \subseteq \mathbb{A}^n(\mathbb{k}')$. We write $\mathbb{A}^n$ for $\mathbb{A}^n(\overline{\mathbb{k}})$ and so $\mathbb{A}^n(\mathbb{k}) \subseteq \mathbb{A}^n$.

Definition 5.1.1. Let $S \subseteq \mathbb{k}[\underline{x}]$. Define

$$V(S) = \{P \in \mathbb{A}^n(\overline{\mathbb{k}}) : f(P) = 0 \text{ for all } f \in S\}.$$

If $S = \{f_1, \ldots, f_m\}$ then we write $V(f_1, \ldots, f_m)$ for $V(S)$. An **affine algebraic set** is a set $X = V(S) \subset \mathbb{A}^n$ where $S \subset \Bbbk[\underline{x}]$.

Let $\Bbbk'/\Bbbk$ be an algebraic extension. The $\Bbbk'$**-rational points** of $X = V(S)$ are

$$X(\Bbbk') = X \cap \mathbb{A}^n(\Bbbk') = \{P \in \mathbb{A}^n(\Bbbk') : f(P) = 0 \text{ for all } f \in S\}.$$

An algebraic set $V(f)$, where $f \in \Bbbk[\underline{x}]$, is a **hypersurface**. If $f(\underline{x})$ is a polynomial of total degree 1 then $V(f)$ is a **hyperplane**.

Informally we often write "the algebraic set $f = 0$" instead of $V(f)$. For example, $y^2 = x^3$ instead of $V(y^2 - x^3)$. We stress that, as is standard, $V(S)$ is the set of solutions over an algebraically closed field.

When an algebraic set is defined as the vanishing of a set of polynomials with coefficients in $\Bbbk$ then it is called a $\Bbbk$-algebraic set. The phrase "defined over $\Bbbk$" has a different meaning and the relation between them will be explained in Remark 5.3.7.

Example 5.1.2. If $X = V(x_1^2 + x_2^2 + 1) \subseteq \mathbb{A}^2$ over $\mathbb{Q}$ then $X(\mathbb{Q}) = \varnothing$. Let $\Bbbk = \mathbb{F}_2$ and let $X = V(y^8 + x^6y + x^3 + 1) \subseteq \mathbb{A}^2$. Then $X(\mathbb{F}_2) = \{(0,1), (1,0), (1,1)\}$.

Exercise 5.1.3. Let $\Bbbk$ be a field. Show that $\{(t, t^2) : t \in \overline{\Bbbk}\} \subseteq \mathbb{A}^2$, $\{(t, \pm\sqrt{t}) : t \in \overline{\Bbbk}\} \subseteq \mathbb{A}^2$ and $\{(t^2 + 1, t^3) : t \in \overline{\Bbbk}\} \subseteq \mathbb{A}^2$ are affine algebraic sets.

Exercise 5.1.4. Let $f(x, y) \in \Bbbk[x, y]$ be a non-constant polynomial. Prove that $V(f(x, y)) \subset \mathbb{A}^2$ is an infinite set.

Example 5.1.5. Let $\Bbbk$ be a field. There is a one-to-one correspondence between the set $\Bbbk^*$ and the $\Bbbk$-rational points $X(\Bbbk)$ of the affine algebraic set $X = V(xy - 1) \subset \mathbb{A}^2$. Multiplication in the field $\Bbbk$ corresponds to the function mult : $X \times X \to X$ given by $\text{mult}((x_1, y_1), (x_2, y_2)) = (x_1x_2, y_1y_2)$. Similarly, inversion in $\Bbbk^*$ corresponds to the function $\text{inverse}(x, y) = (y, x)$. Hence we have represented $\Bbbk^*$ as an algebraic group, which we call $G_m(\Bbbk)$.

Example 5.1.6. Another elementary example of an algebraic group is the affine algebraic set $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$ with the group operation $\text{mult}((x_1, y_1), (x_2, y_2)) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. (These formulae are analogous to the angle addition rules for sine and cosine as, over $\mathbb{R}$, one can identify (x, y) with $(\cos(\theta), \sin(\theta))$.) The reader should verify that the image of mult is contained in X. The identity element is $(1, 0)$ and the inverse of (x, y) is $(x, -y)$. One can verify that the axioms of a group are satisfied. This group is sometimes called the **circle group**.

Exercise 5.1.7. Let $p \equiv 3 \pmod 4$ be prime and define $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 = -1$. Show that the group $X(\mathbb{F}_p)$, where X is the circle group from Example 5.1.6, is isomorphic as a group to the subgroup $G \subseteq \mathbb{F}_{p^2}^*$ of order $p + 1$.

Proposition 5.1.8. *Let $S \subseteq \Bbbk[x_1, \ldots, x_n]$.*

1. *$V(S) = V((S))$ where (S) is the $\Bbbk[\underline{x}]$-ideal generated by S.*
2. *$V(\Bbbk[\underline{x}]) = \varnothing$ and $V(\{0\}) = \mathbb{A}^n$ where $\varnothing$ denotes the empty set.*
3. *If $S_1 \subseteq S_2$ then $V(S_2) \subseteq V(S_1)$.*
4. *$V(fg) = V(f) \cup V(g)$.*
5. *$V(f) \cap V(g) = V(f, g)$.*

Exercise 5.1.9. Prove Proposition 5.1.8.

Exercise 5.1.10. Show that $V(S)(\Bbbk) = \mathbb{A}^n(\Bbbk)$ does not necessarily imply that $S = \{0\}$.

The following result assumes a knowledge of Galois theory. See Section A.7 for background.

Lemma 5.1.11. *Let $X = V(S)$ be an algebraic set with $S \subseteq \Bbbk[\underline{x}]$ (i.e., X is a $\Bbbk$-algebraic set). Let $\Bbbk'$ be an algebraic extension of $\Bbbk$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk')$. For $P = (P_1, \ldots, P_n)$ define $\sigma(P) = (\sigma(P_1), \ldots, \sigma(P_n))$.*

1. *If $P \in X(\overline{\Bbbk})$ then $\sigma(P) \in X(\overline{\Bbbk})$.*
2. *$X(\Bbbk') = \{P \in X(\overline{\Bbbk}) : \sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk')\}$.*

Exercise 5.1.12. Prove Lemma 5.1.11.

Definition 5.1.13. The **ideal** over $\Bbbk$ of a set $X \subseteq \mathbb{A}^n(\overline{\Bbbk})$ is

$$I_{\Bbbk}(X) = \{f \in \Bbbk[\underline{x}] : f(P) = 0 \text{ for all } P \in X(\overline{\Bbbk})\}.$$

We define $I(X) = I_{\overline{\Bbbk}}(X)$.[1]

An algebraic set X is **defined over** $\Bbbk$ (sometimes abbreviated to "X over $\Bbbk$") if $I(X)$ can be generated by elements of $\Bbbk[\underline{x}]$.

Note that if X is an algebraic set defined over $\Bbbk$ then X is a $\Bbbk$-algebraic set. Perhaps surprisingly, it is not necessarily true that an algebraic set described by polynomials defined over $\Bbbk$ is an algebraic set defined over $\Bbbk$. In Remark 5.3.7 we will explain that these concepts are equivalent for the objects of interest in this book.

Exercise 5.1.14. Show that $I_{\Bbbk}(X) = I(X) \cap \Bbbk[\underline{x}]$.

The following example shows that $I_{\Bbbk}(X)$ is not necessarily the same as $I_{\Bbbk}(X(\Bbbk))$.

Example 5.1.15. Let $X = V(x^2 + y^2) \subset \mathbb{A}^2$ be an algebraic set over $\mathbb{R}$. Then $X(\mathbb{R}) = \{(0,0)\}$ while $X(\mathbb{C}) = \{(x, \pm ix) : x \in \mathbb{C}\}$. One has $I_{\mathbb{R}}(X) = (x^2 + y^2)$ where this denotes an $\mathbb{R}[x,y]$-ideal. Similarly, $I_{\mathbb{C}}(X)$ is the $\mathbb{C}[x,y]$-ideal $(x^2 + y^2)$. Indeed, $I_{\mathbb{C}}(X) = I_{\mathbb{R}}(X) \otimes_{\mathbb{R}} \mathbb{C}$. On the other hand, $I_{\mathbb{R}}(X(\mathbb{R}))$ is the $\mathbb{R}[x,y]$-ideal (x,y).

Proposition 5.1.16. *Let $X, Y \subseteq \mathbb{A}^n$ be sets and J a $\Bbbk[\underline{x}]$-ideal. Then*

1. *$I_{\Bbbk}(X)$ is a $\Bbbk[\underline{x}]$-ideal.*
2. *$X \subseteq V(I_{\Bbbk}(X))$.*
3. *If $X \subseteq Y$ then $I_{\Bbbk}(Y) \subseteq I_{\Bbbk}(X)$.*
4. *$I_{\Bbbk}(X \cup Y) = I_{\Bbbk}(X) \cap I_{\Bbbk}(Y)$.*
5. *If X is an algebraic set defined over $\Bbbk$ then $V(I_{\Bbbk}(X)) = X$.*
6. *If X and Y are algebraic sets defined over $\Bbbk$ and $I_{\Bbbk}(X) = I_{\Bbbk}(Y)$ then $X = Y$.*
7. *$J \subseteq I_{\Bbbk}(V(J))$.*
8. *$I_{\Bbbk}(\varnothing) = \Bbbk[\underline{x}]$.*

Exercise 5.1.17. Prove Proposition 5.1.16.

Definition 5.1.18. The **affine coordinate ring** over $\Bbbk$ of an affine algebraic set $X \subseteq \mathbb{A}^n$ defined over $\Bbbk$ is

$$\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/I_{\Bbbk}(X).$$

[1] The notation $I_{\Bbbk}(X)$ is not standard (Silverman [564] calls it $I(X/\Bbbk)$), but the notation $I(X)$ agrees with many elementary books on algebraic geometry, since they work over an algebraically closed field.

Warning: Here $\Bbbk[X]$ does not denote polynomials in the variable X. Hartshorne and Fulton write $A(X)$ and $\Gamma(X)$ respectively for the affine coordinate ring.

Exercise 5.1.19. Prove that $\Bbbk[X]$ is a commutative ring with an identity.

Note that $\Bbbk[X]$ is isomorphic to the ring of all functions $f : X \to \Bbbk$ given by polynomials defined over $\Bbbk$.

Hilbert's Nullstellensatz is a powerful tool for understanding $I_{\overline{\Bbbk}}(X)$ and it has several other applications (for example, we use it in Section 7.5). We follow the presentation of Fulton [216]. Note that it is necessary to work over $\overline{\Bbbk}$.

Theorem 5.1.20. *(Weak Nullstellensatz) Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set defined over $\overline{\Bbbk}$ and let $\mathfrak{m}$ be a maximal ideal of the affine coordinate ring $\overline{\Bbbk}[X]$. Then $V(\mathfrak{m}) = \{P\}$ for some $P = (P_1, \ldots, P_n) \in X(\overline{\Bbbk})$ and $\mathfrak{m} = (x_1 - P_1, \ldots, x_n - P_n)$.*

Proof: Consider the field $F = \overline{\Bbbk}[X]/\mathfrak{m}$, which contains $\overline{\Bbbk}$. Note that F is finitely generated as a ring over $\overline{\Bbbk}$ by the images of $x_1, \ldots, x_n$. By Theorem A.6.2, F is an algebraic extension of $\overline{\Bbbk}$ and so $F = \overline{\Bbbk}$.

It follows that, for $1 \leq i \leq n$, there is some $P_i \in \overline{\Bbbk}$ such that $x_i - P_i \in \mathfrak{m}$. Hence, $\mathfrak{n} = (x_1 - P_1, \ldots, x_n - P_n) \subseteq \mathfrak{m}$ and, since $\overline{\Bbbk}[X]/\mathfrak{n} = \overline{\Bbbk}$ it follows that $\mathfrak{m} = \mathfrak{n}$.

Finally, it is clear that $P \in V(\mathfrak{m})$ and if $Q = (Q_1, \ldots, Q_n) \in X(\overline{\Bbbk}) - \{P\}$ then there is some $1 \leq i \leq n$ such that $Q_i \neq P_i$ and so $(x - P_i)(Q_i) \neq 0$. Hence $V(\mathfrak{m}) = \{P\}$. □

Corollary 5.1.21. *If I is a proper ideal in $\overline{\Bbbk}[x_1, \ldots, x_n]$ then $V(I) \neq \varnothing$.*

Proof: There is some maximal ideal $\mathfrak{m}$ such that $I \subseteq \mathfrak{m}$. By Theorem 5.1.20, $\mathfrak{m} = (x_1 - P_1, \ldots, x_n - P_n)$ for some $P = (P_1, \ldots, P_n) \in \mathbb{A}^n(\overline{\Bbbk})$ and so $P \in V(I)$. □

Indeed, Corollary 5.1.21 is true when one starts with I a proper ideal in $\Bbbk[x_1, \ldots, x_n]$; see Lemma VIII.7.3 of [301].

We can now state the **Hilbert Nullstellensatz**. This form of the theorem (which applies to $I_{\Bbbk}(V(I))$ where $\Bbbk$ is not necessarily algebraically closed), appears as Proposition VIII.7.4 of [301].

Theorem 5.1.22. *Let I be an ideal in $R = \Bbbk[x_1, \ldots, x_n]$. Then $I_{\Bbbk}(V(I)) = \mathrm{rad}_R(I)$ (see Section A.9 for the definition of the radical ideal).*

Proof: One has $\mathrm{rad}_R(I) \subseteq I_{\Bbbk}(V(I))$ since $f^n \in I$ implies $f^n(P) = 0$ for all $P \in V(I)$ and so $f(P) = 0$ for all $P \in V(I)$. For the converse suppose $I = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n))$ and $G(x_1, \ldots, x_n) \in I_{\Bbbk}(V(I))$. Define the $\Bbbk[x_1, \ldots, x_{n+1}]$-ideal

$$J = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n), x_{n+1}G(x_1, \ldots, x_n) - 1).$$

Then $V(J) = \varnothing$ since if $P = (P_1, \ldots, P_{n+1}) \in \mathbb{A}^{n+1}(\overline{\Bbbk})$ is such that $F_i(P_1, \ldots, P_n) = 0$ for all $1 \leq i \leq m$ then $G(P_1, \ldots, P_n) = 0$ too and so one does not have $P_{n+1}G(P) = 1$. It follows from (the stronger form of) Corollary 5.1.21 that $J = (1)$ and so $1 \in J$. In other words, there are polynomials $a_i(x_1, \ldots, x_{n+1}) \in \Bbbk[x_1, \ldots, x_{n+1}]$ for $1 \leq i \leq m+1$ such that

$$1 = a_{m+1}(x_{n+1}G - 1) + \sum_{i=1}^{m} a_i F_i.$$

Write $y = 1/x_{n+1}$ and let $N = 1 + \max_{1 \leq i \leq m+1}\{\deg_{x_{n+1}}(a_i)\}$. One has

$$y^N = b_{m+1}(x_1, \ldots, x_n, y)(G - y) + \sum_{i=1}^{m} b_i(x_1, \ldots, x_n, y)F_i(x_1, \ldots, x_n)$$

for some polynomials $b_i \in \Bbbk[x_1, \ldots, x_n, y]$. Setting $y = G$ proves that $G^N \in I$ and so $G \in \mathrm{rad}_R(I)$. □

Corollary 5.1.23. *Let $f(x,y) \in \Bbbk[x,y]$ be irreducible over $\overline{\Bbbk}$ and let $X = V(f(x,y)) \subset \mathbb{A}^2(\overline{\Bbbk})$. Then $I(X) = (f(x,y))$, i.e., the ideal over $\overline{\Bbbk}[x,y]$ generated by $f(x,y)$.*

Proof: By Theorem 5.1.22 we have $I(X) = \mathrm{rad}_{\overline{\Bbbk}}((f(x,y)))$. Since $\overline{\Bbbk}[x,y]$ is a unique factorisation domain and $f(x,y)$ is irreducible, then $f(x,y)$ is prime. So $g(x,y) \in \mathrm{rad}_{\overline{\Bbbk}}((f(x,y)))$ implies $g(x,y)^n = f(x,y)h(x,y)$ for some $h(x,y) \in \overline{\Bbbk}[x,y]$ which implies $f(x,y) \mid g(x,y)$ and $g(x,y) \in (f(x,y))$. □

Theorem 5.1.24. *Every affine algebraic set X is the intersection of a finite number of hypersurfaces.*

Proof: By Hilbert's basis theorem (Corollary A.9.4) $\Bbbk[\underline{x}]$ is Noetherian. Hence $I_{\Bbbk}(X) = (f_1, \ldots, f_m)$ and $X = V(f_1) \cap \cdots \cap V(f_m)$. □

5.2 Projective Algebraic Sets

Studying affine algebraic sets is not sufficient for our applications. In particular, the set of affine points of the Weierstrass equation of an elliptic curve (see Section 7.2) does not form a group. Projective geometry is a way to "complete" the picture by adding certain "points at infinity".

For example, consider the hyperbola $xy = 1$ in $\mathbb{A}^2(\mathbb{R})$. Projective geometry allows an interpretation of the behaviour of the curve at $x = 0$ or $y = 0$; see Example 5.2.7.

Definition 5.2.1. Projective space over $\Bbbk$ of dimension n is

$$\mathbb{P}^n(\Bbbk) = \{\text{lines through } (0, \ldots, 0) \text{ in } \mathbb{A}^{n+1}(\Bbbk)\}.$$

A convenient way to represent points of $\mathbb{P}^n(\Bbbk)$ is using **homogeneous coordinates**: Let $a_0, a_1, \ldots, a_n \in \Bbbk$ with not all $a_j = 0$ and define $(a_0 : a_1 : \cdots : a_n)$ to be the equivalence class of $(n+1)$-tuples under the equivalence relation

$$(a_0, a_1, \cdots, a_n) \equiv (\lambda a_0, \lambda a_1, \cdots, \lambda a_n)$$

for any $\lambda \in \Bbbk^*$. Thus $\mathbb{P}^n(\Bbbk) = \{(a_0 : \cdots : a_n) : a_i \in \Bbbk \text{ for } 0 \leq i \leq n \text{ and } a_i \neq 0 \text{ for some } 0 \leq i \leq n\}$. Write $\mathbb{P}^n = \mathbb{P}^n(\overline{\Bbbk})$.

In other words, the equivalence class $(a_0 : \cdots : a_n)$ is the set of points on the line between $(0, \ldots, 0)$ and $(a_0, \ldots, a_n)$ with the point $(0, \ldots, 0)$ removed.

There is a map $\varphi : \mathbb{A}^n \to \mathbb{P}^n$ given by $\varphi(x_1, \ldots, x_n) = (x_1 : \cdots : x_n : 1)$. Hence $\mathbb{A}^n$ is identified with a subset of $\mathbb{P}^n$.

Example 5.2.2. The **projective line** $\mathbb{P}^1(\Bbbk)$ is in one-to-one correspondence with $\mathbb{A}^1(\Bbbk) \cup \{\infty\}$ since $\mathbb{P}^1(\Bbbk) = \{(a_0 : 1) : a_0 \in \Bbbk\} \cup \{(1 : 0)\}$. The **projective plane** $\mathbb{P}^2(\Bbbk)$ is in one-to-one correspondence with $\mathbb{A}^2(\Bbbk) \cup \mathbb{P}^1(\Bbbk)$.

Definition 5.2.3. A point $P = (P_0 : P_1 : \cdots : P_n) \in \mathbb{P}^n(\overline{\Bbbk})$ is **defined over** $\Bbbk$ if there is some $\lambda \in \overline{\Bbbk}^*$ such that $\lambda P_j \in \Bbbk$ for all $0 \leq j \leq n$. If $P \in \mathbb{P}^n$ and $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then $\sigma(P) = (\sigma(P_0) : \cdots : \sigma(P_n))$.

Exercise 5.2.4. Show that P is defined over $\Bbbk$ if and only if there is some $0 \leq i \leq n$ such that $P_i \neq 0$ and $P_j/P_i \in \Bbbk$ for all $0 \leq j \leq n$. Show that $\mathbb{P}^n(\Bbbk)$ is equal to the set of points $P \in \mathbb{P}^n(\overline{\Bbbk})$ that are defined over $\Bbbk$. Show that $\sigma(P)$ in Definition 5.2.3 is well-defined (i.e., if $P = (P_0, \ldots, P_n) \equiv P' = (P'_0, \ldots, P'_n)$ then $\sigma(P) \equiv \sigma(P')$).

Lemma 5.2.5. *A point $P \in \mathbb{P}^n(\overline{\Bbbk})$ is defined over $\Bbbk$ if and only if $\sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$.*

Proof: Let $P = (P_0 : \cdots : P_n) \in \mathbb{P}^n(\overline{\Bbbk})$ and suppose $\sigma(P) \equiv P$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then there is some $\xi : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ such that $\sigma(P_i) = \xi(\sigma)P_i$ for all $0 \leq i \leq n$. One can verify[2] that ξ is a 1-cocycle in $\overline{\Bbbk}^*$. It follows by Theorem A.7.2 (Hilbert 90) that $\xi(\sigma) = \sigma(\gamma)/\gamma$ for some $\gamma \in \overline{\Bbbk}^*$. Hence, $\sigma(P_i/\gamma) = P_i/\gamma$ for all $0 \leq i \leq n$ and all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Hence $P_i/\gamma \in \Bbbk$ for all $0 \leq i \leq n$ and the proof is complete. □

Recall that if f is a homogeneous polynomial of degree d then $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in \Bbbk$ and all $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}(\Bbbk)$.

Definition 5.2.6. Let $f \in \Bbbk[x_0, \ldots, x_n]$ be a homogeneous polynomial. A point $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\Bbbk)$ is a **zero** of f if $f(x_0, \ldots, x_n) = 0$ for some (hence, every) point $(x_0, \ldots, x_n)$ in the equivalence class $(x_0 : \cdots : x_n)$. We therefore write $f(P) = 0$. Let S be a set of polynomials and define

$$V(S) = \{P \in \mathbb{P}^n(\overline{\Bbbk}) : P \text{ is a zero of } f(\underline{x}) \text{ for all homogeneous } f(\underline{x}) \in S\}.$$

A **projective algebraic set** is a set $X = V(S) \subseteq \mathbb{P}^n(\overline{\Bbbk})$ for some $S \subseteq \Bbbk[\underline{x}]$. Such a set is also called a projective $\Bbbk$-algebraic set. For $X = V(S)$ and $\Bbbk'$ an algebraic extension of $\Bbbk$ define

$$X(\Bbbk') = \{P \in \mathbb{P}^n(\Bbbk') : f(P) = 0 \text{ for all homogeneous } f(\underline{x}) \in S\}.$$

Example 5.2.7. The hyperbola $y = 1/x$ can be described as the affine algebraic set $X = V(xy-1) \subset \mathbb{A}^2$ over $\mathbb{R}$. One can consider the corresponding projective algebraic set $V(xy - z^2) \subseteq \mathbb{P}^2$ over $\mathbb{R}$ whose points consist the points of X together with the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$. These two points correspond to the asymptotes $x = 0$ and $y = 0$ of the hyperbola and they essentially "tie together" the disconnected components of the affine curve to make a single closed curve in projective space.

Exercise 5.2.8. Describe the sets $V(x^2+y^2-z^2)(\mathbb{R}) \subset \mathbb{P}^2(\mathbb{R})$ and $V(yz-x^2)(\mathbb{R}) \subseteq \mathbb{P}^2(\mathbb{R})$.

Exercise 5.2.9. What is $V(xz + y^2, xyz) \subseteq \mathbb{P}^2(\mathbb{C})$?

Exercise 5.2.10. What is $V(y^2 + x^2, x^2z - y^3) \subseteq \mathbb{P}^2(\mathbb{C})$?

A set of homogeneous polynomials does not in general form an ideal as one cannot simultaneously have closure under multiplication and addition. Hence it is necessary to introduce the following definition.

Definition 5.2.11. A $\Bbbk[x_0, \ldots, x_n]$-ideal $I \subseteq \Bbbk[x_0, \ldots, x_n]$ is a **homogeneous ideal** if for every $f \in I$ with homogeneous decomposition $f = \sum_i f_i$ we have $f_i \in I$.

Exercise 5.2.12. Let $S \subset \Bbbk[\underline{x}]$ be a set of homogeneous polynomials. Define (S) to be the $\Bbbk[\underline{x}]$-ideal generated by S in the usual way, i.e., $(S) = \{\sum_{j=1}^n f_j(\underline{x})s_j(\underline{x}) : n \in \mathbb{N}, f_j(\underline{x}) \in \Bbbk[x_0, \ldots, x_n], s_j(\underline{x}) \in S\}$. Prove that (S) is a homogeneous ideal. Prove that if I is a homogeneous ideal then $I = (S)$ for some set of homogeneous polynomials S.

Definition 5.2.13. For any set $X \subseteq \mathbb{P}^n(\overline{\Bbbk})$ define

$$I_{\Bbbk}(X) = \big(\{f \in \Bbbk[x_0, \ldots, x_n] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in X\}\big).$$

[2] At least, one can verify the formula $\xi(\sigma\tau) = \sigma(\xi(\tau))\xi(\sigma)$. The topological condition also holds, but we do not discuss this.

We stress that $I_{\Bbbk}(X)$ is not the stated set of homogeneous polynomials but the ideal generated by them. We write $I(X) = I_{\overline{\Bbbk}}(X)$.

An algebraic set $X \subseteq \mathbb{P}^n$ is **defined over** $\Bbbk$ if $I(X)$ can be generated by homogeneous polynomials in $\Bbbk[\underline{x}]$.

Proposition 5.2.14. *Let $\Bbbk$ be a field.*

1. *If $S_1 \subseteq S_2 \subseteq \Bbbk[x_0, \ldots, x_n]$ then $V(S_2) \subseteq V(S_1) \subseteq \mathbb{P}^n(\overline{\Bbbk})$.*
2. *If fg is a homogeneous polynomial then $V(fg) = V(f) \cup V(g)$ (recall from Lemma A.5.4 that f and g are both homogeneous).*
3. *$V(f) \cap V(g) = V(f, g)$.*
4. *If $X_1 \subseteq X_2 \subseteq \mathbb{P}^n(\Bbbk)$ then $I_{\Bbbk}(X_2) \subseteq I_{\Bbbk}(X_1) \subseteq \Bbbk[x_0, \ldots, x_n]$.*
5. *$I_{\Bbbk}(X_1 \cup X_2) = I_{\Bbbk}(X_1) \cap I_{\Bbbk}(X_2)$.*
6. *If J is a homogeneous ideal then $J \subseteq I_{\Bbbk}(V(J))$.*
7. *If X is a projective algebraic set defined over $\Bbbk$ then $V(I_{\Bbbk}(X)) = X$. If Y is another projective algebraic set defined over $\Bbbk$ and $I_{\Bbbk}(Y) = I_{\Bbbk}(X)$ then $Y = X$.*

Exercise 5.2.15. Prove Proposition 5.2.14.

Definition 5.2.16. If X is a projective algebraic set defined over $\Bbbk$ then the **homogenous coordinate ring** of X over $\Bbbk$ is $\Bbbk[X] = \Bbbk[x_0, \ldots, x_n]/I_{\Bbbk}(X)$.

Note that elements of $\Bbbk[X]$ are not necessarily homogeneous polynomials.

Definition 5.2.17. Let X be an algebraic set in $\mathbb{A}^n$ (respectively, $\mathbb{P}^n$) The **Zariski topology** is the topology on X defined as follows: The closed sets are $X \cap Y$ for every algebraic set $Y \subseteq \mathbb{A}^n$ (respectively, $Y \subseteq \mathbb{P}^n$).

Exercise 5.2.18. Show that the Zariski topology satisfies the axioms of a topology.

Definition 5.2.19. For $0 \leq i \leq n$ define $U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n : x_i \neq 0\} = \mathbb{P}^n - V(x_i)$. (These are open sets in the Zariski topology.)

Exercise 5.2.20. Show that $\mathbb{P}^n = \cup_{i=0}^n U_i$ (not a disjoint union).

Exercise 5.2.21. What points of $\mathbb{P}^2(\Bbbk)$ do not lie in two of the three sets $U_0(\Bbbk), U_1(\Bbbk), U_2(\Bbbk)$?

Definition. Let $L \in \mathrm{GL}_{n+1}(\Bbbk)$ (i.e., L is an $(n+1) \times (n+1)$ matrix over $\Bbbk$ that is invertible). The map $L : \mathbb{P}^n \to \mathbb{P}^n$ given by

$$L(x_0 : \cdots : x_n) = (L_{0,0}x_0 + \cdots + L_{0,n}x_n : \cdots : L_{n,0}x_0 + \cdots + L_{n,n}x_n)$$

is called a **linear change of variables** on $\mathbb{P}^n$ over $\Bbbk$. The inverse change of variables is given by L^{-1}.

Example 5.2.22. The matrix

$$L = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

gives a linear change of variables $L : \mathbb{P}^2 \to \mathbb{P}^2$ of the form $L(x_0 : x_1 : x_2) = (y_0 : y_1 : y_2) = (x_0 - x_1 : x_1 : x_2)$. This maps the algebraic set $X = V(x_0^2 - x_1^2 + x_1x_2)$ to $Y = V(y_0^2 + 2y_0y_1 + y_1y_2)$. In other words, if $P \in X(\Bbbk)$ then $L(P) \in Y(\Bbbk)$.

A linear change of variable does not change the underlying geometry of an algebraic set, but can be useful for practical computation. For instance, sometimes we will use Exercise 5.2.23 to reduce any pair of points to affine space without changing the "shape" of the algebraic set.

Exercise 5.2.23. Show that if $P, Q \in \mathbb{P}^n(\Bbbk)$ then there is always a linear change of variables L on $\mathbb{P}^n$ over $\Bbbk$ such that $L(P), L(Q) \in U_n$.

We already mentioned the map $\varphi : \mathbb{A}^n \to \mathbb{P}^n$ given by $\varphi(x_1, \ldots, x_n) = (x_1 : \cdots : x_n : 1)$, which has image equal to U_n. A useful way to study a projective algebraic set X is to consider $X \cap U_i$ for $0 \leq i \leq n$ and interpret $X \cap U_i$ as an affine algebraic set. We now introduce the notation for this.

Definition 5.2.24. Let $\varphi_i : \mathbb{A}^n(\Bbbk) \to U_i$ be the one-to-one correspondence

$$\varphi_i(y_1, \ldots, y_n) = (y_1 : \cdots : y_i : 1 : y_{i+1} : \cdots : y_n).$$

We write φ for φ_n. Let

$$\varphi_i^{-1}(x_0 : \cdots : x_n) = (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i).$$

be the map $\varphi_i^{-1} : \mathbb{P}^n(\Bbbk) \to \mathbb{A}^n(\Bbbk)$, which is defined only on U_i (i.e., $\varphi_i^{-1}(X) = \varphi_i^{-1}(X \cap U_i)$).[3]

We write $X \cap \mathbb{A}^n$ as an abbreviation for $\varphi_n^{-1}(X \cap U_n)$.

Let $\varphi_i^* : \Bbbk[x_0, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$ be the **de-homogenisation** map[4]

$$\varphi_i^*(f)(y_1, \ldots, y_n) = f \circ \varphi_i(y_1, \ldots, y_n) = f(y_1, \ldots, y_i, 1, y_{i+1}, \ldots, y_n).$$

We write φ^* for φ_n^*.

Let $\varphi_i^{-1*} : \Bbbk[y_1, \ldots, y_n] \to \Bbbk[x_0, \ldots, x_n]$ be the **homogenisation**

$$\varphi_i^{-1*}(f)(x_0, \ldots, x_n) = x_i^{\deg(f)} f(x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)$$

where $\deg(f)$ is the total degree.

We write $\overline{f}$ as an abbreviation for $\varphi_n^{-1*}(f)$. For notational simplicity we often consider polynomials $f(x, y)$; in this case we define $\overline{f} = z^{\deg(f)} f(x/z, y/z)$.

We now state some elementary relations between projective algebraic sets X and their affine parts $X \cap U_i$.

Lemma 5.2.25. *Let the notation be as above.*

1. *$\varphi_i^* : \Bbbk[x_0, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$ is a $\Bbbk$-algebra homomorphism. The map $\varphi_i^{-1*} : \Bbbk[y_1, \ldots, y_n] \to \Bbbk[x_0, \ldots, x_n]$ satisfies most of the properties of a $\Bbbk$-algebra homomorphism, except that $\varphi_i^{-1*}(f+g) = \varphi_i^{-1*}(f) + \varphi_i^{-1*}(g)$ if and only if f and g have the same total degree.*
2. *Let $P = (P_0 : \cdots : P_n) \in \mathbb{P}^n(\Bbbk)$ with $P_i \neq 0$ and let $f \in \Bbbk[x_0, \ldots, x_n]$ be homogeneous. Then $f(P) = 0$ implies $\varphi_i^*(f)(\varphi_i^{-1}(P)) = 0$.*
3. *Let $f \in \Bbbk[x_0, \ldots, x_n]$ be homogeneous. Then $\varphi_i^{-1}(V(f)) = V(\varphi_i^*(f))$. In particular, $V(f) \cap \mathbb{A}^n = V(f \circ \varphi)$.*

[3] This notation does not seem to be standard. Our notation agrees with Silverman [564], but Hartshorne [278] has φ_i and φ_i^{-1} the other way around.

[4] The upper star notation is extended in Definition 5.5.23.

4. *Let $X \subseteq \mathbb{P}^n(\Bbbk)$. Then $f \in I_{\Bbbk}(X)$ implies $\varphi_i^*(f) \in I_{\Bbbk}(\varphi_i^{-1}(X))$. In particular, $f \in I_{\Bbbk}(X)$ implies $f \circ \varphi \in I_{\Bbbk}(X \cap \mathbb{A}^n)$.*
5. *If $P \in \mathbb{A}^n(\Bbbk)$ and $f \in \Bbbk[y_1, \ldots, y_n]$ then $f(P) = 0$ implies $\varphi_i^{-1*}(f)(\varphi_i(P)) = 0$. In particular, $f(P) = 0$ implies $\overline{f}(\varphi(P)) = 0$.*
6. *For homogeneous $f \in \Bbbk[x_0, \ldots, x_n]$ then $\varphi_i^{-1*}(\varphi_i^*(f)) \mid f$. Furthermore, if f has a monomial that does not include x_i then $\varphi_i^{-1*}(\varphi_i^*(f)) = f$ (in particular, $\overline{f \circ \varphi} = f$).*

Exercise 5.2.26. Prove Lemma 5.2.25.

Definition 5.2.27. Let $I \subseteq \Bbbk[y_1, \ldots, y_n]$. Define the **homogenisation** $\overline{I}$ to be the $\Bbbk[x_0, \ldots, x_n]$-ideal generated by the set $\{\overline{f}(x_0, \ldots, x_n) : f \in I\}$.

Exercise 5.2.28. Let $I \subseteq \Bbbk[y_1, \ldots, y_n]$. Show that $\overline{I}$ is a homogeneous ideal.

Definition 5.2.29. Let $X \subseteq \mathbb{A}^n(\overline{\Bbbk})$. Define the **projective closure** of X to be $\overline{X} = V\left(\overline{I(X)}\right) \subseteq \mathbb{P}^n$.

Lemma 5.2.30. *Let the notation be as above.*

1. *Let $X \subseteq \mathbb{A}^n$, then $\varphi(X) \subseteq \overline{X}$ and $\overline{X} \cap \mathbb{A}^n = X$.*
2. *Let $X \subseteq \mathbb{A}^n(\overline{\Bbbk})$ be non-empty. Then $I_{\Bbbk}\left(\overline{X}\right) = \overline{I_{\Bbbk}(X)}$.*

Proof: Part 1 follows directly from the definitions.

Part 2 is essentially that the homogenisation of a radical ideal is a radical ideal, we give a direct proof. Let $f \in \Bbbk[x_0, \ldots, x_n]$ be such that f is homogeneous and $f(\overline{X}) = 0$. Write $f = x_0^d g$ where $g \in \Bbbk[x_0, \ldots, x_n]$ has a monomial that does not include x_0. By part 1 and $X \neq \varnothing$, g is not constant. Then $g \circ \varphi \in I_{\Bbbk}(X)$ and so $g = \overline{g \circ \varphi} \in \overline{I_{\Bbbk}(X)}$. It follows from part 6 of Lemma 5.2.25 that $f \in \overline{I_{\Bbbk}(X)}$. Hence, $I_{\Bbbk}(\overline{X}) \subseteq \overline{I_{\Bbbk}(X)}$ and the result follows. □

Theorem 5.2.31. *Let $f(x_0, x_1, x_2) \in \Bbbk[x_0, x_1, x_2]$ be a $\overline{\Bbbk}$-irreducible homogeneous polynomial. Let*

$$X = V(f(x_0, x_1, x_2)) \subseteq \mathbb{P}^2.$$

Then $I_{\overline{\Bbbk}}(X) = (f(x_0, x_1, x_2))$.

Proof: Let $0 \leq i \leq 2$ be such that $f(x_0, x_1, x_2)$ has a monomial that does not feature x_i (such an i must exist since f is irreducible). Without loss of generality, suppose $i = 2$. Write $g(y_1, y_2) = \varphi^*(f) = f(y_1, y_2, 1)$. By part 6 of Lemma 5.2.25 the homogenisation of g is f.

Let $Y = X \cap \mathbb{A}^2 = V(g)$. Note that g is $\overline{\Bbbk}$-irreducible (since $g = g_1 g_2$ implies, by taking homogenisation, $f = \overline{g_1}\ \overline{g_2}$). Let $h \in I_{\overline{\Bbbk}}(X)$ then $h \circ \varphi \in I_{\overline{\Bbbk}}(Y)$ and so, by Corollary 5.1.23, $h \circ \varphi \in (g)$. In other words, there is some $h_1(y_1, y_2)$ such that $h \circ \varphi = g h_1$. Taking homogenisations gives $f \mid \overline{h_1}$ and so $h \in (f)$. □

Corollary 5.2.32. *Let $f(x, y) \in \Bbbk[x, y]$ be a $\overline{\Bbbk}$-irreducible polynomial and let $X = V(f) \subseteq \mathbb{A}^2$. Then $\overline{X} = V(\overline{f}) \subseteq \mathbb{P}^2$.*

Exercise 5.2.33. Prove Corollary 5.2.32.

Example 5.2.34. The projective closure of $V(y^2 = x^3 + Ax + B) \subseteq \mathbb{A}^n$ is $V(y^2 z = x^3 + Axz^2 + Bz^3)$.

Exercise 5.2.35. Let $X = V(f(x_0, x_1)) \subseteq \mathbb{A}^2$ and let $\overline{X} \subseteq \mathbb{P}^2$ be the projective closure of X. Show that $\overline{X} - X$ is finite (in other words, there are only finitely many points at infinity).

A generalisation of projective space, called **weighted projective space**, is defined as follows: For $i_0, \ldots, i_n \in \mathbb{N}$ denote by $(a_0 : a_1 : \cdots : a_n)$ the equivalence class of elements in $\mathbb{k}^{n+1}$ under the equivalence relation

$$(a_0, a_1, \cdots, a_n) \equiv (\lambda^{i_0} a_0, \lambda^{i_1} a_1, \cdots, \lambda^{i_n} a_n)$$

for any $\lambda \in \mathbb{k}^*$. The set of equivalence classes is denoted $\mathbb{P}(i_0, \ldots, i_n)(\mathbb{k})$. For example, it makes sense to consider the curve $y^2 = x^4 + ax^2z^2 + z^4$ as lying in $\mathbb{P}(1, 2, 1)$. We will not discuss this topic further in the book (we refer to Reid [498] for details), but it should be noted that certain coordinate systems used for efficient elliptic curve cryptography naturally live in weighted projective space.

5.3 Irreducibility

We have seen that $V(fg)$ decomposes as $V(f) \cup V(g)$ and it is natural to consider $V(f)$ and $V(g)$ as being 'components' of $V(fg)$. It is easier to deal with algebraic sets that cannot be decomposed in this way. This concept is most useful when working over an algebraically closed field, but we give some of the theory in greater generality.

Definition 5.3.1. An affine $\mathbb{k}$-algebraic set $X \subseteq \mathbb{A}^n$ is $\mathbb{k}$-**reducible** if $X = X_1 \cup X_2$ with X_1 and X_2 being $\mathbb{k}$-algebraic sets and $X_i \neq X$ for $i = 1, 2$. An affine algebraic set is $\mathbb{k}$-**irreducible** if there is no such decomposition. An affine algebraic set is **geometrically irreducible** if X is $\overline{\mathbb{k}}$-irreducible. An **affine variety** over $\mathbb{k}$ is a geometrically irreducible $\mathbb{k}$-algebraic set defined over $\mathbb{k}$.

A projective $\mathbb{k}$-algebraic set $X \subseteq \mathbb{P}^n$ is $\mathbb{k}$-**irreducible** (resp. **geometrically irreducible**) if X is not the union $X_1 \cup X_2$ of projective $\mathbb{k}$-algebraic sets $X_1, X_2 \subseteq \mathbb{P}^n$ (respectively, projective $\overline{\mathbb{k}}$-algebraic sets) such that $X_i \neq X$ for $i = 1, 2$. A **projective variety** over $\mathbb{k}$ is a geometrically irreducible projective $\mathbb{k}$-algebraic set defined over $\mathbb{k}$.

Let X be a variety (affine or projective). A **subvariety** of X over $\mathbb{k}$ is a subset $Y \subseteq X$ that is a variety (affine or projective) defined over $\mathbb{k}$.

This definition matches the usual topological definition of a set being irreducible if it is not a union of proper closed subsets.

Example 5.3.2. The algebraic set $X = V(x^2 + y^2) \subseteq \mathbb{A}^2$ over $\mathbb{R}$ is $\mathbb{R}$-irreducible. However, over $\mathbb{C}$ we have $X = V(x + iy) \cup V(x - iy)$ and so X is $\mathbb{C}$-reducible.

Exercise 5.3.3. Show that $X = V(wx - yz, x^2 - yz) \subseteq \mathbb{P}^3$ is not irreducible.

It is often easy to determine that a reducible algebraic set is reducible, just by exhibiting the non-trivial union. However, it is not necessarily easy to show that an irreducible algebraic set is irreducible. We now give an algebraic criterion for irreducibility and some applications of this result.

Theorem 5.3.4. *Let X be an algebraic set (affine or projective). Then X is $\mathbb{k}$-irreducible if and only if $I_{\mathbb{k}}(X)$ is a prime ideal.*

Proof: ($\Rightarrow$): Suppose $X = V(S)$ where $S \subseteq \mathbb{k}[\underline{x}]$ is $\mathbb{k}$-irreducible and that there are elements $f, g \in \mathbb{k}[\underline{x}]$ such that $fg \in I_{\mathbb{k}}(X)$. Then $X \subseteq V(fg) = V(f) \cup V(g)$, so $X = (X \cap V(f)) \cup (X \cap V(g))$. Since $X \cap V(f) = V(S, f)$ and $X \cap V(g) = V(S, g)$ are $\mathbb{k}$-algebraic sets it follows that either $X = X \cap V(f)$ or $X = X \cap V(g)$, and so $f \in I_{\mathbb{k}}(X)$ or $g \in I_{\mathbb{k}}(X)$.

($\Leftarrow$): Suppose $I = I_{\mathbb{k}}(X)$ is a prime ideal and that $X = X_1 \cup X_2$ where X_1 and X_2 are $\mathbb{k}$-algebraic sets. Let $I_1 = I_{\mathbb{k}}(X_1)$ and $I_2 = I_{\mathbb{k}}(X_2)$. By parts 3 and 4 of Proposition 5.1.16

or parts 4 and 5 of Proposition 5.2.14 we have $I \subseteq I_1$, $I \subseteq I_2$ and $I = I_1 \cap I_2$. Since $I_1 I_2 \subseteq I_1 \cap I_2 = I$ and I is a prime ideal, it follows that either $I_1 \subseteq I$ or $I_2 \subseteq I$. Hence either $I = I_1$ or $I = I_2$ and so, by part 6 of Proposition 5.1.16 or part 7 of Proposition 5.2.14, $X = X_1$ or $X = X_2$. □

Exercise 5.3.5. Show that $V(y - x^2)$ is irreducible in $\mathbb{A}^2(\Bbbk)$.

Exercise 5.3.6. Let $X \subset \mathbb{A}^n$ be an algebraic set over $\Bbbk$. Suppose there exist polynomials $f_1, \ldots, f_n \in \Bbbk[t]$ such that $X = \{(f_1(t), f_2(t), \ldots, f_n(t)) : t \in \overline{\Bbbk}\}$. Prove that X is geometrically irreducible.

Remark 5.3.7. A $\Bbbk$-algebraic set X is the vanishing of polynomials in $\Bbbk[x_1, \ldots, x_n]$. However, we say X is defined over $\Bbbk$ if $I_{\overline{\Bbbk}}(X)$ is generated by polynomials in $\Bbbk[x_1, \ldots, x_n]$. Hence, it is clear that an algebraic set defined over $\Bbbk$ is a $\Bbbk$-algebraic set. The converse does not hold in general. However, if X is absolutely irreducible and $\Bbbk$ is a perfect field then these notions are equivalent (see Corollary 10.2.2 of Fried and Jarden [214] and use the fact that when X is absolutely irreducible then the algebraic closure of $\Bbbk$ in $\Bbbk(X)$ is $\Bbbk$). Note that Corollary 5.1.23 proves a special case of this result.

The next few results use the notation of Definitions 5.2.24, 5.2.27 and 5.2.29.

Corollary 5.3.8. *Let $X \subseteq \mathbb{A}^n$ be a variety. Then $\overline{X}$ is geometrically irreducible. Let $X \subseteq \mathbb{P}^n$ be a variety. Then $X \cap \mathbb{A}^n$ is geometrically irreducible.*

Proof: The case where X is empty is trivial so suppose $X \neq \varnothing$. By Lemma 5.2.30, $I\left(\overline{X}\right) = \overline{I(X)}$. Hence, if $g, h \in \Bbbk[x_0, \ldots, x_n]$ are such that $gh \in I\left(\overline{X}\right)$ then $(g \circ \varphi)(h \circ \varphi) = (gh) \circ \varphi \in I(X)$ by part 4 of Lemma 5.2.25. Theorem 5.3.4 implies $I(X)$ is a prime ideal and so either $g \circ \varphi$ or $h \circ \varphi$ is in $I(X)$. Hence either g or h is in $I\left(\overline{X}\right)$.

For the converse, suppose $X \cap \mathbb{A}^n \neq \varnothing$. If $gh \in I(X \cap \mathbb{A}^n)$ then $\overline{g}\,\overline{h} = \overline{gh} \in \overline{I(X \cap \mathbb{A}^n)} \subseteq I(X)$. Hence $\overline{g}$ or $\overline{h}$ is in $I(X)$ and so, by part 4 of Lemma 5.2.25, g or h is in $I(X \cap \mathbb{A}^n)$. □

Theorem 5.3.9. *Let $X \subseteq \mathbb{P}^n$ be an algebraic set such that $X \cap \mathbb{A}^n \neq \varnothing$. Then $\overline{X \cap \mathbb{A}^n} \subseteq X$. If X is a variety then $\overline{X \cap \mathbb{A}^n} = X$.*

Proof: If $f \in I(X)$ then $f \circ \varphi \in I(X \cap \mathbb{A}^n)$ and so $\overline{f \circ \varphi} \in \overline{I(X \cap \mathbb{A}^n)}$. Hence, $f \in \overline{I(X \cap \mathbb{A}^n)}$. In other words, $I(X) \subseteq I\left(\overline{X \cap \mathbb{A}^n}\right)$ and so $\overline{X \cap \mathbb{A}^n} \subseteq X$.

Let $X_1 = \overline{X \cap \mathbb{A}^n} \subseteq X$ and $X_2 = X \cap V(x_0)$. Then $X = X_1 \cup X_2$ and so, if X is irreducible and $X \cap \mathbb{A}^n \neq \varnothing$ then $X = X_1$. □

Theorem 5.3.10. *Let $\Bbbk$ be a field and let $f(x, y) \in \Bbbk[x, y]$ (or $f(x, y, z) \in \Bbbk[x, y, z]$ homogeneous) have no repeated factors over $\overline{\Bbbk}$. Let $X = V(f(x, y)) \subset \mathbb{A}^2(\Bbbk)$ or $X = V(f(x, y, z)) \subseteq \mathbb{P}^2(\Bbbk)$. Then X is geometrically irreducible if and only if f is irreducible over $\overline{\Bbbk}$.*

Proof: Suppose $X = V(f)$ is geometrically irreducible but that $f = gh$ is a factorization in $\overline{\Bbbk}[x, y]$ or $\overline{\Bbbk}[x, y, z]$ with both g and h having degree ≥ 1. Since f has no repeated factors we have that g and h have no irreducible factors in common. Now, $V(f) = V(gh) = V(g) \cup V(h)$. Since $V(f)$ is irreducible either $V(g) = V(f)$ or $V(h) = V(f)$. Without loss of generality we may assume $V(g) = V(f)$. By Hilbert's Nullstellensatz (Theorem 5.1.22) it follows that $g^m \in \langle f \rangle$ for some integer m, which means that $f \mid g^m$. Now, let q be an irreducible factor of h. Then $q \mid f$ and so $q \mid g^m$ and so $q \mid g$. But g and h are supposed to have no common irreducible factors, so this is a contradiction. Hence, if X is geometrically irreducible then f is $\overline{\Bbbk}$-irreducible.

Conversely, by Corollary 5.1.23 (respectively, Theorem 5.2.31) we have $I_{\overline{\Bbbk}}(V(f)) = (f)$. Since f is irreducible it follows that (f) is a prime ideal and so X is irreducible. □

Example 5.3.11. It is necessary to work over $\overline{\Bbbk}$ for Theorem 5.3.10. For example, let $f(x,y) = y^2 + x^2(x-1)^2$. Then $V(f(x,y)) \subseteq \mathbb{A}^2(\mathbb{R})$ consists of two points and so is reducible, even though $f(x,y)$ is $\mathbb{R}$-irreducible.

Lemma 5.3.12. *Let X be a variety and $U \subset X$ a non-empty set. If U is open (in the Zariski topology) in X then U is **dense** in X (i.e., the topological closure of U in X in the Zariski topology is X).*

Proof: Let X_1 be the closure of U in X and $X_2 = X - U$. Then $X = X_1 \cup X_2$ and X_1, X_2 are closed sets. Since X is irreducible and $X_2 \neq X$ it follows that $X_1 = X$. □

Lemma 5.3.13. *Let X be a variety and U a non-empty open subset of X. Then $I_{\Bbbk}(U) = I_{\Bbbk}(X)$.*

Proof: Since $U \subseteq X$ we have $I_{\Bbbk}(X) \subseteq I_{\Bbbk}(U)$. Now let $f \in I_{\Bbbk}(U)$. Then $U \subseteq V(f) \cap X$. Write $X_1 = V(f) \cap X$, which is an algebraic set, and $X_2 = X - U$, which is also an algebraic set. Then $X = X_1 \cup X_2$ and, since X is irreducible and $X_2 \neq X$, $X = X_1$. In other words, $f \in I_{\Bbbk}(X)$. □

Exercise 5.3.14. Let X be an irreducible variety. Prove that if $U_1, U_2 \subseteq X$ are non-empty open sets then $U_1 \cap U_2 \neq \varnothing$.

5.4 Function Fields

If X is a variety defined over $\Bbbk$ then $I_{\Bbbk}(X)$ is a prime ideal and so the affine or homogeneous coordinate ring is an integral domain. One can therefore consider its field of fractions. If X is affine then the field of fractions has a natural interpretation as a set of maps $X \to \Bbbk$. When X is projective then a ratio f/g of polynomials does not give a well-defined function on X unless f and g are homogeneous of the same degree.

Definition 5.4.1. Let X be an affine variety defined over $\Bbbk$. The **function field** $\Bbbk(X)$ is the set

$$\Bbbk(X) = \{f_1/f_2 : f_1, f_2 \in \Bbbk[X], f_2 \notin I_{\Bbbk}(X)\}$$

of classes under the equivalence relation $f_1/f_2 \equiv f_3/f_4$ if and only if $f_1 f_4 - f_2 f_3 \in I_{\Bbbk}(X)$. In other words, $\Bbbk(X)$ is the field of fractions of the affine coordinate ring $\Bbbk[X]$ over $\Bbbk$.

Let X be a projective variety. The **function field** is

$$\Bbbk(X) = \{f_1/f_2 : f_1, f_2 \in \Bbbk[X] \text{ homogeneous of the same degree}, f_2 \notin I_{\Bbbk}(X)\}$$

with the equivalence relation $f_1/f_2 \equiv f_3/f_4$ if and only if $f_1 f_4 - f_2 f_3 \in I_{\Bbbk}(X)$.

Elements of $\Bbbk(X)$ are called **rational functions**. For $a \in \Bbbk$ the rational function $f : X \to \Bbbk$ given by $f(P) = a$ is called a **constant function**.

Exercise 5.4.2. Prove that the field of fractions of an integral domain is a field. Hence, deduce that if X is an affine variety then $\Bbbk(X)$ is a field. Prove also that if X is a projective variety then $\Bbbk(X)$ is a field.

We stress that, when X is projective, $\Bbbk(X)$ is not the field of fractions of $\Bbbk[X]$ and that $\Bbbk[X] \not\subseteq \Bbbk(X)$. Also note that elements of the function field are not functions $X \to \Bbbk$ but maps $X \to \Bbbk$ (i.e., they are not necessarily defined everywhere).

Example 5.4.3. One has $\Bbbk(\mathbb{A}^2) \cong \Bbbk(x,y)$ and $\Bbbk(\mathbb{P}^2) \cong \Bbbk(x,y)$.

Definition 5.4.4. Let X be a variety and let $f_1, f_2 \in \Bbbk[X]$. Then f_1/f_2 is **defined** or **regular** at P if $f_2(P) \neq 0$. An equivalence class $f \in \Bbbk(X)$ is **regular** at P if it contains some f_1/f_2 with $f_1, f_2 \in \Bbbk[X]$ (if X is projective then necessarily $\deg(f_1) = \deg(f_2)$) such that f_1/f_2 is regular at P.

Note that there may be many choices of representative for the equivalence class of f, and only some of them may be defined at P.

Example 5.4.5. Let $\Bbbk$ be a field of characteristic not equal to 2. Let X be the algebraic set $V(y^2 - x(x-1)(x+1)) \subset \mathbb{A}^2(\Bbbk)$. Consider the functions

$$f_1 = \frac{x(x-1)}{y} \qquad \text{and} \qquad f_2 = \frac{y}{x+1}.$$

One can check that f_1 is equivalent to f_2. Note that f_1 is not defined at $(0,0), (1,0)$ or $(-1,0)$ while f_2 is defined at $(0,0)$ and $(1,0)$ but not at $(-1,0)$. The equivalence class of f_1 is therefore regular at $(0,0)$ and $(1,0)$. Section 7.3 gives techniques to deal with these issues for curves, from which one can deduce that no function in the equivalence class of f_1 is defined at $(-1,0)$.

Exercise 5.4.6. Let X be a variety over $\Bbbk$. Suppose f_1/f_2 and f_3/f_4 are equivalent functions on X that are both defined at $P \in X(\Bbbk)$. Show that $(f_1/f_2)(P) = (f_3/f_4)(P)$.

Hence, if f is a function that is defined at a point P then it makes sense to speak of the **value** of the function at P. If the value of f at P is zero then P is called a **zero** of f.[5]

Exercise 5.4.7. Let $X = V(w^2x^2 - w^2z^2 - y^2z^2 + x^2z^2) \subseteq \mathbb{P}^3(\Bbbk)$. Show that $(x^2 + yz)/(x^2 - w^2) \equiv (x^2 - z^2)/(x^2 - yz)$ in $\Bbbk(X)$. Hence find the value of $(x^2 - z^2)/(x^2 - yz)$ at the point $(w : x : y : z) = (0 : 1 : 1 : 1)$. Show that both representations of the function have the same value on the point $(w : x : y : z) = (2 : 1 : -1 : 1)$.

Theorem 5.4.8. *Let X be a variety and let f be a rational function. Then there is a non-empty open set $U \subset X$ such that f is regular on U. Conversely, if $U \subset X$ is non-empty and open and $f : U \to \Bbbk$ is a function given by a ratio f_1/f_2 of polynomials (homogeneous polynomials of the same degree if X is projective) that is defined for all $P \in U$ then f extends uniquely to a rational function $f : X \to \Bbbk$.*

Proof: Let $f = f_1/f_2$ where $f_1, f_2 \in \Bbbk[X]$. Define $U = X - V(f_2)$. Since $f_2 \neq 0$ in $\Bbbk[X]$ we have U a non-empty open set, and f is regular on U.

For the converse, Let $f = f_1/f_2$ be a function on U given as a ratio of polynomials. Then one can consider f_1 and f_2 as elements of $\Bbbk[X]$ and f_2 non-zero on U implies $f_2 \neq 0$ in $\Bbbk[X]$. Hence f_1/f_2 corresponds to an element of $\Bbbk(X)$. Finally, suppose f_1/f_2 and f_3/f_4 are functions on X (where f_1, f_2, f_3, f_4 are polynomials) such that the restrictions $(f_1/f_2)|_U$ and $(f_3/f_4)|_U$ are equal. Then $f_1f_4 - f_2f_3$ is zero on U and, by Lemma 5.3.13, $(f_1f_4 - f_2f_3) \in I_{\Bbbk}(X)$ and $f_1/f_2 \equiv f_3/f_4$ on X. □

Corollary 5.4.9. *If X is a projective variety and $X \cap \mathbb{A}^n \neq \varnothing$ then $\Bbbk(X) \cong \Bbbk(X \cap \mathbb{A}^n)$. If X is non-empty affine variety then $\Bbbk(X) \cong \Bbbk(\overline{X})$.*

Proof: The result follows since $X \cap \mathbb{A}^n = X - V(x_n)$ is open in X and X is open in $\overline{X}$. □

[5]For curves we will later define the notion of a function f having a pole at a point P. This notion does not make sense for general varieties, as shown by the function x/y on $\mathbb{A}^2$ at $(0,0)$ for example.

Definition 5.4.10. Let X be a variety and $U \subseteq X$. Define $\mathcal{O}(U)$ to be the elements of $\overline{\Bbbk}(X)$ that are regular on all $P \in U(\overline{\Bbbk})$.

Lemma 5.4.11. *If X is an affine variety over $\Bbbk$ then $\mathcal{O}(X) = \overline{\Bbbk}[X]$.*

Proof: (Sketch) Clearly $\overline{\Bbbk}[X] \subseteq \mathcal{O}(X)$. The converse follows since $\mathcal{O}(X)$ is the intersection of the local rings (see Definition 7.1.1) at all $P \in X(\overline{\Bbbk})$. We refer to Proposition 2 on page 43, Chapter 2 of [216] or Theorem I.3.2(a) of [278] for the details. □

Definition 5.4.12. Let X be a variety over $\Bbbk$ and $f \in \overline{\Bbbk}(X)$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. If $f = f_1/f_2$ where $f_1, f_2 \in \overline{\Bbbk}[\underline{x}]$ define $\sigma(f) = \sigma(f_1)/\sigma(f_2)$ where $\sigma(f_1)$ and $\sigma(f_2)$ denote the natural Galois action on polynomials (i.e., $\sigma(\sum_i a_i x^i) = \sum_i \sigma(a_i) x^i$). Some authors write this as f^σ.

Exercise 5.4.13. Prove that $\sigma(f)$ is well-defined (i.e., if $f \equiv f'$ then $\sigma(f) \equiv \sigma(f')$). Let $P \in X(\overline{\Bbbk})$. Prove that $f(P) = 0$ if and only if $\sigma(f)(\sigma(P)) = 0$.

Remark 5.4.14. Having defined an action of $G = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ on $\overline{\Bbbk}(X)$ it is natural to ask whether $\overline{\Bbbk}(X)^G = \{f \in \overline{\Bbbk}(X) : \sigma(f) = f \ \forall \sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)\}$ is the same as $\Bbbk(X)$. The issue is whether a function being "defined over $\Bbbk$" is the same as "can be written with coefficients in $\Bbbk$". Indeed, this is true but not completely trivial.

A sketch of the argument is given in Exercise 1.12 of Silverman [564] and we give a few extra hints here. Let X be a projective variety. One first shows that if X is defined over $\Bbbk$ and if $\Bbbk'$ is a finite Galois extension of $\Bbbk$ then $I_{\Bbbk'}(X)$ is an induced Galois module (see page 110 of Serre [542]) for $\mathrm{Gal}(\Bbbk'/\Bbbk)$. It follows from Section VII.1 of [542] that the Galois cohomology group $H^1(\mathrm{Gal}(\Bbbk'/\Bbbk), I_{\Bbbk'}(X))$ is trivial and hence, by Section X.3 of [542], that $H^1(G, I_{\Bbbk'}(X)) = 0$. One can therefore deduce, as in Exercise 1.12(a) of [564], that $\overline{\Bbbk}[X]^G = \Bbbk[X]$.

To show that $\overline{\Bbbk}(X)^G = \Bbbk(X)$ let $(f_0 : f_1) : X \to \mathbb{P}^1$ and let $\sigma \in G$. Then $\sigma(f_0) = \lambda_\sigma f_0 + G_{0,\sigma}$ and $\sigma(f_1) = \lambda_\sigma f_1 + G_{1,\sigma}$ where $\lambda_\sigma \in \overline{\Bbbk}^*$ and $G_{0,\sigma}, G_{1,\sigma} \in I_{\overline{\Bbbk}}(X)$. One shows first that $\lambda_\sigma \in H^1(G, \overline{\Bbbk}^*)$, which is trivial by Hilbert 90, and so $\lambda_\sigma = \sigma(\alpha)/\alpha$ for some $\alpha \in \overline{\Bbbk}$. Replacing f_0 by αf_0 and f_1 by αf_1 gives $\lambda_\sigma = 1$ and one can proceed to showing that $G_{0,\sigma}, G_{1,\sigma} \in H^1(G, I_{\overline{\Bbbk}}(X)) = 0$ as above. The result follows.

For a different approach see Theorem 7.8.3 and Remark 8.4.11 below, or Corollary 2 of Section VI.5 (page 178) of Lang [364].

5.5 Rational Maps and Morphisms

Definition 5.5.1. Let X be an affine or projective variety over a field $\Bbbk$ and Y an affine variety in $\mathbb{A}^n$ over $\Bbbk$. Let $\phi_1, \ldots, \phi_n \in \Bbbk(X)$. A map $\phi : X \to \mathbb{A}^n$ of the form

$$\phi(P) = (\phi_1(P), \ldots, \phi_n(P)) \tag{5.1}$$

is **regular** at a point $P \in X(\overline{\Bbbk})$ if all ϕ_i, for $1 \leq i \leq n$, are regular at P. A **rational map** $\phi : X \to Y$ defined over $\Bbbk$ is a map of the form (5.1) such that, for all $P \in X(\overline{\Bbbk})$ for which ϕ is regular at P then $\phi(P) \in Y(\overline{\Bbbk})$.

Let X be an affine or projective variety over a field $\Bbbk$ and Y a projective variety in $\mathbb{P}^n$ over $\Bbbk$. Let $\phi_0, \ldots, \phi_n \in \Bbbk(X)$. A map $\phi : X \to \mathbb{P}^n$ of the form

$$\phi(P) = (\phi_0(P) : \cdots : \phi_n(P)) \tag{5.2}$$

is **regular** at a point $P \in X(\overline{\Bbbk})$ if there is some function $g \in \Bbbk(X)$ such that all $g\phi_i$, for $0 \leq i \leq n$, are regular at P and, for some $0 \leq i \leq n$, one has $(g\phi_i)(P) \neq 0$.[6] A **rational**

[6] This last condition is to prevent ϕ mapping to $(0 : \cdots : 0)$, which is not a point in $\mathbb{P}^n$.

map $\phi : X \to Y$ defined over $\Bbbk$ is a map of the form (5.2) such that, for all $P \in X(\overline{\Bbbk})$ for which ϕ is regular at P, then $\phi(P) \in Y(\overline{\Bbbk})$.

We stress that a rational map is not necessarily defined at every point of the domain. In other words, it is not necessarily a function.

Exercise 5.5.2. Let X and Y be projective varieties. Show that one can write a rational map in the form $\phi(P) = (\phi_0(P) : \cdots : \phi_n(P))$ where the $\phi_i(\underline{x}) \in \Bbbk[\underline{x}]$ are all homogeneous polynomials of the same degree, not all $\phi_i(\underline{x}) \in I_\Bbbk(X)$, and for every $f \in I_\Bbbk(Y)$ we have $f(\phi_0(\underline{x}), \ldots, \phi_n(\underline{x})) \in I_\Bbbk(X)$.

Example 5.5.3. Let $X = V(x - y) \subseteq \mathbb{A}^2$ and $Y = V(x - z) \subseteq \mathbb{P}^2$. Then

$$\phi(x, y) = (x : xy : y)$$

is a rational map from X to Y. Note that this formula for ϕ is not defined at $(0, 0)$. However, ϕ is regular at $(0, 0)$ since taking $g = x^{-1}$ gives the equivalent form $\phi(x, y) = (x^{-1}x : x^{-1}xy : x^{-1}y) = (1 : y : y/x)$ and $y/x \equiv 1$ in $\Bbbk(X)$. Also note that the image of ϕ is not equal to $Y(\Bbbk)$ as it misses the point $(0 : 1 : 0)$.

Similarly, $\psi(x : y : z) = (x/y, z/y)$ is a rational map from Y to X. This map is not regular at $(1 : 0 : 1)$ but it is surjective to X. The composition $\psi \circ \phi$ maps (x, y) to $(1/y, 1/x)$.

Example 5.5.4. Let $X = V(y^2z - (x^3 + Axz^2)) \subseteq \mathbb{P}^2$ and $Y = \mathbb{P}^1$. Consider the rational map

$$\phi(x : y : z) = (x/z : 1).$$

Note that this formula for ϕ is defined at all points of X except $P_0 = (0 : 1 : 0)$. Let $g(x : y : z) = (x^2 + Az^2)/y^2 \in \Bbbk(X)$. Then the map $(x : y : z) \mapsto (gx/z : g)$ can be written as $(x : y : z) \mapsto (1 : g)$ and this is defined at $(0 : 1 : 0)$. It follows that ϕ is regular at P_0 and that $\phi(P_0) = (1 : 0)$.

Lemma 5.5.5. *Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a rational map. Then there is an open set $U \subseteq X$ such that ϕ is regular on U.*

Proof: Write ϕ as $(\phi_1, \ldots, \phi_n)$ if Y is affine or $(\phi_0 : \cdots : \phi_n)$ if Y is projective. By Theorem 5.4.8 for each ϕ_i for $1 \leq \phi_i \leq n$ (respectively, $0 \leq \phi_i \leq n$) there is a non-empty open set $U_i \subset X$ such that ϕ_i is regular. Taking $U = \cap_i U_i$ gives the result. □

It immediately follows that Theorem 5.4.8 generalises to rational maps.

Theorem 5.5.6. *Let X and Y be varieties. Suppose $\phi_1, \phi_2 : X \to Y$ are rational maps that are regular on non-empty open sets $U_1, U_2 \subseteq X$. Suppose further that $\phi_1|_{U_1 \cap U_2} = \phi_2|_{U_1 \cap U_2}$. Then $\phi_1 = \phi_2$.*

Exercise 5.5.7. Prove Theorem 5.5.6.

Definition 5.5.8. Let X and Y be algebraic varieties over $\Bbbk$. A rational map $\phi : X \to Y$ defined over $\Bbbk$ is a **birational equivalence** over $\Bbbk$ if there exists a rational map $\psi : Y \to X$ over $\Bbbk$ such that:

1. $\psi \circ \phi(P) = P$ for all points $P \in X(\overline{\Bbbk})$ such that $\psi \circ \phi(P)$ is defined;
2. $\phi \circ \psi(Q) = Q$ for all points $Q \in Y(\overline{\Bbbk})$ such that $\phi \circ \psi(Q) = Q$ is defined.

Varieties X and Y are **birationally equivalent** if there is a birational equivalence $\phi : X \to Y$ between them.

Exercise 5.5.9. Show that $X = V(xy-1) \subseteq \mathbb{A}^2$ and $Y = V(x_1-x_2) \subseteq \mathbb{P}^2$ are birationally equivalent.

Exercise 5.5.10. Verify that birational equivalence is an equivalence relation.

Example 5.5.11. The maps $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ and $\varphi_i^{-1} : \mathbb{P}^n \to \mathbb{A}^n$ from Definition 5.2.24 are rational maps. Hence $\mathbb{A}^n$ and $\mathbb{P}^n$ are birationally equivalent.

Definition 5.5.12. Let X and Y be varieties over $\Bbbk$ and let $U \subseteq X$ be open. A rational map $\phi : U \to Y$ over $\Bbbk$ which is regular at every point $P \in U(\overline{\Bbbk})$ is called a **morphism** over $\Bbbk$.

Let $U \subseteq X$ and $V \subseteq Y$ be open. If $\phi : U \to Y$ is a morphism over $\Bbbk$ and $\psi : V \to X$ is a morphism over $\Bbbk$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity on V and U respectively then we say that U and V are **isomorphic** over $\Bbbk$. If U and V are isomorphic we write $U \cong V$.

Example 5.5.13. Let X be $V(xy - z^2) \subseteq \mathbb{P}^2$ and let $\phi : X \to \mathbb{P}^1$ be given by $\phi(x : y : z) = (x/z : 1)$. Then ϕ is a morphism (for $(1 : 0 : 0)$ replace ϕ by the equivalent form $\phi(x : y : z) = (1 : z/x)$ and for $(0 : 1 : 0)$ use $\phi(x : y : z) = (z/y : 1)$). Indeed, ϕ is an isomorphism with inverse $\psi(x : z) = (x/z : z/x : 1)$.

Lemma 5.5.5 shows that every rational map $\phi : X \to Y$ restricts to a morphism $\phi : U \to Y$ on some open set $U \subseteq X$.

Exercise 5.5.14. Let $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$ over $\Bbbk$. By taking a line of slope $t \in \Bbbk$ through $(-1, 0)$ give a formula for a rational map $\phi : \mathbb{A}^1 \to X$. Explain how to extend this to a morphism from $\mathbb{P}^1$ to $V(x^2 + y^2 - 1)$. Show that this is an isomorphism.

We now give the notion of a dominant rational map (or morphism). This is the appropriate analogue of surjectivity for maps between varieties. Essentially, a rational map from X to Y is dominant if its image is not contained in a proper subvariety of Y. For example, the map $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ is dominant. Birational maps are also dominant.

Definition 5.5.15. Let X and Y be varieties over $\Bbbk$. A set $U \subseteq Y(\overline{\Bbbk})$ is **dense** if its closure in the Zariski topology in $Y(\overline{\Bbbk})$ is equal to $Y(\overline{\Bbbk})$. A rational map $\phi : X \to Y$ is **dominant** if $\phi(X(\overline{\Bbbk}))$ is **dense** in $Y(\overline{\Bbbk})$.

Example 5.5.16. Let $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ be given by $\phi(x, y) = (x, x)$. Then ϕ is not dominant (though it is dominant to $V(x-y) \subseteq \mathbb{A}^2$). Let $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ be given by $\phi(x, y) = (x, xy)$. Then ϕ is dominant, even though it is not surjective.

We now show that a morphism is a continuous map for the Zariski topology.

Lemma 5.5.17. *Let X and Y be varieties over $\Bbbk$. Let $\phi : X \to Y$ be a morphism. Let $V \subseteq Y$ be an open set such that $\phi(X) \cap V \neq \varnothing$. Then $\phi^{-1}(V)$ is an open set in X. Similarly, let $Z \subseteq Y$ be a closed set such that $\phi(X) \cap Z \neq \varnothing$. Then $\phi^{-1}(Z)$ is closed in X.*

Exercise 5.5.18.★ Prove Lemma 5.5.17.

Exercise 5.5.19. Let X and Y be varieties and let $\phi : X \to Y$ be a morphism. Show that the Zariski closure of $\phi(X)$ in Y is irreducible.

Lemma 5.5.20. *Let X and Y be affine varieties over $\Bbbk$, let $U \subseteq X$ be open, and let $\phi : U \to Y$ be a morphism. Then the composition $f \circ \phi$ induces a well-defined ring homomorphism from $\overline{\Bbbk}[Y]$ to $\mathcal{O}(U)$.*

Proof: If $f \in \overline{\Bbbk}[Y]$ then f is regular on Y and, since ϕ is regular on U, $f \circ \phi$ is regular on U. Hence, $f \circ \phi \in \mathcal{O}(U)$.

We now show that the map is well-defined. Suppose $f \equiv 0$ in $\overline{\Bbbk}[Y]$. Since f vanishes on Y it follows that, for all $P \in U(\overline{\Bbbk})$, $f(\phi(P)) = 0$. Write $f \circ \phi = f_1/f_2$ where f_1 and f_2 are polynomials. It follows that $f_1 \in I(U) = I(X)$ (using Lemma 5.3.13). Hence, $f \circ \phi \equiv 0$ in $\mathcal{O}(U)$. Finally, the map is a ring homomorphism since $(f_1 + f_2) \circ \phi = (f_1 \circ \phi) + (f_2 \circ \phi)$ and similarly for multiplication. □

Definition 5.5.21. Let X and Y be affine varieties over $\Bbbk$, let $U \subseteq X$ be open, and let $\phi : U \to Y$ be a morphism. The **pullback**[7] is the ring homomorphism $\phi^* : \overline{\Bbbk}[Y] \to \mathcal{O}(U)$ defined by $\phi^*(f) = f \circ \phi$.

Lemma 5.5.22. *Let X and Y be affine varieties over $\Bbbk$, let $U \subseteq X$ be open, and let $\phi : U \to Y$ be a morphism. Then ϕ is dominant if and only if ϕ^* is injective.*

Proof: Let $f \in \overline{\Bbbk}[Y]$ be in the kernel of ϕ^*. Now $\phi^*(f) = 0$ is the same as $f \circ \phi = 0$ on U, which implies $\phi(U) \subseteq V(f) \cap Y$. If $\phi(U)$ is dense in Y then $Y \subseteq V(f)$ and so $f \in I(Y)$ and ϕ^* is injective. Conversely, if $\phi(U)$ is not dense in Y then there is some polynomial $f \notin I(Y)$ such that $\phi(U) \subseteq Y \cap V(f)$. It follows that $\phi^*(f) = 0$ and ϕ^* is not injective. □

Note that if X and ϕ are defined over $\Bbbk$ then $\phi^* : \overline{\Bbbk}[Y] \to \mathcal{O}(U)$ restricts to $\phi^* : \Bbbk[Y] \to \Bbbk(X)$. If ϕ^* is injective then one can extend it to get a homomorphism of the field of fractions of $\Bbbk[Y]$ to $\Bbbk(X)$.

Definition 5.5.23. Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a dominant rational map defined over $\Bbbk$. Define the **pullback** $\phi^* : \Bbbk(Y) \to \Bbbk(X)$ by $\phi^*(f) = f \circ \phi$.

We will now sketch a proof that ϕ^* is a $\Bbbk$-algebra homomorphism. Recall that a $\Bbbk$-algebra homomorphism of fields is a field homomorphism that is the identity map on $\Bbbk$.

Theorem 5.5.24. *Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a dominant rational map defined over $\Bbbk$. Then the pullback $\phi^* : \Bbbk(Y) \to \Bbbk(X)$ is an injective $\Bbbk$-algebra homomorphism.*

Proof: Without loss of generality we may assume that X and Y are affine. The rational map ϕ is therefore given by $\phi(\underline{x}) = (\phi_1(\underline{x}), \ldots, \phi_n(\underline{x}))$. Let $U \subseteq X$ be an open set on which ϕ is regular. Then $\phi : U \to Y$ is a morphism and we know $\phi^* : \overline{\Bbbk}[Y] \to \mathcal{O}(U)$ is a ring homomorphism by Lemma 5.5.20. The field of fractions of $\overline{\Bbbk}[Y]$ is $\overline{\Bbbk}(Y)$ and the field of fractions of $\mathcal{O}(U)$ is $\overline{\Bbbk}(X)$. The natural extension of ϕ^* to $\phi^* : \overline{\Bbbk}(Y) \to \overline{\Bbbk}(X)$ is well-defined.

It immediately follows that ϕ^* is a ring homomorphism and that ϕ^* is the identity on $\overline{\Bbbk}$. Hence, ϕ^* is a $\overline{\Bbbk}$-algebra homomorphism. Furthermore, ϕ^* is injective by Lemma 5.5.22. Finally, since ϕ is defined over $\Bbbk$ it restricts to an injective homomorphism from $\Bbbk(Y)$ to $\Bbbk(X)$. □

Example 5.5.25. Consider the rational maps from Example 5.5.16. The map $\phi(x, y) = (x, x)$ is not dominant and does not induce a well-defined function from $\Bbbk(x, y)$ to $\Bbbk(x, y)$ since, for example, $\phi^*(1/(x - y)) = 1/(x - x) = 1/0$.

The map $\phi(x, y) = (x, xy)$ is dominant and $\phi^*(f(x, y)) = f(x, xy)$ is a field isomorphism.

[7] Pullback is just a fancy name for "composition"; but we think of it as "pulling" a structure from the image of ϕ back to the domain.

Exercise 5.5.26. Let K_1, K_2 be fields containing a field $\Bbbk$. Let $\theta : K_1 \to K_2$ be a $\Bbbk$-algebra homomorphism. Show that θ is injective.

Theorem 5.5.27. *Let X and Y be varieties over $\Bbbk$ and let $\theta : \Bbbk(Y) \to \Bbbk(X)$ be a $\Bbbk$-algebra homomorphism. Then θ induces a dominant rational map $\phi : X \to Y$ defined over $\Bbbk$.*

Proof: If Y is projective it suffices to construct a rational map to an affine part, say $Y \cap \mathbb{A}^n$. Hence, we assume that $Y \subseteq \mathbb{A}^n$ is affine and described by coordinates $(y_1, \ldots, y_n)$.

The homomorphism θ maps each y_i to some $\phi_i(\underline{x}) \in \Bbbk(X)$ for $1 \leq i \leq n$. Define $\phi : X \to \mathbb{A}^n$ by

$$\phi(P) = (\phi_1(P), \ldots, \phi_n(P)).$$

We now show that if $P \in X(\overline{\Bbbk})$ and if ϕ is regular at P then $\phi(P) \in Y(\overline{\Bbbk})$. Let $f \in I(Y)$. Then

$$f(\phi(P)) = f(\phi_1(P), \ldots, \phi_n(P)) = f(\theta(y_1)(P), \ldots, \theta(y_n)(P)).$$

Now, θ is a $\Bbbk$-algebra homomorphism and f is a polynomial in $\Bbbk[y_1, \ldots, y_n]$. Hence

$$f(\theta(y_1), \ldots, \theta(y_n)) = \theta(f(y_1, \ldots, y_n)).$$

Since $f(y_1, \ldots, y_n) \in I(Y)$ it follows that $f(y_1, \ldots, y_n) = 0$ in $\Bbbk(Y)$ and so $\theta(f) = 0$. It follows that $f(\phi(P)) = \theta(f)(P) = \theta(0)(P) = 0$ for all $f \in I(Y)$ and so $P \in Y(\overline{\Bbbk})$ by part 5 of Proposition 5.1.16.

Finally, by Exercise 5.5.26, θ is injective. Also, ϕ^* equals θ and so ϕ^* is injective. Hence, Lemma 5.5.22 implies that ϕ is dominant. □

Theorem 5.5.28. *Let X and Y be varieties over $\Bbbk$. Then X and Y are birationally equivalent over $\Bbbk$ if and only if $\Bbbk(X) \cong \Bbbk(Y)$ (isomorphic as fields).*

Proof: Let $\phi : X \to Y$ and $\psi : Y \to X$ be the birational equivalence. First we must deduce that ϕ and ψ are dominating. There are subsets $U \subseteq X$ and $V \subseteq Y$ such that ϕ is regular on U, ψ is regular on V and $\psi \circ \phi$ is the identity on U (in other words, $\phi : U \to V$ is an isomorphism). The maps $\phi^* : \overline{\Bbbk}[V] \to \mathcal{O}(U)$ and $\psi^* : \overline{\Bbbk}[X] \to \mathcal{O}(V)$ therefore satisfy $\phi^*\psi^*(f) = f \circ (\psi \circ \psi) = f$ (at least, they are equal on $U \cap \phi^{-1}(V)$, which can be shown to be open) and so are injective. It follows from Lemma 5.5.22 that ϕ and ψ are dominant.

Hence, ϕ induces a $\Bbbk$-algebra homomorphism $\phi^* : \Bbbk(Y) \to \Bbbk(X)$ and ψ induces a $\Bbbk$-algebra homomorphism $\phi^* : \Bbbk(X) \to \Bbbk(Y)$. Finally, $\psi \circ \phi$ induces a $\Bbbk$-algebra homomorphism $\phi^*\psi^* : \Bbbk(X) \to \Bbbk(X)$ that is the identity (since it is the identity on a dense open set). It follows that ψ^* and ϕ^* are isomorphisms.

For the converse, if $\theta : \Bbbk(Y) \to \Bbbk(X)$ is an isomorphism then we associate a dominant rational map $\phi : X \to Y$ to θ and $\psi : Y \to X$ to θ^{-1}. Since $\theta^{-1}\theta$ is the identity it follows that $\psi \circ \phi$ is the identity whenever it is regular. □

Some authors prefer to study function fields rather than varieties, especially in the case of dimension 1 (there are notable classical texts that take this point of view by Chevalley and Deuring; see Stichtenoth [589] for a more recent version). By Theorem 5.5.28 (and other results) the study of function fields up to isomorphism is the study of varieties up to birational equivalence. A specific set of equations to describe a variety is called a **model**.

Definition 5.5.29. Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a rational map over $\overline{\Bbbk}$ given by $\phi(P) = (\phi_1(P), \ldots, \phi_n(P))$ if Y is affine and $(\phi_0(P) : \cdots : \phi_n(P))$ if Y is projective. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Define $\sigma(\phi) : X \to Y$ by $\sigma(\phi)(P) = (\sigma(\phi_1)(P), \ldots, \sigma(\phi_n(P)))$ if Y is affine and $\sigma(\phi)(P) = (\sigma(\phi_0)(P) : \cdots : \sigma(\phi_n(P)))$ if Y is projective. Many authors act by Galois on the right and so write the action as ϕ^σ.

Lemma 5.5.30. *Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a rational map over $\overline{\Bbbk}$. If $\sigma(\phi) = \phi$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then ϕ is defined over $\Bbbk$.*

Proof: If Y is affine then $\phi(P) = (\phi_1(P), \ldots, \phi_n(P))$ where $\phi_i \in \overline{\Bbbk}(X)$. If $\sigma(\phi) = \phi$ then $\sigma(\phi_i) = \phi_i$ for all $1 \leq i \leq n$. Remark 5.4.14 therefore implies that $\phi_i \in \Bbbk(X)$ for all i and so ϕ is defined over $\Bbbk$.

If Y is projective then $\phi(P) = (\phi_0(P) : \cdots : \phi_n(P))$ where $\phi_i \in \overline{\Bbbk}(X)$ for $0 \leq i \leq n$. If $\phi(P) = \sigma(\phi)(P)$ then, for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$, there is some $xi(\sigma) \in \overline{\Bbbk}^*$ such that $\sigma(\phi_i) = \xi(\sigma)\phi_i$ for all $0 \leq i \leq n$. As in Lemma 5.2.5, $\xi : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ is a 1-cocycle and so by Hilbert 90 is a co-boundary. It follows that one can choose the ϕ_i so that $\sigma(\phi_i) = \phi_i$ and hence, by Remark 5.4.14, $\phi_i \in \Bbbk(X)$ for $0 \leq i \leq n$. □

5.6 Dimension

The natural notion of dimension (a point has dimension 0, a line has dimension 1, a plane has dimension 2, etc) generalises to algebraic varieties. There are algebraic and topological ways to define dimension. We use an algebraic approach.[8]

We stress that the notion of dimension only applies to irreducible algebraic sets. For example $X = V(x, y) \cup V(x-1) = V(x(x-1), y(x-1)) \subseteq \mathbb{A}^2$ is the union of a point and a line so has components of different dimension.

Recall the notion of transcendence degree of an extension $\Bbbk(X)$ over $\Bbbk$ from Definition A.6.3.

Definition 5.6.1. Let X be a variety over $\Bbbk$. The **dimension** of X, denoted $\dim(X)$, is the transcendence degree of $\Bbbk(X)$ over $\Bbbk$.

Example 5.6.2. The dimension of $\mathbb{A}^n$ is n. The dimension of $\mathbb{P}^n$ is n.

Theorem 5.6.3. *Let X and Y be varieties. If X and Y are birationally equivalent then $\dim(X) = \dim(Y)$.*

Proof: Immediate from Theorem 5.5.28. □

Corollary 5.6.4. *Let X be a projective variety such that $X \cap \mathbb{A}^n$ is non-empty. Then $\dim(X) = \dim(X \cap \mathbb{A}^n)$. Let X be an affine variety. Then $\dim(X) = \dim\left(\overline{X}\right)$.*

Exercise 5.6.5. Let f be a non-constant polynomial and let $X = V(f)$ be a variety in $\mathbb{A}^n$. Show that $\dim(X) = n - 1$.

Exercise 5.6.6. Show that if X is a non-empty variety of dimension zero then $X = \{P\}$ is a single point.

An useful alternative formulation of dimension is as follows.

Definition 5.6.7. Let R be a ring. The **Krull dimension** of R is the supremum of $n \in \mathbb{Z}_{\geq 0}$ such that there exists a chain $I_0 \subset I_1 \subset \cdots \subset I_n$ of prime R-ideals such that $I_{j-1} \neq I_j$ for $1 \leq j \leq n$.

Theorem 5.6.8. *Let X be an affine variety over $\Bbbk$. Then $\dim(X)$ is equal to the Krull dimension of the affine coordinate ring $\Bbbk[X]$.*

Proof: See Proposition I.1.7 and Theorem I.1.8A of [278]. □

[8] See Chapter 8 of Eisenbud [191] for a clear criticism of this approach.

Corollary 5.6.9. *Let X and Y be affine varieties over $\Bbbk$ such that Y is a proper subset of X. Then* $\dim(Y) < \dim(X)$.

Proof: Since $Y \neq X$ we have $I_{\Bbbk}(X) \subsetneq I_{\Bbbk}(Y)$ and both ideals are prime since X and Y are irreducible. It follows that the Krull dimension of $\Bbbk[X]$ is at least one more than the Krull dimension of $\Bbbk[Y]$. □

Exercise 5.6.10. Show that a proper closed subset of a variety of dimension 1 is finite.

5.7 Weil Restriction of Scalars

Weil restriction of scalars is simply the process of re-writing a system of polynomial equations over a finite algebraic extension $\Bbbk'/\Bbbk$ as a system of equations in more variables over $\Bbbk$. The canonical example is identifying the complex numbers $\mathbb{A}^1(\mathbb{C})$ with $\mathbb{A}^2(\mathbb{R})$ via $z = x + iy \in \mathbb{A}^1(\mathbb{C}) \mapsto (x, y) \in \mathbb{A}^2(\mathbb{R})$. We only need to introduce this concept in the special case of affine algebraic sets over finite fields.

Lemma 5.7.1. *Let q be a prime power, $m \in \mathbb{N}$ and fix a vector space basis $\{\theta_1, \ldots, \theta_m\}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $x_1, \ldots, x_n$ be coordinates for $\mathbb{A}^n$ and let $y_{1,1}, \ldots, y_{1,m}, \ldots, y_{n,1}, \ldots, y_{n,m}$ be coordinates for $\mathbb{A}^{nm}$. The map $\phi : \mathbb{A}^{nm} \to \mathbb{A}^n$ given by*

$$\phi(y_{1,1}, \ldots, y_{n,m}) = (y_{1,1}\theta_1 + \cdots + y_{1,m}\theta_m, y_{2,1}\theta_1 + \cdots + y_{2,m}\theta_m, \ldots, y_{n,1}\theta_1 + \cdots + y_{n,m}\theta_m)$$

gives a bijection between $\mathbb{A}^{nm}(\mathbb{F}_q)$ and $\mathbb{A}^n(\mathbb{F}_{q^m})$.

Exercise 5.7.2. Prove Lemma 5.7.1.

Definition 5.7.3. Let $X = V(S) \subseteq \mathbb{A}^n$ be an affine algebraic set over $\mathbb{F}_{q^m}$. Let ϕ be as in Lemma 5.7.1. For each polynomial $f(x_1, \ldots, x_n) \in S \subseteq \mathbb{F}_{q^m}[x_1, \ldots, x_n]$ write

$$\phi^*(f) = f \circ \phi = f(y_{1,1}\theta_1 + \cdots + y_{1,m}\theta_m, y_{2,1}\theta_1 + \cdots + y_{2,m}\theta_m, \ldots, y_{n,1}\theta_1 + \cdots + y_{n,m}\theta_m) \tag{5.3}$$

as

$$f_1(y_{1,1}, \ldots, y_{n,m})\theta_1 + f_2(y_{1,1}, \ldots, y_{n,m})\theta_2 + \cdots + f_m(y_{1,1}, \ldots, y_{n,m})\theta_m \tag{5.4}$$

where each $f_j \in \mathbb{F}_q[y_{1,1}, \ldots, y_{n,m}]$. Define $S' \subseteq \mathbb{F}_q[y_{1,1}, \ldots, y_{n,m}]$ to be the set of all such polynomials f_j over all $f \in S$. The **Weil restriction of scalars** of X with respect to $\mathbb{F}_{q^m}/\mathbb{F}_q$ is the affine algebraic set $Y \subseteq \mathbb{A}^{mn}$ defined by

$$Y = V(S').$$

Example 5.7.4. Let $p \equiv 3 \pmod 4$ and define $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 = -1$. Consider the algebraic set $X = V(x_1x_2 - 1) \subseteq \mathbb{A}^2$. The Weil restriction of scalars of X with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$ with basis $\{1, i\}$ is

$$Y = V(y_{1,1}y_{2,1} - y_{1,2}y_{2,2} - 1, y_{1,1}y_{2,2} + y_{1,2}y_{2,1}) \subseteq \mathbb{A}^4.$$

Recall from Example 5.1.5 that X is an algebraic group. The multiplication operation $\text{mult}((x_1, x_2), (x_1', x_2')) = (x_1x_1', x_2x_2')$ on X corresponds to the operation

$$\begin{gathered}\text{mult}((y_{1,1}, y_{1,2}, y_{2,1}, y_{2,2}), (y_{1,1}', y_{1,2}', y_{2,1}', y_{2,2}')) \\ = (y_{1,1}y_{1,1}' - y_{1,2}y_{1,2}', y_{1,1}y_{1,2}' + y_{1,2}y_{1,1}', y_{2,1}y_{2,1}' - y_{2,2}y_{2,2}', y_{2,1}y_{2,2}' + y_{2,2}y_{2,1}')\end{gathered}$$

on Y.

Exercise 5.7.5. Let $p \equiv 3 \pmod 4$. Write down the Weil restriction of scalars of $X = V(x^2 - 2i) \subset \mathbb{A}^1$ with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$.

Exercise 5.7.6. Let $p \equiv 3 \pmod 4$. Write down the Weil restriction of scalars of $V(x_1^2 + x_2^2 - (1 + 2i)) \subset \mathbb{A}^2$ with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$.

Theorem 5.7.7. *Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set over $\mathbb{F}_{q^m}$. Let $Y \subseteq \mathbb{A}^{mn}$ be the Weil restriction of X. Let $k \in \mathbb{N}$ be coprime to m. Then there is a bijection between $X(\mathbb{F}_{q^{mk}})$ and $Y(\mathbb{F}_{q^k})$.*

Proof: When $\gcd(k, m) = 1$ it is easily checked that the map ϕ of Lemma 5.7.1 gives a a one-to-one correspondence between $\mathbb{A}^{nm}(\mathbb{F}_{q^k})$ and $\mathbb{A}^n(\mathbb{F}_{q^{mk}})$.

Now, let $P = (x_1, \ldots, x_n) \in X$ and write $Q = (y_{1,1} \ldots, y_{n,m})$ for the corresponding point in $\mathbb{A}^{mn}$. For any $f \in S$ we have $f(P) = 0$. Writing $f_1, \ldots, f_m$ for the polynomials in equation (5.4) we have

$$f_1(Q)\theta_1 + f_2(Q)\theta_2 + \cdots + f_m(Q)\theta_m = 0.$$

Since $\{\theta_1, \ldots, \theta_m\}$ is also a vector space basis for $\mathbb{F}_{q^{mk}}$ over $\mathbb{F}_{q^k}$ we have

$$f_1(Q) = f_2(Q) = \cdots = f_m(Q) = 0.$$

Hence $f(Q) = 0$ for all $f \in S'$ and so $Q \in Y$. Similarly, if $Q \in Y$ then $f_j(Q) = 0$ for all such f_j and so $f(P) = 0$ for all $f \in S$. □

Note that, as the following example indicates, when k is not coprime to m then $X(\mathbb{F}_{q^{mk}})$ is not usually in one-to-one correspondence with $Y(\mathbb{F}_{q^k})$.

Exercise 5.7.8. Consider the algebraic set X from Exercise 5.7.5. Show that $X(\mathbb{F}_{p^4}) = \{1 + i, -1 - i\}$. Let Y be the Weil restriction of X with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$. Show that $Y(\mathbb{F}_{p^2}) = \{(1, 1), (-1, -1), (i, -i), (-i, i)\}$.

Note that the Weil restriction of $\mathbb{P}^n$ with respect to $\mathbb{F}_{q^m}/\mathbb{F}_q$ is not the projective closure of $\mathbb{A}^{mn}$. For example, considering the case $n = 1$, $\mathbb{P}^1$ has one point not contained in $\mathbb{A}^1$, whereas the projective closure of $\mathbb{A}^m$ has an $(m - 1)$-dimensional algebraic set of points at infinity.

Exercise 5.7.9. Recall from Exercise 5.5.14 that there is a morphism from $\mathbb{P}^1$ to $Y = V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$. Determine the Weil restriction of scalars of Y with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$. It makes sense to call this algebraic set the Weil restriction of $\mathbb{P}^1$ with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$.

Chapter 6

Tori, LUC and XTR

Recall from Example 5.1.5 that $\mathbb{F}_q^*$ satisfies our informal notion of an algebraic group. This chapter concerns certain subgroups of the multiplicative group of finite fields of the form $\mathbb{F}_{q^n}$ with $n > 1$. The main goal is to find short representations for elements. Algebraic tori give short representations of elements of certain subgroups of $\mathbb{F}_{q^n}^*$. Traces can be used to give short representations of certain algebraic group quotients in $\mathbb{F}_{q^n}^*$, and the most successful implementations of this are called LUC and XTR. These ideas are sometimes called **torus based cryptography** or **trace based cryptography**, though this is misleading: the issue is only about representation of elements and is independent of any specific cryptosystem.

6.1 Cyclotomic Subgroups of Finite Fields

Definition 6.1.1. Let $n \in \mathbb{N}$. A complex number z is an n-th **root of unity** if $z^n = 1$, and is a **primitive** n-th root of unity if $z^n = 1$ and $z^d \neq 1$ for any divisor $d \mid n$ with $1 \leq d < n$.

The n-th **cyclotomic polynomial** $\Phi_n(x)$ is the product $(x - z)$ over all primitive n-th roots of unity z.

Lemma 6.1.2. *Let $n \in \mathbb{N}$. Then*

1. $\deg(\Phi_n(x)) = \varphi(n)$.
2. $\Phi_n(x) \in \mathbb{Z}[x]$.
3. $$x^n - 1 = \prod_{d|n, 1 \leq d \leq n} \Phi_d(x).$$
4. *If $m \in \mathbb{N}$ is such that $m \neq n$ then* $\gcd(\Phi_n(x), \Phi_m(x)) = 1$.

5.

$$\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$$

where $\mu(d)$ is the Möbius function (Definition 4.3 of [468]).

Proof: Let z be a primitive n-th root of unity. Then every n-th root of unity is a power of z and, for $0 \leq i < n$, z^i is a primitive n-th root of unity if and only if $\gcd(n, i) = 1$. Therefore

$$\Phi_n(x) = \prod_{0 \leq i < n, \gcd(n,i)=1} (x - z^i)$$

and so $\deg(\Phi_n(x)) = \varphi(n)$.

Galois theory implies $\Phi_n(x) \in \mathbb{Q}[x]$ and, since z is an algebraic integer, it follows that $\Phi_n(x) \in \mathbb{Z}[x]$.[1]

The third fact follows since $x^n - 1 = \prod_{i=0}^{n-1}(x - z^i)$ and each z^i has some order $d \mid n$.

Let z be a root of $\gcd(\Phi_n(x), \Phi_m(x))$. Then z has order equal to both n and m, which is impossible if $n \neq m$.

Finally, writing z_d for some primitive d-th root of unity, note that

$$\begin{aligned}
\prod_{d|n}(x^{n/d} - 1)^{\mu(d)} &= \prod_{d|n}\prod_{j=1}^{n/d}\left(x - z_{n/d}^j\right)^{\mu(d)} \\
&= \prod_{d|n}\prod_{j=1}^{n/d}\left(x - z_n^{dj}\right)^{\mu(d)} \\
&= \prod_{i=1}^{n}(x - z_n^i)^{\sum_{d|\gcd(n,i)}\mu(d)}.
\end{aligned}$$

Since $\sum_{d|n}\mu(d)$ is 0 when $n > 1$ and is 1 when $n = 1$ (Theorem 4.7 of [468]) the result follows. □

Exercise 6.1.3. Show that $\Phi_1(x) = x - 1, \Phi_2(x) = x + 1$, $\Phi_6(x) = x^2 - x + 1$ and $\Phi_l(x) = x^{l-1} + x^{l-2} + \cdots + x + 1$ if l is prime.

Exercise 6.1.4. Prove that if $p \mid n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$ and that if $p \nmid n$ then $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$. Prove that if n is odd then $\Phi_{2n}(x) = \Phi_n(-x)$.
[Hint: Use part 5 of Lemma 6.1.2.]

It is well-known that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$; we do not need this result so we omit the proof.

Lemma 6.1.5. *Let $n \in \mathbb{N}$. The greatest common divisor of the polynomials $(x^n - 1)/(x^d - 1)$ over all $1 \leq d < n$ such that $d \mid n$ is $\Phi_n(x)$.*

Proof: Define $I = \{d \in \mathbb{N} : 1 \leq d < n, d \mid n\}$. By part 3 of Lemma 6.1.2 we have $\Phi_n(x) = (x^n - 1)/f(x)$ where $f(x) = \prod_{d \in I}\Phi_d(x) = \operatorname{lcm}(x^d - 1 : d \in I)$. Hence

$$\Phi_n(x) = \frac{x^n - 1}{\operatorname{lcm}(x^d - 1 : d \in I)} = \gcd\left(\frac{x^n - 1}{x^d - 1} : d \in I\right).$$

□

[1] One can find elementary proofs of this fact in any book on polynomials.

Definition 6.1.6. Let $n \in \mathbb{N}$ and q a prime power. Define the **cyclotomic subgroup** $G_{q,n}$ to be the subgroup of $\mathbb{F}_{q^n}^*$ of order $\Phi_n(q)$.

The subgroups $G_{q,n}$ are of interest as most elements of $G_{q,n}$ do not lie in any subfield of $\mathbb{F}_{q^n}$ (see Corollary 6.2.3 below). In other words, $G_{q,n}$ is the "hardest part" of $\mathbb{F}_{q^n}^*$ from the point of view of the DLP. Note that $G_{q,n}$ is trivially an algebraic group, by virtue of being a subgroup of the algebraic group $\mathbb{F}_{q^n}^* = G_m(\mathbb{F}_{q^n})$ (see Example 5.1.5). The goal of this subject area is to develop compact representations for the groups $G_{q,n}$ and efficient methods to compute with them.

The two most important cases are $G_{q,2}$, which is the subgroup of $\mathbb{F}_{q^2}^*$ of order $q+1$, and $G_{q,6}$, which is the subgroup of $\mathbb{F}_{q^6}^*$ of order $q^2 - q + 1$. We give compact representations of these groups in Sections 6.3 and 6.4.

6.2 Algebraic Tori

Algebraic tori are a classical object in algebraic geometry and their relevance to cryptography was first explained by Rubin and Silverberg [503]. An excellent survey of this area is [504].

Recall from Theorem 5.7.7 that the Weil restriction of scalars of $\mathbb{A}^1$ with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$ is $\mathbb{A}^n$. Let $n > 1$ and let $f : \mathbb{A}^n(\mathbb{F}_q) \to \mathbb{F}_{q^n}$ be a bijective $\mathbb{F}_q$-linear function (e.g., corresponding to the fact that $\mathbb{F}_{q^n}$ is a vector space of dimension n over $\mathbb{F}_q$). For any $d \mid n$ define the norm $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = \prod_{i=0}^{n/d-1} g^{q^{di}}$. The equation $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(f(x_1, \ldots, x_n)) = 1$ defines an algebraic set in $\mathbb{A}^n$.

Definition 6.2.1. The **algebraic torus**[2] $\mathbb{T}_n$ is the algebraic set

$$V(\{\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(f(x_1, \ldots, x_n)) - 1 : 1 \leq d < n, d \mid n\}) \subset \mathbb{A}^n.$$

Note that there is a group operation on $\mathbb{T}_n(\mathbb{F}_q)$, given by polynomials, inherited from multiplication in $\mathbb{F}_{q^n}^*$. Hence (at least, ignoring for the moment the inverse map) $\mathbb{T}_n(\mathbb{F}_q)$ satisfies our informal definition of an algebraic group.

Lemma 6.2.2. *Let the notation be as above.*

1. $G_{q,n} = \{g \in \mathbb{F}_{q^n}^* : \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = 1$ *for all* $1 \leq d < n$ *such that* $d \mid n\}$.
2. $\mathbb{T}_n(\mathbb{F}_q)$ *is isomorphic as a group to* $G_{q,n}$.
3. $\#\mathbb{T}_n(\mathbb{F}_q) = \Phi_n(q)$.

Proof: For the first statement note that

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = \prod_{i=0}^{n/d-1} g^{q^{di}} = g^{(q^n-1)/(q^d-1)}.$$

Recall that $\Phi_n(q) \mid (q^n - 1)/(q^d - 1)$ and, by Lemma 6.1.5, $\gcd((q^n - 1)/(q^d - 1) : 1 \leq d < n, d \mid n) = \Phi_n(q)$. Hence, all the norms are 1 if and only if $g^{\Phi_n(q)} = 1$, which proves the first claim. The second and third statements follow immediately. □

Corollary 6.2.3. *Let* $n \in \mathbb{N}$ *and* q *a prime power. Suppose* $g \in G_{q,n}$ *has order* $r > n$. *Then* g *does not lie in any proper subfield of* $\mathbb{F}_{q^n}$.

[2]The plural of "torus" is "tori".

Proof: Suppose $g \in \mathbb{F}_{q^d}$ for some $1 \leq d < n$ such that $d \mid n$. Then $1 = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = g^{n/d}$, but this contradicts the order of g being $> n$. □

It follows from the general theory that $\mathbb{T}_n$ is irreducible and of dimension $\varphi(n)$. Hence, $\mathbb{T}_n$ is a variety and one can speak of birational maps from $\mathbb{T}_n$ to another algebraic set. We refer to Section 5 of [504] for details and references.

Definition 6.2.4. The torus $\mathbb{T}_n$ is **rational** if there is a birational map from $\mathbb{T}_n$ to $\mathbb{A}^{\varphi(n)}$.

If $\mathbb{T}_n$ is rational then $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ is a compact representation for $G_{q,n}$. Performing discrete logarithm cryptography by transmitting elements of $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ is called **torus based cryptography** and was developed by Rubin and Silverberg [503].

If $\mathbb{T}_n$ is rational then there is an induced "partial" group operation on $\mathbb{A}^{\varphi(n)}$, given by rational functions. This is not an algebraic group in general since there is not usually a one-to-one correspondence between $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ and $G_{q,n}$. Nevertheless, "most" of the elements of the group $G_{q,n}$ appear in $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ and, for many cryptographic purposes, the partial group law is sufficient. In practice, however, working with the partial group operation on $\mathbb{A}^{\varphi(n)}$ is not usually as efficient as using other representations for the group. The main application of tori is therefore the compact representation for elements of certain subgroups of $\mathbb{F}_{q^n}^*$.

It is not known if $\mathbb{T}_n$ is rational for all $n \in \mathbb{N}$ (we refer to [504] for more details and references about when $\mathbb{T}_n$ is known to be rational). The cryptographic applications of $\mathbb{T}_2$ and $\mathbb{T}_6$ rely on the well-known fact that these tori are both rational. The details are given in the following sections.

As mentioned in Section 4.3, sometimes it is convenient to consider quotients of algebraic groups by an equivalence relation. In the following sections we describe algebraic group quotients (more commonly known by the names LUC and XTR) for $G_{q,2}$ and $G_{q,6}$, but we construct them directly without using the theory of tori.

6.3 The Group $G_{q,2}$

Define $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ where

$$\theta^2 + A\theta + B = 0 \tag{6.1}$$

for some $A, B \in \mathbb{F}_q$ such that $x^2 + Ax + B$ is irreducible over $\mathbb{F}_q$ (e.g., if q is odd then $A^2 - 4B$ is not a square in $\mathbb{F}_q$). In practice there are performance advantages from using a simpler equation, such as $\theta^2 = B$ or $\theta^2 + \theta = B$ where B is "small". Every element of $\mathbb{F}_{q^2}$ is of the form $u + v\theta$ where $u, v \in \mathbb{F}_q$.

The **conjugate** of θ is $\overline{\theta} = \theta^q = -A - \theta$. We have $\theta + \overline{\theta} = -A$ and $\theta\overline{\theta} = B$. The conjugate of an element $g = u + v\theta \in \mathbb{F}_{q^2}$ is $u + v\overline{\theta}$ and g has **norm**

$$\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = (u + v\theta)(u + v\overline{\theta}) = u^2 - Auv + Bv^2. \tag{6.2}$$

The group $G_{q,2}$ is defined to be the set of elements $g \in \mathbb{F}_{q^2}$ such that $g^{q+1} = 1$. Equivalently this is the set of $u + v\theta$ such that $u^2 - Auv + Bv^2 = 1$.

Exercise 6.3.1. Show that if $g = u + v\theta \in G_{q,2}$ then $g^{-1} = g^q = u + v\overline{\theta} = (u - Av) + (-v)\theta$. Hence, inversion in $G_{q,2}$ is cheaper than a general group operation (especially if $A = 0$ or A is "small").

Exercise 6.3.2. Suppose q is not a power of 2. Suppose $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ where $\theta^2 + A\theta + B = 0$ and multiplying an element of $\mathbb{F}_q$ by A or B has negligible cost (e.g., $A = 0$ and $B = 1$). Show that one can compute a product (respectively: squaring; inversion) in $\mathbb{F}_{q^2}^*$

using 3 multiplications (respectively: 3 squarings; one inversion, 3 multiplications and 2 squarings) in $\mathbb{F}_q$. Ignore the cost of additions and multiplication by small constants such as 2 (since they are significantly faster to perform than multiplications etc).

Exercise 6.3.3.★ Suppose $q \equiv 3 \pmod 4$ is prime. Show that one can represent $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(\theta)$ where $\theta^2 + 1 = 0$. Show that, using this representation, one can compute a product (respectively: squaring; inversion; square root) in $\mathbb{F}_{q^2}^*$ using 3 multiplications (respectively: 2 multiplications; one inversion, 2 squarings and 2 multiplications; 2 square roots, one inversion, one Legendre symbol, one multiplication and 2 squarings) in $\mathbb{F}_q$. Ignore the cost of additions.

6.3.1 The Torus $\mathbb{T}_2$

Recall that $G_{q,2}$ can be represented as the $\mathbb{F}_q$-points of the algebraic torus $\mathbb{T}_2 = V(\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(f(x,y)) - 1) \subset \mathbb{A}^2$, where $f : \mathbb{A}^2(\mathbb{F}_q) \to \mathbb{F}_{q^2}$. By equation (6.2), an affine equation for $\mathbb{T}_2$ is $V(x^2 - Axy + By^2 - 1)$. Being a conic with a rational point, it is immediate from general results in geometry (see Exercise 5.5.14 for a special case) that $\mathbb{T}_2$ is birational with $\mathbb{A}^1$.

The next two results give a more algebraic way to show that $\mathbb{T}_2$ is rational. Rather than directly constructing a birational map from $\mathbb{T}_2$ to $\mathbb{A}^1$ we go via $G_{q,2}$. Lemma 6.3.4 provides a map from $\mathbb{A}^1(\mathbb{F}_q)$ to $G_{q,2}$ while Lemma 6.3.6 provides a map from $G_{q,2}$ to $\mathbb{A}^1(\mathbb{F}_q)$.

Lemma 6.3.4. *The set $G_{q,2} \subseteq \mathbb{F}_{q^2}^*$ is equal to the set*

$$\{(a+\theta)/(a+\overline{\theta}) : a \in \mathbb{F}_q\} \cup \{1\}.$$

Proof: Clearly, every element $g = (a+\theta)/(a+\overline{\theta})$ satisfies $g\overline{g} = 1$. It is also easy to check that $(a+\theta)/(a+\overline{\theta}) = (a'+\theta)/(a'+\overline{\theta})$ implies $a = a'$. Hence we have obtained q distinct elements of $G_{q,2}$. The missing element is evidently 1 and the result follows. □

Exercise 6.3.5. Suppose q is odd. Determine the value for a such that $(a+\theta)/(a+\overline{\theta}) = -1$.

Lemma 6.3.6. *Let $g = u + v\theta \in G_{q,2}$, $g \neq \pm 1$. Then $u + v\theta = (a+\theta)/(a+\overline{\theta})$ for the unique value $a = (u+1)/v$.*

Proof: The value a must satisfy

$$a + \theta = (u+v\theta)(a+\overline{\theta}) = ua + u\overline{\theta} + av\theta + v\theta\overline{\theta} = (ua - Au + Bv) + \theta(av - u).$$

Equating coefficients of θ gives $av = u + 1$ and the result follows as long as $v \neq 0$ (i.e., $g \neq \pm 1$). □

The above results motivate the following definition.

Definition 6.3.7. The $\mathbb{T}_2$ **decompression map** is the function $\mathrm{decomp}_2 : \mathbb{A}^1 \to G_{q,2}$ given by $\mathrm{decomp}_2(a) = (a+\theta)/(a+\overline{\theta})$.

The $\mathbb{T}_2$ **compression map** is the function $\mathrm{comp}_2 : G_{q,2} - \{1, -1\} \to \mathbb{A}^1$ given by $\mathrm{comp}_2(u + v\theta) = (u+1)/v$.

Lemma 6.3.8. *The maps* comp_2 *and* decomp_2 *are injective. The compression map is not defined at* ± 1. *If* $g \in G_{q,2} - \{1, -1\}$ *then* $\mathrm{decomp}_2(\mathrm{comp}_2(g)) = g$.

Exercise 6.3.9. Prove Lemma 6.3.8.

Alert readers will notice that the maps comp_2 and decomp_2 are between $G_{q,2}$ and $\mathbb{A}^1$, rather than between $\mathbb{T}_2$ and $\mathbb{A}^1$. For completeness we now give a map from $G_{q,2}$ to $\mathbb{T}_2 \subset \mathbb{A}^2$. From this one can deduce birational maps between $\mathbb{T}_2$ and $\mathbb{A}^1$, which prove that $\mathbb{T}_2$ is indeed rational.

Lemma 6.3.10. *An element of the form $(a+\theta)/(a+\overline{\theta}) \in G_{q,2}$ corresponds to the element*

$$\left(\frac{a^2 - B}{a^2 - aA + B}, \frac{2a - A}{a^2 - aA + B} \right)$$

of $\mathbb{T}_2$.

Proof: Let (x, y) be the image point in $\mathbb{T}_2$. In other words

$$(a + \theta)/(a + \overline{\theta}) = x + y\theta$$

and so $a + \theta = (x + y\theta)(a + \overline{\theta}) = (ax + By - Ax) + \theta(ay - x)$. Equating coefficients gives the result. □

Exercise 6.3.11. Prove that $\mathbb{T}_2$ is rational.

We now present the partial group operations on $\mathbb{A}^1$ induced by the map from $\mathbb{A}^1$ to $G_{q,2}$. We stress that $\mathbb{A}^1$ is not a group with respect to these operations, since the identity element of $G_{q,2}$ is not represented as an element of $\mathbb{A}^1$.

Lemma 6.3.12. *Let the notation be as above. For $a, b \in \mathbb{A}^1$ define $a \star b = (ab - B)/(a + b - A)$ and $a' = A - a$. Then $a \star b$ is the product and a' is the inverse for the partial group law.*

Proof: The partial group law on $\mathbb{A}^1$ is defined by $\text{comp}_2(\text{decomp}_2(a)\text{decomp}_2(b))$. Now,

$$\text{decomp}_2(a)\text{decomp}_2(b) = \left(\frac{a + \theta}{a + \overline{\theta}} \right) \left(\frac{b + \theta}{b + \overline{\theta}} \right) = \frac{ab - B + (a + b - A)\theta}{ab - B + (a + b - A)\overline{\theta}}.$$

The formula for $a \star b$ follows.

Similarly,

$$\text{decomp}_2(a)^{-1} = \frac{a + \overline{\theta}}{a + \theta} = \frac{a + (-A - \theta)}{a + (-A - \overline{\theta})},$$

which gives the formula for a'. □

It follows that one can compute directly with the compressed representation of elements of $\mathbb{T}_2(\mathbb{F}_q)$. Note that computing the partial group law on $\mathbb{A}^1$ requires an inversion, so is not very efficient. For cryptographic applications one is usually computing $\text{comp}_2(g^n)$ from $\text{comp}_2(g)$; to do this one decompresses to obtain $g \in G_{q,2}$, then computes g^n using any one of a number of techniques, and finally applies comp_2 to obtain a compact representation.[3]

6.3.2 Lucas Sequences

Lucas[4] sequences can be used for efficient computation in quadratic fields. We give the details for $G_{q,2} \subset \mathbb{F}_{q^2}^*$. The name LUC cryptosystem is applied to any cryptosystem using Lucas sequences to represent elements in an algebraic group quotient of $G_{q,2}$. Recall the **trace** $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = g + g^q$ for $g \in \mathbb{F}_{q^2}$.

[3] This is analgous to using projective coordinates for efficient elliptic curve arithmetic; see Exercise 9.1.5.

[4] They are named after Edouard Lucas (1842-1891); who apparently died due to a freak accident involving broken crockery. Lucas sequences were used for primality testing and factorisation before their cryptographic application was recognised.

Definition 6.3.13. Let $g \in \mathbb{F}_{q^2}^*$ satisfy $g^{q+1} = 1$. For $i \in \mathbb{Z}$ define $V_i = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^i)$.

Lemma 6.3.14. *Let $g = v_1 + w_1\theta$ with $v_1, w_1 \in \mathbb{F}_q$ and θ as in equation (6.1). Suppose $g^{q+1} = 1$ and let V_i be as in Definition 6.3.13. Then, for $i, j \in \mathbb{Z}$,*

1. $V_0 = 2$ *and* $V_1 = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = 2v_1 - Aw_1$.
2. $V_{-i} = V_i$.
3. $V_{i+1} = V_1V_i - V_{i-1}$.
4. $V_{2i} = V_i^2 - 2$.
5. $V_{2i-1} = V_iV_{i-1} - V_1$.
6. $V_{2i+1} = V_iV_{i+1} - V_1$.
7. $V_{2i+1} = V_1V_i^2 - V_iV_{i-1} - V_1$.
8. $V_{i+j} = V_iV_j - V_{i-j}$.

Proof: Let $\overline{g} = g^q = v_1 + w_1\overline{\theta}$. Then $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = g + \overline{g} = (v_1 + w_1\theta) + (v_1 + w_1(-\theta - A)) = 2v_1 - Aw_1$. Similarly, $g^0 = 1$ and the first statement is proven. The second statement follows from $g^{-1} = \overline{g}$. Statements 3 to 6 are all special cases of statement 8, which follows from the equation

$$V_{i+j} = g^{i+j} + \overline{g}^{i+j} = (g^i + \overline{g}^i)(g^j + \overline{g}^j) - g^j\overline{g}^j(g^{i-j} + \overline{g}^{i-j}).$$

(An alternative proof of Statement 3 is to use the fact that g satisfies $g^2 = V_1g - 1$.) Statement 7 then follows from 3 and 6. □

Exercise 6.3.15. Define $U_i = (g^i - \overline{g}^i)/(g - \overline{g})$. Prove that $U_{i+1} = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)U_i - U_{i-1}$, $U_{2i} = V_iU_i$, $U_{i+j} = U_iU_{j+1} - U_{i-1}U_j$.

Definition 6.3.16. Denote by $G_{q,2}/\langle\sigma\rangle$ the set of equivalence classes of $G_{q,2}$ under the equivalence relation $g \equiv \sigma(g) = g^q = g^{-1}$. Denote the class of $g \in G_{q,2}$ by $[g] = \{g, g^q\}$.

The main observation is that $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^q)$ and so a class $[g]$ can be identified with the value $V = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)$. This motivates Definition 6.3.18. When q is odd, the classes $[1]$ and $[-1]$ correspond to $V = 2$ and $V = -2$ respectively; apart from these cases, the other possible values for V are those for which the polynomial $x^2 - Vx + 1$ is irreducible over $\mathbb{F}_q$.

Exercise 6.3.17. Prove that if $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g')$ for $g, g' \in G_{q,2}$ then $g' \in \{g, g^q\}$. Hence, show that when q is odd there are $2 + (q-1)/2$ values for $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)$ over $g \in G_{q,2}$.

The set $G_{q,2}/\langle\sigma\rangle$ is not a group, however for a class $[g] \in G_{q,2}/\langle\sigma\rangle$ and $n \in \mathbb{N}$ one can define $[g]^n$ to be $[g^n]$.

Definition 6.3.18. Let $G'_{q,2} = \{\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) : g \in G_{q,2}\}$. For $V \in G'_{q,2}$ and $n \in \mathbb{N}$ define $[n]V = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^n)$ for any $g \in G_{q,2}$ such that $V = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)$.

It follows that we may treat the set $G'_{q,2}$ as an algebraic group quotient. One method to efficiently compute $[n]V$ for $n \in \mathbb{N}$ is to take a root $g \in \mathbb{F}_{q^2}$ of $x^2 - Vx + 1 = 0$, compute g^n in $\mathbb{F}_{q^2}$ using the square-and-multiply method, and then compute $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^n)$. However, we want to be able to compute $[n]V$ directly using an analogue of the square-and-multiply

method.[5] Lemma 6.3.14 shows that, although V_{2n} is determined by V_n and n, V_{n+1} is not determined by V_n alone. Hence it is necessary to develop an algorithm that works on a pair (V_n, V_{n-1}) of consecutive values. Such algorithms are known as **ladder methods**. One starts the ladder computation with $(V_1, V_0) = (V, 2)$.

Lemma 6.3.19. *Given (V_i, V_{i-1}) and V one can compute (V_{2i}, V_{2i-1}) (i.e., "squaring") or (V_{2i+1}, V_{2i}) (i.e., "square-and-multiply") in one multiplication, one squaring and two or three additions in $\mathbb{F}_q$.*

Proof: One must compute V_i^2 and $V_i V_{i-1}$ and then apply part 4 and either part 5 or 7 of Lemma 6.3.14. □

Exercise 6.3.20. Write the ladder algorithm for computing $[n]V$ using Lucas sequences in detail.

The storage requirement of the ladder algorithm is the same as when working in $\mathbb{F}_{q^2}$, although the output value is compressed to a single element of $\mathbb{F}_q$. Note however that computing a squaring alone in $\mathbb{F}_{q^2}$ already requires more computation (at least when q is not a power of 2) than Lemma 6.3.19.

We have shown that for $V \in G'_{q,2}$ one can compute $[n]V$ using polynomial operations starting with the pair $(V, 2)$. Since $G'_{q,2}$ is in one-to-one correspondence with $G_{q,2}/\langle\sigma\rangle$, it is natural to consider $G'_{q,2}$ as being an algebraic group quotient.

Performing discrete logarithm based cryptography in $G'_{q,2}$ is sometimes called the LUC cryptosystem.[6] To solve the discrete logarithm problem in $G'_{q,2}$ one usually lifts the problem to the **covering group** $G_{q,2} \subset \mathbb{F}_{q^2}^*$ by taking one of the roots in $\mathbb{F}_{q^2}$ of the polynomial $x^2 - Vx + 1$.

Example 6.3.21. Define $\mathbb{F}_{37^2} = \mathbb{F}_{37}(\theta)$ where $\theta^2 - 3\theta + 1 = 0$. The element $g = -1 + 3\theta$ has order 19 and lies in $G_{37,2}$. Write $V = \mathrm{Tr}_{\mathbb{F}_{37^2}/\mathbb{F}_{37}}(g) = 7$. To compute $[6]V$ one uses the addition chain $(V_1, V_0) = (7, 2) \to (V_3, V_2) = (26, 10) \to (V_6, V_5) = (8, 31)$; this is because $6 = (110)_2$ in binary so the intermediate values for i are $(1)_2 = 1$ and $(11)_2 = 3$.

Exercise 6.3.22. Using the same values as Example 6.3.21 compute $[10]V$.

Exercise 6.3.23.★ Compare the number of $\mathbb{F}_q$ multiplications and squarings to compute a squaring or a squaring-and-multiplication in the quotient $G'_{q,2}$ using Lucas sequences with the cost for general arithmetic in $G_{q,2} \subset \mathbb{F}_{q^2}$.

6.4 The Group $G_{q,6}$

The group $G_{q,6}$ is the subgroup of $\mathbb{F}_{q^6}^*$ of order $\Phi_6(q) = q^2 - q + 1$. The natural representation of elements of $G_{q,6}$ requires 6 elements of $\mathbb{F}_q$.

Assume (without loss of generality) that $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(\theta)$ where $\theta \in \mathbb{F}_{q^2}$ and $\theta^2 + A\theta + B = 0$ for some $A, B \in \mathbb{F}_q$.

[5] In practice it is often more efficient to use other processes instead of the traditional square-and-multiply method. We refer to Chapter 3 of [579] for more details.

[6] The original LUC cryptosystem due to Smith and Lennon [574] was using Lucas sequences modulo a composite integer N; we refer to Section 6.6 for further discussion. The finite field version is only very briefly mentioned in [574], but is further developed in [575].

6.4.1 The Torus $\mathbb{T}_6$

Recall that $\mathbb{T}_6$ is a two dimensional algebraic set in $\mathbb{A}^6$ defined by the intersection of the kernels of the norm maps $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}$ and $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$. It is known that $\mathbb{T}_6$ is rational, so the goal is to represent elements of $G_{q,6}$ using only two elements of $\mathbb{F}_q$.

The kernel of the norm map $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}$ is identified with $\mathbb{T}_2(\mathbb{F}_{q^3}) \subset \mathbb{A}^2(\mathbb{F}_{q^3})$. As in Section 6.3.1, $\mathbb{T}_2$ is birational to $\mathbb{A}^1(\mathbb{F}_{q^3})$ (which can then be identified with $\mathbb{A}^3(\mathbb{F}_q)$) via the map $\mathrm{decomp}_2(a) = (a+\theta)/(a+\overline{\theta})$ where $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(\theta)$. The next step is to compute the kernel of the norm map with respect to $\mathbb{F}_{q^6}/\mathbb{F}_{q^2}$.

Lemma 6.4.1. *The Weil restriction of the kernel of* $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$ *on* $\mathbb{T}_2(\mathbb{F}_{q^3})$ *is birational with a quadratic hypersurface* U *in* $\mathbb{A}^3(\mathbb{F}_q)$.

Proof: First, we represent an element of $\mathbb{T}_2(\mathbb{F}_{q^3}) - \{1\}$ as a single value $a \in \mathbb{F}_{q^3}$. Now impose the norm equation on the image of $\mathrm{decomp}_2(a)$

$$\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\mathrm{decomp}_2(a)) = \left(\frac{a+\theta}{a+\overline{\theta}}\right)\left(\frac{a+\theta}{a+\overline{\theta}}\right)^{q^2}\left(\frac{a+\theta}{a+\overline{\theta}}\right)^{q^4} = \left(\frac{a+\theta}{a+\overline{\theta}}\right)\left(\frac{a^{q^2}+\theta}{a^{q^2}+\overline{\theta}}\right)\left(\frac{a^{q^4}+\theta}{a^{q^4}+\overline{\theta}}\right).$$

To solve $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\mathrm{decomp}_2(a)) = 1$ one clears the denominator and equates coefficients of θ, giving

$$\begin{aligned} & a^{1+q^2+q^4} + \theta(a^{1+q^2} + a^{1+q^4} + a^{q^2+q^4}) + \theta^2(a + a^{q^2} + a^{q^4}) + \theta^3 \\ = \;& a^{1+q^2+q^4} + \overline{\theta}(a^{1+q^2} + a^{1+q^4} + a^{q^2+q^4}) + \overline{\theta}^2(a + a^{q^2} + a^{q^4}) + \overline{\theta}^3. \end{aligned}$$

The crucial observations are that the cubic terms in a cancel and that $\theta^2 - \overline{\theta}^2 = -A(\theta - \overline{\theta})$ and $\theta^3 - \overline{\theta}^3 = (A^2 - B)(\theta - \overline{\theta})$. Hence we obtain a single equation in a.

Now, we identify $a \in \mathbb{A}^1(\mathbb{F}_{q^3})$ with a 3-tuple $(a_0, a_1, a_2) \in \mathbb{A}^3(\mathbb{F}_q)$. Using the fact that $a \mapsto a^q$ corresponds to an $\mathbb{F}_q$-linear map on $\mathbb{A}^3(\mathbb{F}_q)$, it follows that the single equation given above is actually a quadratic polynomial in (a_0, a_1, a_2). In other words, the values (a_0, a_1, a_2) corresponding to solutions of the norm equation are points on a quadratic hypersurface in $\mathbb{A}^3(\mathbb{F}_q)$, which we call U. □

The general theory (see Rubin and Silverberg [504]) implies that U is irreducible, but we do not prove this. It remains to give a rational parameterisation $p_U : U \to \mathbb{A}^2$ of the hypersurface. This is done using essentially the same method as Example 5.5.14.

Lemma 6.4.2. *An irreducible quadratic hypersurface* $U \subset \mathbb{A}^3$ *over a field* $\Bbbk$ *is birational over* $\Bbbk$ *to* $\mathbb{A}^2$.

Proof: (Sketch) Let $P = (x_P, y_P, z_P)$ be a point on U and change variables so that the tangent plane T to U at P is $x = x_P$. We have not discussed T in this book; the only property we need is that T contains every line through P that is not contained in U and that intersects U at P with multiplicity 2.

Let $Q \in U(\Bbbk)$ be such that $Q \neq P$ and such that the line between P and Q is not contained in U (this is generically the case for an irreducible quadratic hypersurface). Then the line between P and Q does not lie in T and so is given by an equation of the form[7]

$$(x, y, z) = P + t(1, a, b) \tag{6.3}$$

for some $a, b \in \Bbbk$ (in other words, the equations $x = x_P + t, y = y_P + at$, etc). Such a line hits U at precisely one point $Q \in U(\Bbbk)$ with $Q \neq P$. Writing $U = V(F(x, y, z))$ it

[7]Here, and below, $P + Q$ denotes the usual coordinate-wise addition of 3-tuples over a field.

follows that $F(x_P + t, y_P + at, z_P + bt) = 0$ has the form $t(h(a,b)t - g(a,b)) = 0$ for some quadratic polynomial $h(a,b) \in \Bbbk[a,b]$ and some linear polynomial $g(a,b) \in \Bbbk[a,b]$. Hence we have a rational map $\mathbb{A}^2 \to U$ given by

$$(a,b) \mapsto P + \tfrac{g(a,b)}{h(a,b)}(1,a,b).$$

The inverse is the rational map

$$p_U(x_Q, y_Q, z_Q) = ((y_Q - y_P)/(x_Q - x_P), (z_Q - z_P)/(x_Q - x_P))$$

such that $p_U : U \to \mathbb{A}^2$. □

Recall the map $\mathrm{comp}_2 : G_{q^3,2} \to \mathbb{A}^1(\mathbb{F}_{q^3})$ from the study of $\mathbb{T}_2$. We identify $\mathbb{A}^1(\mathbb{F}_{q^3})$ with $\mathbb{A}^3(\mathbb{F}_q)$. The image of comp_2 is U, which is birational via p_U to $\mathbb{A}^2$. This motivates the following definition.

Definition 6.4.3. The $\mathbb{T}_6$ **compression map** is $\mathrm{comp}_6 : G_{q,6} \to \mathbb{A}^2$ is given by $\mathrm{comp}_6 = p_U \mathrm{comp}_2$. The inverse of comp_6 is the $\mathbb{T}_6$ **decompression map** $\mathrm{decomp}_6 = \mathrm{decomp}_2\, p_U^{-1}$.

Example 6.4.4. Let $q \equiv 2, 5 \pmod 9$ be an odd prime power so that $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_9)$ where ζ_9 is a primitive 9-th root of unity (see Exercise 6.4.5). Let $\theta = \zeta_9^3$ and $\alpha = \zeta_9 + \zeta_9^{-1}$. Then $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ and $\mathbb{F}_{q^3} = \mathbb{F}_q(\alpha)$. Note that $\alpha^3 - 3\alpha + 1 = 0$. Identify $\mathbb{A}^3(\mathbb{F}_q)$ with $\mathbb{A}^1(\mathbb{F}_{q^3})$ by $f : (x,y,z) \mapsto x + y\alpha + z(\alpha^2 - 2)$. As in the proof of Lemma 6.4.1 one can verify that the equation

$$\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}((f(x,y,z) + \theta)/(f(x,y,z) + \overline{\theta})) = 1$$

is equivalent to

$$F(x,y,z) = x^2 - x - y^2 + yz - z^2 = 0.$$

Denote by U the hyperplane $V(F(x,y,z))$ in $\mathbb{A}^3$. Let $P = (0,0,0)$. The tangent plane to U at P is given by the equation $x = 0$. Note that, since -3 is not a square in $\mathbb{F}_q$, the only solution to $F(0,y,z) = 0$ over $\mathbb{F}_q$ is $(y,z) = (0,0)$ (but this statement is not true over $\overline{\mathbb{F}}_q$; U contains, for example, the line $(0, -\zeta_3 t, t)$). Given $a, b \in \mathbb{F}_q$ the line (t, at, bt) hits U at $t = 0$ and

$$t = 1/(1 - a^2 + ab - b^2).$$

One therefore defines a birational map $g : \mathbb{A}^2 \to \mathbb{A}^3$ by

$$g : (a,b) \mapsto \left(\frac{1}{1 - a^2 + ab - b^2}, \frac{a}{1 - a^2 + ab - b^2}, \frac{b}{1 - a^2 + ab - b^2} \right).$$

Finally, the map decomp_6 from $\mathbb{A}^2$ to $G_{q,6}$ is $(f(g(a,b)) + \theta)/((f(g(a,b)) + \overline{\theta})$. It is then straightforward to compute comp_6.

Exercise 6.4.5. Let q be a prime power and ζ_9 a primitive 9-th root of unity in $\overline{\mathbb{F}}_q$. Show that $\mathbb{F}_q(\zeta_9) = \mathbb{F}_{q^6}$ if and only if $q \equiv 2, 5 \pmod 9$.

In principle one can write down the partial group operations on $\mathbb{A}^2$ induced from $G_{q,6}$, but this is not an efficient way to compute. Instead, to compute $\mathrm{comp}_6(g^n)$ from $\mathrm{comp}_6(g)$ one decompresses to obtain an element $g \in G_{q,6}$ (or $G_{q^3,2}$), computes g^n, and then compresses again.

6.4.2 XTR

An excellent survey of work in this area is the thesis of Stam [579].

The Galois group of $\mathbb{F}_{q^6}/\mathbb{F}_{q^2}$ is cyclic of order 3 and generated by the q^2-power Frobenius map σ. One can consider the set $G_{q,6}/\langle\sigma\rangle = G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ of equivalence classes under the relation $g \equiv \sigma^i(g)$ for $0 \leq i \leq 2$. This gives an algebraic group quotient. which was named **XTR**[8] by Lenstra and Verheul. The goal is to give a compressed representation for this quotient; this is achieved by using the trace with respect to $\mathbb{F}_{q^6}/\mathbb{F}_{q^2}$.

Lemma 6.4.6. *Let $g \in G_{q,6}$. Let $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g) \in \mathbb{F}_{q^2}$. Then $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g) = g^{1+q^2+q^4} = 1$ and the characteristic polynomial of g over $\mathbb{F}_{q^2}$ is $\chi_g(x) = x^3 - tx^2 + t^q x - 1$.*

Proof: The first claim follows since $g^{q^2-q+1} = 1$ and $(q^2-q+1)(q^2+q+1) = q^4+q^2+1$. Now, write $(x-g)(x-g^{q^2})(x-g^{q^4}) = x^3 - tx^2 + sx - 1$. Since this polynomial is fixed by $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ it follows that $s, t \in \mathbb{F}_{q^2}$. Indeed, $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g) = g + g^{q^2} + g^{q^4} = g + g^{q-1} + g^{-q}$. Also

$$s = g^{1+q^2} + g^{1+q^4} + g^{q^2+q^4} = g^q + g^{1-q} + g^{-1}.$$

Finally, $s^q = g^{q^2} + g^{q^2-q} + g^{-q} = t$, from which we have $s = t^q$. □

This result shows that one can represent an equivalence class of $g \in G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ using a single element $t \in \mathbb{F}_{q^2}$, as desired. It remains to explain how to perform exponentiation in the quotient (as usual, the quotient structure is not a group and so it makes no sense to try to compute a general group operation on it).

Exercise 6.4.7. Write $f(x) = x^3 - tx^2 + t^q x - 1$ for $t \in \mathbb{F}_{q^2}$. Prove that if $f(a) = 0$ for $a \in \overline{\mathbb{F}}_q$ then $f(a^{-q}) = 0$. Hence prove that either $f(x)$ is irreducible over $\mathbb{F}_{q^2}$ or splits completely over $\mathbb{F}_{q^2}$.

Definition 6.4.8. Fix $g \in G_{q,6}$. For $n \in \mathbb{Z}$ write $t_n = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^n)$.

Lemma 6.4.9. *Let the notation be as above. Then, for $n, m \in \mathbb{Z}$,*

1. $t_{-n} = t_{nq} = t_n^q$.
2. $t_{n+m} = t_n t_m - t_m^q t_{n-m} + t_{n-2m}$.

Proof: We have $t_n = g^n + g^{n(q-1)} + g^{n(-q)}$ The first statement follows from the proof of Lemma 6.4.6, where it is proved that $t^q = g^q + g^{1-q} + g^{-1} = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^{-1})$.

For the second statement, an elementary calculation verifies that

$$\begin{aligned} t_n t_m - t_{n+m} &= (g^n + g^{n(q-1)} + g^{-nq})(g^m + g^{m(q-1)} + g^{-mq}) - (g^{n+m} + g^{(n+m)(q-1)} + g^{-(n+m)q}) \\ &= g^{n+m(q-1)} + g^{n-mq} + g^{n(q-1)+m} + g^{n(q-1)-mq} + g^{-nq+m} + g^{-nq+m(q-1)}. \end{aligned}$$

This is equal to $t_m^q t_n - t_{n-2m}$. □

It remains to give a ladder algorithm to compute t_n. In this case one can work with triples (t_{n+1}, t_n, t_{n-1}) of 'adjacent' values centered at t_n. This is the **XTR representation** of Lenstra and Verheul. Note that, given $t_1 = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g)$ one can compute the triple $(t_1, t_0, t_{-1}) = (t_1, 3, t_1^q)$. Given a triple (t_{n+1}, t_n, t_{n-1}) and t_1 one can compute the triple centered at t_{2n} or t_{2n+1} using the following exercise.

Exercise 6.4.10. Prove that

[8] XTR is an abbreviation for ECSTR, which stands for "Efficient and Compact Subgroup Trace Representation".

1. $t_{2n-1} = t_{n-1}t_n - t_1^q t_n^q + t_{n+1}^q$;
2. $t_{2n} = t_n^2 - 2t_n^q$;
3. $t_{2n+1} = t_{n+1}t_n - t_1 t_n^q + t_{n-1}^q$.

Exercise 6.4.11. If one uses triples (t_{n+1}, t_n, t_{n-1}) as above then what is the cost of a square or square-and-multiply in $G_{q,6}$?

Exercise 6.4.12.★ Give a more efficient ladder for XTR, for which the cost of squaring and square-and-multiply are the same.

In other words, one can compute $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^n)$ from $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g)$ using polynomial arithmetic and so $G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ is an algebraic group quotient. Performing discrete logarithm based cryptography in this setting is called the **XTR cryptosystem**. To solve the discrete logarithm problem in $G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ one usually lifts the problem to the **covering group** $G_{q,6} \subset \mathbb{F}_{q^6}^*$ by taking any root of the polynomial $x^3 - tx^2 + t^q x - 1$. For further details about efficient arithmetic using XTR we refer to [579].

Exercise 6.4.13. Represent $\mathbb{F}_{67^2}$ as $\mathbb{F}_{67}(i)$ where $i^2 = -1$. Given that $t_1 = \mathrm{Tr}_{\mathbb{F}_{67^6}/\mathbb{F}_{67^2}}(g) = 48 + 63i$ for some $g \in G_{67,6}$ compute $t_7 = \mathrm{Tr}_{\mathbb{F}_{67^6}/\mathbb{F}_{67^2}}(g^7)$.

Exercise 6.4.14. (The Gong-Harn cryptosystem [259]) Consider the quotient $G'_{q,3} = G_{q,3}/\langle\sigma\rangle$ where σ is the q-power Frobenius in $\mathbb{F}_{q^3}$. Fix $g \in G_{q,3}$ and define $t_n = g^n + g^{nq} + g^{nq^2} \in \mathbb{F}_q$. Show that the characteristic polynomial for g is $x^3 - t_1 x^2 + t_{-1}x - 1$. Hence, show that an element of $G'_{q,3}$ can be represented using two elements of $\mathbb{F}_q$. Show that

$$t_{n+m} = t_n t_m - t_{n-m}t_{-m} + t_{n-2m}$$

Hence develop a ladder algorithm for exponentiation in $G'_{q,3}$.

Exercise 6.4.15. (Shirase, Han, Hibino, Kim and Takagi [551]) Let $q = 3^m$ with m odd. Show that $(q - \sqrt{3q} + 1)(q + \sqrt{3q} + 1) = q^2 - q + 1$. Let $g \in \mathbb{F}_{3^{6m}}^*$ have order dividing $q - \sqrt{3q} + 1$. Show that $g^{q+1} = g^{\sqrt{3q}}$ and $g^{q^3+1} = 1$. Let $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g)$ and $s = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(g)$. Show that the roots of $x^2 - sx + s^{\sqrt{3q}}$ are t and t^q.

Hence, one can use s as a compressed representative for g; requiring only half the storage of XTR. To compute $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(g^n)$ one solves the quadratic to obtain t, computes $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^n)$ using the XTR formulae, and then performs the further compression.

6.5 Further Remarks

Granger and Vercauteren [266] have proposed an index calculus algorithm for $\mathbb{T}_n(\mathbb{F}_{p^m})$ where $m > 1$. Kohel [351] has shown that one might map the discrete logarithm problem in an algebraic torus $\mathbb{T}_n(\mathbb{F}_q)$ to the discrete logarithm problem in the generalised Jacobian (which is a certain type of divisor class group) of a singular hyperelliptic curve over $\mathbb{F}_q$. This latter problem might be attacked using an index calculus method such as Gaudry's algorithm (see Section 15.6.3). It seems this approach will not be faster than performing index calculus methods in $\mathbb{F}_{p^n}^*$, but further investigation would be of interest.

6.6 Algebraic Tori over Rings

Applications in factoring and primality testing motivate the study of tori over $\mathbb{Z}/N\mathbb{Z}$. As mentioned in Section 4.4, the simplest approach is to restrict to N being square-free

and to use the Chinese remainder theorem to define the groups. First we explain how to construct rings isomorphic to the direct product of finite fields.

Example 6.6.1. Let $N = \prod_{i=1}^{k} p_i$ be square-free. Let $F(x) = x^2 + Ax + B \in \mathbb{Z}[x]$ be a quadratic polynomial such that $F(x)$ is irreducible modulo p_i for all $1 \leq i \leq k$. Define $R = (\mathbb{Z}/N\mathbb{Z})[x]/(F(x))$. By the Chinese remainder theorem, $R \cong \oplus \mathbb{F}_{p_i^2}$. We will usually write θ for the image of x in R and $\overline{\theta} = -A - x = Bx^{-1}$.

Define $G_{N,2}$ to be the subgroup of R^* of order $\prod_{i=1}^{k}(p_i + 1)$ isomorphic to the direct sum of the groups $G_{p_i,2}$. Note that $G_{N,2}$ is not usually cyclic.

We would like to represent a "general" element of $G_{N,2}$ using a single element of $\mathbb{Z}/N\mathbb{Z}$. In other words, we would like to have a map from $\mathbb{Z}/N\mathbb{Z}$ to $G_{N.2}$. One can immediately apply Definition 6.3.7 to obtain the map $a \mapsto (a+\theta)/(a+\overline{\theta})$. Since the reduction modulo p_i of this map correctly maps to $G_{p_i,2}$, for each prime p_i, it follows that it correctly maps to $G_{N,2}$. Hence, we can identify $\mathbb{T}_2(\mathbb{Z}/N\mathbb{Z})$ with $\mathbb{Z}/N\mathbb{Z}$. The group operation $\star$ from Lemma 6.3.12 can also be applied in $\mathbb{Z}/N\mathbb{Z}$ and its correctness follows from the Chinese remainder theorem.

Note that the image of $\mathbb{Z}/N\mathbb{Z}$ in $G_{N.2}$ under this map has size $N = \prod p_i$, whereas $G_{N,2}$ has order $\prod_i (p_i + 1)$. Hence, there are many elements of $G_{N,2}$ that are missed by the decompression map. Note that these "missed" elements are those which correspond to the identity element of $G_{p_i,2}$ for at least one prime p_i. In other words, they are of the form $g = u + v\theta$ where $\gcd(v, N) > 1$.

Similarly, Lucas sequences can be used modulo N when N is square-free, and their properties follow from the properties modulo p_i for all prime factors p_i of N. However, one should be careful when interpreting the Galois theory. In Section 6.3.2 the non-trivial element of $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ is written as $\sigma(g) = g^q$, but this formulation does not naturally generalise to the ring R of Example 6.6.1. Instead, define $\sigma(u + v\theta) = u + v\overline{\theta}$ so that $\sigma : R \to R$ is a ring homomorphism and $\sigma(g) \pmod{p_i} = \sigma(g \pmod{p_i})$. One can then define the trace map $\mathrm{Tr}_{R/(\mathbb{Z}/N\mathbb{Z})}(g) = g + \sigma(g)$. The theory of Section 6.3.2 can then immediately be adapted to give Lucas sequences modulo N.

Exercise 6.6.2. Let $N = \prod_{i=1}^{k} p_i$ be a square-free integer and let R be as in Example 6.6.1. Let $g \in G_{N,2}$. Determine how many elements $h \in G_{N,2}$, in general, satisfy $\mathrm{Tr}_{R/(\mathbb{Z}/N\mathbb{Z})}(h) = \mathrm{Tr}_{R/(\mathbb{Z}/N\mathbb{Z})}(g)$. Show that roughly $N/2^k$ of the values $V \in \mathbb{Z}/N\mathbb{Z}$ correspond to the trace of an element in $G_{N,2}$.

Using similar methods to the above it is straightforward to adapt the torus $\mathbb{T}_6$ and XTR to the ring $\mathbb{Z}/N\mathbb{Z}$ when N is square-free. We leave the details to the reader.

Chapter 7

Curves and Divisor Class Groups

The purpose of this chapter is to develop some basic theory of divisors and functions on curves. We use this theory to prove that the set of points on an elliptic curve over a field is a group. There exist more elementary proofs of this fact, but I feel the approach via divisor class groups gives a deeper understanding of the subject.

We start by introducing the theory of singular points on varieties. Then we define uniformizers and the valuation of a function at a point on a curve. When working over a field $\Bbbk$ that is not algebraically closed it turns out to be necessary to consider not just points on C defined over $\Bbbk$ but also those defined over $\overline{\Bbbk}$ (alternatively, one can generalise the notion of point to places of degree greater than one; see [589] for details). We then discuss divisors, principal divisors and the divisor class group. The hardest result is that the divisor of a function has degree zero; the proof for general curves is given in Chapter 8. Finally, we discuss the "chord and tangent" group law on elliptic curves.

7.1 Non-Singular Varieties

The word "local" is used throughout analysis and topology to describe any property that holds in a neighbourhood of a point. We now develop some tools to study "local" properties of points of varieties. The algebraic concept of "localisation" is the main technique used.

Definition 7.1.1. Let X be a variety over $\Bbbk$. The **local ring** over $\Bbbk$ of X at a point $P \in X(\Bbbk)$ is

$$\mathcal{O}_{P,\Bbbk}(X) = \{f \in \Bbbk(X) : f \text{ is regular at } P\}.$$

Define

$$\mathfrak{m}_{P,\Bbbk}(X) = \{f \in \mathcal{O}_{P,\Bbbk}(X) : f(P) = 0\} \subseteq \mathcal{O}_{P,\Bbbk}(X).$$

When the variety X and field $\Bbbk$ are clear from the context we simply write $\mathcal{O}_P$ and $\mathfrak{m}_P$.

Lemma 7.1.2. *Let the notation be as above. Then*

1. $\mathcal{O}_{P,\Bbbk}(X)$ *is a ring;*
2. $\mathfrak{m}_{P,\Bbbk}(X)$ *is an* $\mathcal{O}_{P,\Bbbk}(X)$*-ideal;*
3. $\mathfrak{m}_{P,\Bbbk}(X)$ *is a maximal ideal;*
4. $\mathcal{O}_{P,\Bbbk}(X)$ *is a Noetherian local ring.*

Proof: The first three parts are straightforward. The fourth part follows from the fact that, if X is affine, $\mathcal{O}_{P,\Bbbk}(X)$ is the localisation of $\Bbbk[X]$ (which is Noetherian) at the maximal ideal $\mathfrak{m} = \{f \in \Bbbk[X] : f(P) = 0\}$. Lemma A.9.5 shows that the localisation of a Noetherian ring at a maximal ideal is Noetherian. Similarly, if X is projective then $\mathcal{O}_{P,\Bbbk}(X)$ is isomorphic to a localisation of $R = \Bbbk[\varphi_i^{-1}(X)]$ (again, Noetherian) where i is such that $P \in U_i$. □

Note that, for an affine variety X,

$$\Bbbk \subseteq \Bbbk[X] \subseteq \mathcal{O}_P(X) \subseteq \Bbbk(X).$$

Remark 7.1.3. We remark that $\mathcal{O}_{P,\Bbbk}(X)$ and $\mathfrak{m}_{P,\Bbbk}(X)$ are defined in terms of $\Bbbk(X)$ rather than any particular model for X. Hence, if $\phi : X \to Y$ is a birational map over $\Bbbk$ of varieties over $\Bbbk$ and ϕ is defined at $P \in X(\Bbbk)$ then $\mathcal{O}_{P,\Bbbk}(X)$ is isomorphic as a ring to $\mathcal{O}_{\phi(P),\Bbbk}(Y)$ (precisely, if $f \in \mathcal{O}_{\phi(P),\Bbbk}(Y)$ then $\phi^*(f) = f \circ \phi \in \mathcal{O}_{P,\Bbbk}(X)$). Similarly, $\mathfrak{m}_{P,\Bbbk}(X)$ and $\mathfrak{m}_{\phi(P),\Bbbk}(Y)$ are isomorphic.

Let X be a projective variety, let $P \in X(\Bbbk)$, and let i such that $P \in U_i$. By Corollary 5.4.9, $\Bbbk(X) \cong \Bbbk(\varphi_i^{-1}(X))$ and so $\mathcal{O}_{P,\Bbbk}(X) \cong \mathcal{O}_{\varphi_i^{-1}(P),\Bbbk}(\varphi_i^{-1}(X \cap U_i))$. It is therefore sufficient to consider affine varieties when determining local properties of a variety.

Example 7.1.4. Let $X \subseteq \mathbb{A}^n$ be an affine variety and suppose $P = (0, \ldots, 0) \in X(\Bbbk)$. Then $\mathcal{O}_P = \mathcal{O}_{P,\Bbbk}(X)$ is the set of equivalence classes

$$\{f_1(x_1, \ldots, x_n)/f_2(x_1, \ldots, x_n) : f_1, f_2 \in \Bbbk[x_1, \ldots, x_n], f_2(0, \ldots, 0) \neq 0\}.$$

In other words, the ratios of polynomials such that the denominators always have non-zero constant coefficient. Similarly, $\mathfrak{m}_P$ is the $\mathcal{O}_P$-ideal generated by $x_1, \ldots, x_n$. Since $f_1(x_1, \ldots, x_n)$ can be written in the form $f_1 = c + h(x_1, \ldots, x_n)$ where $c \in \Bbbk$ is the constant coefficient and $h(x_1, \ldots, x_n) \in \mathfrak{m}_P$, it follows that $\mathcal{O}_P/(x_1, \ldots, x_n) \cong \Bbbk$. Hence $\mathfrak{m}_P$ is a maximal ideal.

Exercise 7.1.5. Let $X \subseteq \mathbb{A}^n$ be a variety over $\Bbbk$ and let $P = (P_1, \ldots, P_n) \in X(\Bbbk)$. Consider the **translation** morphism $\phi : X \to \mathbb{A}^n$ given by $\phi(x_1, \ldots, x_n) = (x_1 - P_1, \ldots, x_n - P_n)$. Show that $\phi(P) = (0, \ldots, 0)$ and that ϕ maps X to a variety Y that is isomorphic to X. Show further that $\mathcal{O}_{\phi(P),\Bbbk}(\phi(X))$ is isomorphic to $\mathcal{O}_{P,\Bbbk}(X)$ as a $\Bbbk$-algebra.

We now introduce the notion of singular points and non-singular varieties. These concepts are crucial in our discussion of curves: on a non-singular curve one can define the order of a pole or zero of a function in a well-behaved way. Since singularity is a local property of a point (i.e., it can be defined in terms of $\mathcal{O}_P$) it is sufficient to restrict attention to affine varieties. Before stating the definition we need a lemma.

Lemma 7.1.6. *Let $X \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk$ and let $P \in X(\Bbbk)$. Then the quotient ring $\mathcal{O}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)$ is isomorphic to $\Bbbk$ as a $\Bbbk$-algebra. Furthermore the quotient $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ of $\mathcal{O}_{P,\Bbbk}(X)$-ideals is a $\Bbbk$-vector space of dimension at most n.*

Exercise 7.1.7. Prove Lemma 7.1.6.

As the following example shows, the dimension of the vector space $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ carries information about the local geometry of X at the point P.

Example 7.1.8. Let $X = \mathbb{A}^2$ and $P = (0,0) \in X(\Bbbk)$. We have $\mathfrak{m}_P = (x,y)$, $\mathfrak{m}_P^2 = (x^2, xy, y^2)$ and so the $\Bbbk$-vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$ has dimension 2. Note that X has dimension 2.

Let $X = V(y^2 - x) \subseteq \mathbb{A}^2$, which has dimension 1. Let $P = (0,0) \in X(\Bbbk)$. Then $\mathfrak{m}_P = (x,y)$ and $\{x,y\}$ span the $\Bbbk$-vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$. Since $x = y^2$ in $\Bbbk(X)$ it follows that $x \in \mathfrak{m}_P^2$ and so $x = 0$ in $\mathfrak{m}_P/\mathfrak{m}_P^2$. Hence $\mathfrak{m}_P/\mathfrak{m}_P^2$ is a one-dimensional vector space over $\Bbbk$ with basis vector y.

Consider now $X = V(y^2 - x^3) \subseteq \mathbb{A}^2$, which has dimension 1. Let $P = (0,0)$. Again, $\{x,y\}$ spans $\mathfrak{m}_P/\mathfrak{m}_P^2$ over $\Bbbk$. Unlike the previous example, there is no linear dependence among the elements $\{x,y\}$ (as there is no polynomial relation between x and y having a non-zero linear component). Hence $\mathfrak{m}_P/\mathfrak{m}_P^2$ has basis $\{x,y\}$ and has dimension 2.

Exercise 7.1.9. Let $X = V(x^4 + x + yx - y^2) \subseteq \mathbb{A}^2$ over $\Bbbk$ and let $P = (0,0)$. Find a basis for the $\Bbbk$-vector space $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$. Repeat the exercise for $X = V(x^4 + x^3 + yx - y^2)$.

Example 7.1.8 motivates the following definition. One important feature of this definition is that it is in terms of the local ring at a point P and so applies equally to affine and projective varieties.

Definition 7.1.10. Let X be a variety (affine or projective) over $\Bbbk$ and let $P \in X(\overline{\Bbbk})$ be point. Then P is **non-singular** if $\dim_{\overline{\Bbbk}} \mathfrak{m}_{P,\overline{\Bbbk}}(X)/\mathfrak{m}_{P,\overline{\Bbbk}}(X)^2 = \dim(X)$ and is **singular** otherwise.[1] The variety X is **non-singular** or **smooth** if every point $P \in X\left(\overline{\Bbbk}\right)$ is non-singular.

Indeed, it follows from the arguments in this section that if $P \in X(\Bbbk)$ then P is non-singular if and only if $\dim_{\Bbbk} \mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2 = \dim(X)$. The condition of Definition 7.1.10 is inconvenient for practical computation. Hence, we now give an equivalent condition (Corollary 7.1.13) for a point to be singular.

Suppose $X \subseteq \mathbb{A}^n$ is an affine variety and let $P = (0,\ldots,0)$. The key idea for Theorem 7.1.12 is to consider the map $\theta : \Bbbk[x_1,\ldots,x_n] \to \Bbbk^n$ defined by

$$\theta(f(x_1,\ldots,x_n)) = \left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P)\right).$$

This is essentially the same map as used in the proof of Lemma 7.1.6, but there it was defined on $\mathfrak{m}_{P,\Bbbk}(X) \subseteq \mathcal{O}_{P,\Bbbk}(X)$ whereas θ is defined on $\Bbbk[x_1,\ldots,x_n]$. Note that θ is $\Bbbk$-linear. Let $\mathfrak{m}_0(\mathbb{A}^n)$ be the $\Bbbk[x_1,\ldots,x_n]$-ideal $(x_1,\ldots,x_n)$. Then $\theta(\mathfrak{m}_0(\mathbb{A}^n)) = \Bbbk^n$, $\ker(\theta) = \mathfrak{m}_0(\mathbb{A}^n)^2$ and θ induces an isomorphism of $\Bbbk$-vector spaces $\mathfrak{m}_0(\mathbb{A}^n)/\mathfrak{m}_0(\mathbb{A}^n)^2 \cong \Bbbk^n$.

Lemma 7.1.11. *Let $X \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk$ and let $P \in X(\Bbbk)$. Define*[2] *$\mathfrak{m} = \{f \in \Bbbk[X] : f(P) = 0\}$. Then $\Bbbk[X]/\mathfrak{m} \cong \Bbbk$ and $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ as $\Bbbk$-vector spaces.*

[1] The dimension of the vector space $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ is always greater than or equal to $\dim(X)$, but we don't need this.

[2] We stress that $\mathfrak{m}$ is different from the ideals $\mathfrak{m}_{P,\Bbbk}(X)$ and $\mathfrak{m}_0(\mathbb{A}^n)$ above. One has $\mathfrak{m} \subseteq \mathfrak{m}_{P,\Bbbk}(X)$ and, for $P = (0,\ldots,0)$, $\mathfrak{m} = \mathfrak{m}_0(\mathbb{A}^n)/I_{\Bbbk}(X)$.

Proof: We assume without loss of generality that $P = (0, \ldots, 0)$. Since $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/I_\Bbbk(X)$ it follows that $\mathfrak{m}$ is the $\Bbbk[X]$-ideal $(x_1, \ldots, x_n)$. The first statement is then immediate. For the second statement note that one has $\Bbbk[X] \subseteq \mathcal{O}_{P,\Bbbk}(X)$, $\mathfrak{m} = \mathfrak{m}_{P,\Bbbk}(X) \cap \Bbbk[X]$ and $\mathfrak{m}_{P,\Bbbk}(X)$ is the $\mathcal{O}_{P,\Bbbk}(X)$-ideal generated by $\mathfrak{m}$. Similarly, $\mathfrak{m}^2 = \mathfrak{m}_{P,\Bbbk}(X)^2 \cap \Bbbk[X]$.

We now construct a ring isomorphism $\omega : \mathcal{O}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2 \rightarrow \Bbbk[X]/\mathfrak{m}^2$. Every $f \in \mathcal{O}_{P,\Bbbk}(X)$ has a representation f_1/f_2 where $f_1, f_2 \in \Bbbk[X]$ and $f_2(P) \neq 0$. Write $f_2 = a_0 + f_3 + f_4$ where $a_0 \in \Bbbk$, $a_0 \neq 0$, $f_3 \in \mathfrak{m}$ and $f_4 \in \mathfrak{m}^2$. Define $g = a_0^{-1} - a_0^{-2} f_3 \notin \mathfrak{m}$. Then $f_2 g - 1 \in \mathfrak{m}^2$ and so g is f_2^{-1} in $\Bbbk[X]/\mathfrak{m}^2$. It follows that

$$f_1/f_2 \equiv f_1 g$$

in $\mathcal{O}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$. Hence, if $f = f_1/f_2 \in \mathcal{O}_{P,\Bbbk}(X)$ with $f_1, f_2 \in \Bbbk[X]$ then we define $\omega(f) = f_1 g$. One can verify that ω is a well-defined ring homomorphism, that ω is surjective, and that $\ker(\omega) = \mathfrak{m}_{P,\Bbbk}(X)^2$. Hence ω is an isomorphism of rings as claimed.

Finally, if $f = f_1/f_2 \in \mathfrak{m}_{P,\Bbbk}(X)$ with $f_1, f_2 \in \Bbbk[X]$ then $f_1 \in \mathfrak{m}$ and $f_2 \in \Bbbk[X] - \mathfrak{m}$ and so $\omega(f) \in \mathfrak{m}$. It follows that $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2 \cong \mathfrak{m}/\mathfrak{m}^2$. □

Theorem 7.1.12. *Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ be a variety defined over $\Bbbk$ and let $P \in X(\Bbbk)$. Let d_1 be the dimension of the $\Bbbk$-vector space $\mathfrak{m}_{P,\Bbbk}/\mathfrak{m}_{P,\Bbbk}^2$. Let d_2 be the rank of the **Jacobian matrix***

$$J_{X,P} = \left(\frac{\partial f_i}{\partial x_j}(P) \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}.$$

Then $d_1 + d_2 = n$.

Proof: By Exercise 7.1.5 we may assume without loss of generality that $P = (0, \ldots, 0)$. Let the notation be as in Lemma 7.1.11. We have $d_1 = \dim_\Bbbk(\mathfrak{m}/\mathfrak{m}^2)$. Recall the map $\theta : \Bbbk[x_1, \ldots, x_n] \rightarrow \Bbbk^n$ from above, which gives an isomorphism from $\mathfrak{m}_0(\mathbb{A}^n)/\mathfrak{m}_0(\mathbb{A}^n)^2$ to $\Bbbk^n$.

Now, $\mathfrak{m}$ is the image of $\mathfrak{m}_0(\mathbb{A}^n)$ in $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/I_\Bbbk(X)$. Similarly, $\mathfrak{m}^2$ is the image of $\mathfrak{m}_0(\mathbb{A}^n)^2$ in $\Bbbk[X]$. Hence $\mathfrak{m}/\mathfrak{m}^2$ is isomorphic as a $\Bbbk$-vector space to $\mathfrak{m}_0(\mathbb{A}^n)/(\mathfrak{m}_0(\mathbb{A}^n)^2, I_\Bbbk(X))$. Similarly, the span of the rows of the matrix $J_{X,P}$ in $\Bbbk^n$ is $\theta(I_\Bbbk(X))$, which is isomorphic as a $\Bbbk$-vector space to $(I_\Bbbk(X), \mathfrak{m}_0(\mathbb{A}^n)^2)/\mathfrak{m}_0(\mathbb{A}^n)^2$. One therefore has $\dim_\Bbbk(\mathfrak{m}/\mathfrak{m}^2) + \operatorname{rank}(J_{X,P}) = n$. □

Corollary 7.1.13. *Let $X = V(f_1(\underline{x}), \ldots, f_m(\underline{x})) \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk$ of dimension d. Let $P \in X(\Bbbk)$. Then $P \in X(\Bbbk)$ is a **singular point** of X if and only if the Jacobian matrix $J_{X,P}$ has rank not equal to $n - d$. The point is **non-singular** if the rank of $J_{X,P}$ is equal to $n - d$.*

Corollary 7.1.14. *Let $X = V(f(x_1, \ldots, x_n)) \subseteq \mathbb{A}^n$ be irreducible and let $P \in X(\Bbbk)$. Then P is singular if and only if*

$$\frac{\partial f}{\partial x_j}(P) = 0$$

for all $1 \leq j \leq n$

Exercise 7.1.15. Prove Corollaries 7.1.13 and 7.1.14.

Exercise 7.1.16. Let $\Bbbk$ be a field such that $\operatorname{char}(\Bbbk) \neq 2$ and let $F(x) \in \Bbbk[x]$ be such that $\gcd(F(x), F'(x)) = 1$. Show that

$$X : y^2 = F(x)$$

is non-singular as an affine algebraic set. Now consider the projective closure $\overline{X} \subseteq \mathbb{P}^2$. Show that if $\deg(F(x)) \geq 4$ then there is a unique point in $\overline{X} - X$ and that it is a singular point.

Finally we can define what we mean by a curve.

Definition 7.1.17. A **curve** is a projective non-singular variety of dimension 1. A **plane curve** is a curve that is given by an equation $V(F(x,y,z)) \subseteq \mathbb{P}^2$.

Remark 7.1.18. We stress that in this book a curve is always projective and non-singular. Note that many authors (including Hartshorne [278] and Silverman [564]) allow affine and/or singular dimension 1 varieties X to be curves. A fact that we won't prove is that every finitely generated, transcendence degree 1 extension K of an algebraic closed field $\overline{\Bbbk}$ is the function field $\overline{\Bbbk}(C)$ of a curve (see Theorem I.6.9 of Hartshorne [278]; note that working over $\overline{\Bbbk}$ is essential as there are finitely generated, transcendence degree 1 extensions of $\Bbbk$ that are not $\Bbbk(C)$ for a curve C defined over $\Bbbk$). It follows that every irreducible algebraic set of dimension 1 over $\Bbbk$ is birational over $\overline{\Bbbk}$ to a non-singular curve (see Theorem 1.1 of Moreno [439] for the details). Hence, in practice one often writes down an affine and/or singular equation X that is birational to the projective, non-singular curve C one has in mind. In our notation, the commonly used phrase "singular curve" is an oxymoron. Instead one can say "singular equation for a curve" or "singular model for a curve".

The following result is needed in a later proof.

Lemma 7.1.19. *Let C be a curve over $\Bbbk$. Let $P, Q \in C(\overline{\Bbbk})$. Then $\mathcal{O}_{P,\overline{\Bbbk}} \subseteq \mathcal{O}_{Q,\overline{\Bbbk}}$ implies $P = Q$.*

Proof: By Exercise 5.2.23 we may assume that $P, Q \in U_n(\overline{\Bbbk}) \subseteq \mathbb{P}^n(\overline{\Bbbk})$ and applying φ_n^{-1} we have $P, Q \in \varphi_n^{-1}(C) \subseteq \mathbb{A}^n(\overline{\Bbbk})$. Let $R = \overline{\Bbbk}[\varphi_n^{-1}(C)]$ and define $\mathfrak{m} = \mathfrak{m}_{P,\overline{\Bbbk}} \cap R = \{f \in R : f(P) = 0\}$ as in Lemma 7.1.11. By Lemma 7.1.11, $R/\mathfrak{m} \cong \overline{\Bbbk}$ and so $\mathfrak{m}$ is a maximal R-ideal. Finally, $P \in V(\mathfrak{m})$ since every polynomial in $\mathfrak{m}_{P,\overline{\Bbbk}}$ vanishes at P, and by the Nullstellensatz $V(\mathfrak{m}) = \{P\}$.

If $\mathcal{O}_{P,\overline{\Bbbk}} \subseteq \mathcal{O}_{Q,\overline{\Bbbk}}$ then the inclusion map gives rise to $\mathcal{O}_{P,\overline{\Bbbk}} \to \mathcal{O}_{Q,\overline{\Bbbk}}/\mathfrak{m}_{Q,\overline{\Bbbk}}$ with kernel $\mathcal{O}_{P,\overline{\Bbbk}} \cap \mathfrak{m}_{Q,\overline{\Bbbk}}$. In other words, $\mathcal{O}_{P,\overline{\Bbbk}}/(\mathcal{O}_{P,\overline{\Bbbk}} \cap \mathfrak{m}_{Q,\overline{\Bbbk}})$ injects into $\mathcal{O}_{Q,\overline{\Bbbk}}/\mathfrak{m}_{Q,\overline{\Bbbk}} \cong \overline{\Bbbk}$. Hence $\mathcal{O}_{P,\overline{\Bbbk}} \cap \mathfrak{m}_{Q,\overline{\Bbbk}}$ is a maximal ideal and so $\mathfrak{m}_{P,\overline{\Bbbk}} \subseteq \mathfrak{m}_{Q,\overline{\Bbbk}}$. Therefore $\mathfrak{m} \subseteq \mathfrak{n} := \mathfrak{m}_{Q,\overline{\Bbbk}} \cap R$. But $\mathfrak{m}$ is maximal in R and $1 \notin \mathfrak{n}$ so $\mathfrak{m} = \mathfrak{n}$. Since $V(\mathfrak{m}) = \{P\}$ and $V(\mathfrak{n}) = \{Q\}$ we have $P = Q$.

The above proof was influenced by Lemma I.6.4 of Hartshorne [278], but it was pointed out to me by Noel Robinson that there should be a simpler proof: If $P \neq Q$ then one can write down a function f such that $f \in \mathcal{O}_{P,\overline{\Bbbk}}$ but $f \notin \mathcal{O}_{Q,\overline{\Bbbk}}$ as follows: Letting, as above, $P = (a_1, \ldots, a_n)$ and $Q = (b_1, \ldots, b_n)$ in some affine patch, then $P \neq Q$ implies $a_i \neq b_i$ for some index i. Then the function $f = 1/(x_i - b_i)$ has a pole at Q but is regular at P. □

7.2 Weierstrass Equations

Definition 7.2.1. Let $a_1, a_2, a_3, a_4, a_6 \in \Bbbk$. A **Weierstrass equation** is a projective algebraic set E over $\Bbbk$ given by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{7.1}$$

The **affine Weierstrass equation** is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{7.2}$$

Exercise 7.2.2. Let E be a Weierstrass equation as in Definition 7.2.1. Let $\iota(x : y : z) = (x : -y - a_1x - a_3z : z)$. Show that if $P \in E(\Bbbk)$ then $\iota(P) \in E(\Bbbk)$ and that ι is an isomorphism over $\Bbbk$ from E to itself.

Lemma 7.2.3. *Let $H(x), F(x) \in \Bbbk[x]$, $\deg(F) = 3$, $\deg(H) \leq 1$. Then $E(x, y) = y^2 + H(x)y - F(x)$ is irreducible over $\overline{\Bbbk}$.*

Proof: A non-trivial factorisation of $E(x, y)$ in $\Bbbk[x, y]$ must be of the form $E(x, y) = (y + M(x))(y + N(x))$ for some $M(x), N(x) \in \Bbbk[x]$. Then $\deg(M) + \deg(N) = 3$ and, without loss of generality, $\deg(M) \geq 2$ and $\deg(N) \leq 1$. But then $\deg(M + N) \geq 2$, which is incompatible with $M + N = H$. □

Theorem 5.3.10 therefore implies a Weierstrass equation describes a projective variety. By Exercise 5.6.5, the variety has dimension 1. Not every Weierstrass equation gives a curve, since some of them are singular. We now give conditions for when a Weierstrass equation is non-singular.

Exercise 7.2.4. Show that a Weierstrass equation has a unique point with $z = 0$. Show that this point is not a singular point.

Definition 7.2.5. Let E be a Weierstrass equation over $\Bbbk$. The point $(0 : 1 : 0) \in E(\Bbbk)$ is denoted by $\mathcal{O}_E$ and is called the **point at infinity**.

Exercise 7.2.6. Show that if $\mathrm{char}(\Bbbk) \neq 2, 3$ then every Weierstrass equation over $\Bbbk$ is isomorphic over $\Bbbk$ to a Weierstrass equation

$$y^2z = x^3 + a_4xz^2 + a_6z^3 \tag{7.3}$$

for some $a_4, a_6 \in \Bbbk$. This is called the **short Weierstrass form**. Show that this equation is non-singular if and only if the **discriminant** $4a_4^3 + 27a_6^2 \neq 0$ in $\Bbbk$.

Exercise 7.2.7. Show that if $\mathrm{char}(\Bbbk) = 2$ then every Weierstrass equation over $\Bbbk$ is isomorphic over $\Bbbk$ to a Weierstrass equation

$$y^2z + xyz = x^3 + a_2x^2z + a_6z^3 \quad \text{or} \quad y^2z + yz^2 = x^3 + a_4xz^2 + a_6z^3. \tag{7.4}$$

The former is non-singular if $a_6 \neq 0$ and the latter is non-singular for all $a_4, a_6 \in \Bbbk$.

Formulae to determine whether a general Weierstrass equation is singular are given in Section III.1 of [564].

Definition 7.2.8. An **elliptic curve** is a curve given by a non-singular Weierstrass equation.

The following easy result is useful for explicit calculations.

Lemma 7.2.9. *Let E be an elliptic curve over $\Bbbk$. Then every function $f \in \Bbbk(E)$ restricts to a function on the affine Weierstrass equation of E that is equivalent to a function of the form*

$$\frac{a(x) + b(x)y}{c(x)} \tag{7.5}$$

where $a(x), b(x), c(x) \in \Bbbk[x]$. Conversely, every such function on the affine curve corresponds to a unique[3] function on the projective curve.

[3]By unique we mean that there is only one function on the projective curve corresponding to a given function on the affine curve. The actual polynomials $a(x), b(x)$ and $c(x)$ are, of course, not unique.

Proof: Write U for the affine algebraic set obtained from E by setting $z = 1$. Note that $U\left(\overline{\Bbbk}\right) \neq \varnothing$. Corollary 5.4.9 shows that $\Bbbk(E) \cong \Bbbk(U)$ and so it is sufficient to consider functions on U. Every such function can be written in the form of equation (7.5) since any denominators can be cleared by multiplying through by appropriate polynomials (the polynomial $(a(x) + b(x)y)(a(x) + b(x)\iota(y))$ is a polynomial in x only) and y^n for $n > 1$ can be replaced using the equation $y^2 = (x^3 + a_2x^2 + a_4x + a_6) - y(a_1x + a_3)$. Both claims of the Lemma follow immediately. □

7.3 Uniformizers on Curves

Let C be a curve over $\Bbbk$ with function field $\Bbbk(C)$. It is necessary to formalise the notion of multiplicity of a zero or pole of a function at a point. The basic definition will be that $f \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ has multiplicity m at P if $f \in \mathfrak{m}^m_{P,\overline{\Bbbk}}$ and $f \notin \mathfrak{m}^{m+1}_{P,\overline{\Bbbk}}$. However, there are a number of technicalities to be dealt with before we can be sure this definition makes sense. We introduce uniformizers in this section as a step towards the rigorous treatment of multiplicity of functions.

First we recall the definition of non-singular from Definition 7.1.10: Let C be a non-singular curve over $\Bbbk$ and $P \in C(\Bbbk)$, then the quotient $\mathfrak{m}_{P,\Bbbk}(C)/\mathfrak{m}_{P,\Bbbk}(C)^2$ (which is a $\Bbbk$-vector space by Lemma 7.1.6) has dimension one as a $\Bbbk$-vector space.

Lemma 7.3.1. *Let C be a curve (in particular, non-singular) over a field $\Bbbk$ and let $P \in C(\Bbbk)$. Then the ideal $\mathfrak{m}_{P,\Bbbk}(C)$ is principal as an $\mathcal{O}_{P,\Bbbk}(C)$-ideal.*

Proof: Write $\mathfrak{m}$ for $\mathfrak{m}_{P,\Bbbk}(C)$. Since C is non-singular, $\dim_{\Bbbk} \mathfrak{m}_{P,\Bbbk}(C)/\mathfrak{m}_{P,\Bbbk}(C)^2 = 1$. Let $x \in \mathfrak{m}$ be such that $\{\mathfrak{m}^2 + x\}$ is a $\Bbbk$-vector space basis for $\mathfrak{m}/\mathfrak{m}^2$. Let $\mathfrak{n}$ be the $\mathcal{O}_{P,\Bbbk}(C)$-ideal (x). Then $\mathfrak{n} \subseteq \mathfrak{m}$. For every $y \in \mathfrak{m}$ we have $y = f + ux$ where $u \in \Bbbk$ and $f \in \mathfrak{m}^2$. Hence, $\mathfrak{m} = (\mathfrak{n}, \mathfrak{m}^2)$. Let A be the $\mathcal{O}_{P,\Bbbk}(C)$-module $\mathfrak{m}/\mathfrak{n}$. We want to prove that $A = 0$. This follows by Nakayama's Lemma (see Proposition 2.6 of [15]) but we give a direct proof.

First note that $\mathfrak{m}A = \mathfrak{m}(\mathfrak{m}/\mathfrak{n}) = (\mathfrak{m}^2, \mathfrak{n})/\mathfrak{n} = A$ (the middle equality since $y(\mathfrak{n} + z) = \mathfrak{n} + yz$ for all $y, z \in \mathfrak{m}$). Suppose now that $A \neq 0$. Since $\mathcal{O}_{P,\Bbbk}(C)$ is Noetherian it follows that $\mathfrak{m}$ is finitely generated as an $\mathcal{O}_{P,\Bbbk}(C)$-module and so A is finitely generated as an $\mathcal{O}_{P,\Bbbk}(C)$-module. Let $\{a_1, \ldots, a_k\}$ be a minimal set of generators for A. Since $A = \mathfrak{m}A$ we have

$$a_1 = \sum_{j=1}^{k} m_j a_j$$

for $m_j \in \mathfrak{m}$. Hence,

$$a_1(1 - m_1) = \sum_{j=2}^{k} m_j a_j.$$

Note that $1 - m_1 \notin \mathfrak{m}$ and so, since $\mathfrak{m}$ is a maximal ideal, $(1 - m_1)$ is a unit in $\mathcal{O}_{P,\Bbbk}(C)$. Hence, $a_1 \in (a_2, \ldots, a_k)$, which contradicts the minimality of the generating set. Hence $A = 0$ and $\mathfrak{m} = \mathfrak{n} = (x)$. □

Definition 7.3.2. Let C be a curve (in particular, non-singular) over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. A **uniformizer** (or **uniformizing parameter**) at P is an element $t_P \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ such that $\mathfrak{m}_{P,\overline{\Bbbk}}(C) = (t_P)$ as an $\mathcal{O}_{P,\overline{\Bbbk}}(C)$-ideal.

One can choose t_P to be any element of $\mathfrak{m}_{P,\overline{\Bbbk}}(C) - \mathfrak{m}_{P,\overline{\Bbbk}}(C)^2$; in other words, the uniformizer is not unique. If P is defined over $\Bbbk$ then one can take $t_P \in \mathfrak{m}_{P,\Bbbk}(C) -$

$\mathfrak{m}_{P,\Bbbk}(C)^2$, i.e., take the uniformizer to be defined over $\Bbbk$; this is typically what one does in practice.

For our presentation it is necessary to know uniformizers on $\mathbb{P}^1$ and on a Weierstrass equation. The next two examples determine such uniformizers.

Example 7.3.3. Let $C = \mathbb{P}^1$. For a point $(a : 1) \in U_1 \subseteq \mathbb{P}^1$ one can work instead with the point a on the affine curve $\mathbb{A}^1 = \varphi_1^{-1}(U_1)$. One has $\mathfrak{m}_a = (x - a)$ and so $t_a = (x - a)$ is a uniformizer at a. In terms of the projective equation one has $t_a = (x - az)/z$ being a uniformizer. For the point $\infty = (1 : 0) \in U_0 \subseteq \mathbb{P}^1$ one again works with the corresponding point $0 \in \varphi_0^{-1}(U_0)$. The uniformizer is $t_a = z$ which, projectively, is $t_a = z/x$. A common abuse of notation is to say that $1/x$ is a uniformizer at ∞ on $\mathbb{A}^1 = \varphi_1^{-1}(U_1)$.

Example 7.3.4. We determine uniformizers for the points on an elliptic curve. First consider points (x_P, y_P) on the affine equation

$$E(x, y) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right).$$

Without loss of generality we can translate the point to $P_0 = (0, 0)$, in which case write $a'_1, \ldots, a'_6$ for the coefficients of the translated equation $E'(x, y) = 0$ (i.e., $E'(x, y) = E(x + x_P, y + y_P)$). One can verify that $a'_6 = 0$, $a'_3 = (\partial E/\partial y)(P)$ and $a'_4 = (\partial E/\partial x)(P)$. Then $\mathfrak{m}_{P_0} = (x, y)$ and, since the curve is not singular, at least one of a'_3 or a'_4 is non-zero.

If $a'_3 = 0$ then[4]

$$x(x^2 + a'_2x + a'_4 - a'_1y) = y^2.$$

Since $(x^2 + a'_2x + a'_4 - a'_1y)(P_0) = a'_4 \neq 0$ we have $(x^2 + a'_2x + a'_4 - a'_1y)^{-1} \in \mathcal{O}_{P_0}$ and so

$$x = y^2(a'_4 + a'_2x + x^2 - a'_1y)^{-1}.$$

In other words, $x \in (y^2) \subseteq \mathfrak{m}_{P_0}^2$ and y is a uniformizer at P_0.

Similarly, if $a'_4 = 0$ then $y(a'_3 + a'_1x + y) = x^2(x + a'_2)$ and so $y \in (x^2) \subseteq \mathfrak{m}_{P_0}^2$ and x is a uniformizer at P_0. If $a'_3, a'_4 \neq 0$ then either x or y can be used as a uniformizer. (Indeed, any linear combination $ax + by$ except $a'_3y - a'_4x$ can be used as a uniformizer; geometrically, any line through P, except the line which is tangent to the curve at P, is a uniformizer.)

Now consider the point at infinity $\mathcal{O}_E = (x : y : z) = (0 : 1 : 0)$ on E. Taking $y = 1$ transforms the point to $(0, 0)$ on the affine curve

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{7.6}$$

It follows that

$$z(1 + a_1x + a_3z - a_2x^2 - a_4xz - a_6z^2) = x^3$$

and so $z \in (x^3) \subseteq \mathfrak{m}_P^3$ and so x is a uniformizer (which corresponds to x/y in homogeneous coordinates).

In practice it is not necessary to move P to $(0, 0)$ and compute the a'_i. We have shown that if $P = (x_P, y_P)$ then $t_P = x - x_P$ is a uniformizer unless $P = \mathcal{O}_E$, in which case $t_P = x/y$, or $P = \iota(P)$,[5] in which case $t_P = y - y_P$.

Lemma 7.3.5. *Let C be a curve over $\Bbbk$, let $P \in C(\overline{\Bbbk})$ and let t_P be a uniformizer at P. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then $\sigma(t_P)$ is a uniformizer at $\sigma(P)$.*

[4] We will see later that $a'_3 = 0$ implies $(0, 0)$ has order 2 (since $-(x, y) = (x, -y - a'_1x - a'_3)$).

[5] i.e., has order 2.

Proof: Since $\sigma(f)(\sigma(P)) = \sigma(f(P))$ the map $f \mapsto \sigma(f)$ is an isomorphism of local rings $\sigma : \mathcal{O}_{P,\overline{\Bbbk}}(C) \to \mathcal{O}_{\sigma(P),\overline{\Bbbk}}(C)$. It also follows that $\sigma(\mathfrak{m}_P) = \mathfrak{m}_{\sigma(P)}$. Since $\mathfrak{m}_P = (t_P)$ one has $\mathfrak{m}_{\sigma(P)} = (\sigma(t_P))$, which completes the proof. □

We now give an application of uniformizers. It will be used in several later results.

Lemma 7.3.6. *Let C be a non-singular curve over $\Bbbk$ and let $\phi : C \to Y \subseteq \mathbb{P}^n$ be a rational map for any projective variety Y. Then ϕ is a morphism.*

Exercise 7.3.7. Prove Lemma 7.3.6.

7.4 Valuation at a Point on a Curve

The aim of this section is to define the multiplicity of a zero or pole of a function on a curve. For background on discrete valuation rings see Chapter 1 of Serre [542], Section I.7 of Lang [365] or Sections XII.4 and XII.6 of Lang [367].

Definition 7.4.1. Let K be a field. A **discrete valuation** on K is a function $v : K^* \to \mathbb{Z}$ such that:

1. for all $f, g \in K^*$, $v(fg) = v(f) + v(g)$;
2. for all $f, g \in K^*$ such that $f + g \neq 0$, $v(f + g) \geq \min\{v(f), v(g)\}$;
3. there is some $f \in K^*$ such that $v(f) = 1$ (equivalently, v is surjective to $\mathbb{Z}$).

Lemma 7.4.2. *Let K be a field and v a discrete valuation.*

1. $v(1) = 0$.
2. *If $f \in K^*$ then $v(1/f) = -v(f)$.*
3. $R_v = \{f \in K^* : v(f) \geq 0\} \cup \{0\}$ *is a ring, called the* ***valuation ring****.*
4. $\mathfrak{m}_v = \{f \in K^* : v(f) > 0\}$ *is a maximal ideal in R_v, called the* ***maximal ideal*** *of the valuation.*
5. *If $f \in K$ is such that $f \notin R_v$ then $1/f \in \mathfrak{m}_v$.*
6. *R_v is a local ring.*

Exercise 7.4.3. Prove Lemma 7.4.2.

Lemma 7.4.4. *Let C be a curve over $\Bbbk$ and $P \in C(\Bbbk)$. For every non-zero function $f \in \mathcal{O}_{P,\Bbbk}(C)$ there is some $m \in \mathbb{N}$ such that $f \notin \mathfrak{m}_{P,\Bbbk}^m$.*

Proof: We drop the terms $\Bbbk$ and C in $\mathcal{O}_{P,\Bbbk}(C)$ and $\mathfrak{m}_{P,\Bbbk}(C)$. If $f \notin \mathfrak{m}_P$ then $m = 1$ and we are done, so suppose $f \in \mathfrak{m}_P$. Let t_P be a uniformizer at P. Then $f = t_P f_1$ for some $f_1 \in \mathcal{O}_P$. If $f_1 \notin \mathfrak{m}_P$ then $f \notin \mathfrak{m}_P^2$ and we are finished. If $f_1 \in \mathfrak{m}_P$ then $f_1 = t_P f_2$ for some $f_2 \in \mathcal{O}_P$. Continuing this way, if $f \in \mathfrak{m}_P^m$ for all $m \in \mathbb{N}$ one obtains an infinite sequence of functions $f_i \in \mathfrak{m}_P$. Consider the chain of $\mathcal{O}_P$-ideals $(f_1) \subseteq (f_2) \subseteq \cdots$. We have $(f_i) \neq (f_{i+1})$ since $f_i = t_P f_{i+1}$ and $t_P^{-1} \notin \mathcal{O}_P$ (if $t_P^{-1}(P) \in \Bbbk$ then $1 = 1(P) = (t_P t_P^{-1})(P) = t_P(P) t_P^{-1}(P) = 0$, which is a contradiction). Since $\mathcal{O}_P$ is Noetherian (Lemma 7.1.2) the ascending chain of ideals is finite, hence $f \in \mathfrak{m}_P^m$ for some $m \in \mathbb{N}$. □

Definition 7.4.5. Let C be a curve over $\Bbbk$ and $P \in C(\Bbbk)$. Let $\mathfrak{m}_P = \mathfrak{m}_{P,\Bbbk}(C)$ be as in Definition 7.1.1 and define $\mathfrak{m}_P^0 = \mathcal{O}_{P,\Bbbk}(C)$. Let $f \in \mathcal{O}_{P,\Bbbk}(C)$ be such that $f \neq 0$ and define the **order** of f at P to be $v_P(f) = \max\{m \in \mathbb{Z}_{\geq 0} : f \in \mathfrak{m}_P^m\}$. If $v_P(f) = 1$ then f has a **simple zero** at P. (We exclude the constant function $f = 0$, though one could define $v_P(0) = \infty$.)

We stress that $v_P(f)$ is well-defined. If $f, h \in \mathcal{O}_{P,\Bbbk}(C)$ and $f \equiv h$ then $f - h = 0$ in $\mathcal{O}_{P,\Bbbk}(C)$. Hence, if $f \in \mathfrak{m}_P^m$ then $h \in \mathfrak{m}_P^m$ (and vice versa).

Exercise 7.4.6. Show that $v_P(f)$ does not depend on the underlying field. In other words, if $\Bbbk'$ is an algebraic extension of $\Bbbk$ in $\overline{\Bbbk}$ then $v_P(f) = \max\{m \in \mathbb{Z}_{\geq 0} : f \in \mathfrak{m}_{P,\Bbbk'}(C)^m\}$.

Lemma 7.4.7. *Let C be a curve over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. Let $t_P \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ be any uniformizer at P. Let $f \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ be such that $f \neq 0$. Then $v_P(f) = \max\{m \in \mathbb{Z}_{\geq 0} : f/t_P^m \in \mathcal{O}_{P,\overline{\Bbbk}}(C)\}$ and $f = t_P^{v_P(f)}u$ for some $u \in \mathcal{O}_{P,\overline{\Bbbk}}(C)^*$.*

Exercise 7.4.8. Prove Lemma 7.4.7.

Writing a function f as $t_P^{v_P(f)}u$ for some $u \in \mathcal{O}_{P,\overline{\Bbbk}}(C)^*$ is analogous to writing a polynomial $F(x) \in \Bbbk[x]$ in the form $F(x) = (x-a)^m G(x)$ where $G(x) \in \Bbbk[x]$ satisfies $G(a) \neq 0$. Hopefully the reader is convinced that this is a powerful tool. For example, it enables a simple proof of Exercise 7.4.9. Further, one can represent a function f as a formal power series $\sum_{n=v_P(f)}^{\infty} a_n t_P^n$ where $a_n \in \Bbbk$; see Exercises 2-30 to 2-32 of Fulton [216]. Such expansions will used in Chapters 25 and 26 but we don't develop the theory rigorously.

Exercise 7.4.9. Let C be a curve over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. Let $f, h \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ be such that $f, h \neq 0$. Show that $v_P(fh) = v_P(f) + v_P(h)$.

Lemma 7.4.10. *Let C be a curve over $\Bbbk$, let $P \in C(\overline{\Bbbk})$ and let $f \in \Bbbk(C)$. Then f can be written as f_1/f_2 where $f_1, f_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$.*

Proof: Without loss of generality C is affine. By definition, $f = f_1/f_2$ where $f_1, f_2 \in \Bbbk[C]$. Since $\Bbbk[C] \subset \overline{\Bbbk}[C] \subset \mathcal{O}_{P,\overline{\Bbbk}}(C)$ the result follows. □

Definition 7.4.11. Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)$. A point $P \in C(\overline{\Bbbk})$ is called a **pole** of f if $f \notin \mathcal{O}_{P,\overline{\Bbbk}}(C)$. If $f = f_1/f_2 \in \Bbbk(C)$ where $f_1, f_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ then define $v_P(f) = v_P(f_1) - v_P(f_2)$.

Exercise 7.4.12. Show that if $P \in C(\overline{\Bbbk})$ is a pole of $f \in \Bbbk(C)$ then $v_P(f) < 0$ and P is a zero of $1/f$.

Lemma 7.4.13. *For every function $f \in \Bbbk(C)$ the order $v_P(f)$ of f at P is independent of the choice of representative of f.*

Proof: Suppose $f_1/f_2 \equiv g_1/g_2$ where $f_1, f_2, g_1, g_2 \in \mathcal{O}_P$. Then $f_1g_2 - f_2g_1 \in I_\Bbbk(C)$ and so $f_1g_2 = f_2g_1$ in $\mathcal{O}_P$. Since v_P is well-defined in $\mathcal{O}_P$ we have $v_P(f_1g_2) = v_P(f_2g_1)$. Applying Exercise 7.4.9 gives $v_P(f_1) + v_P(g_2) = v_P(f_2) + v_P(g_1)$. Re-arranging and applying Definition 7.4.11 proves the result. □

We now give some properties of $v_P(f)$.

Lemma 7.4.14. *Let $P \in C(\overline{\Bbbk})$. Then v_P is a discrete valuation on $\Bbbk(C)$. Furthermore, the following properties hold.*

1. *If $f \in \overline{\Bbbk}^*$ then $v_P(f) = 0$.*
2. *If $c \in \overline{\Bbbk}$ and if $v_P(f) < 0$ then $v_P(f + c) = v_P(f)$.*
3. *If $f_1, f_2 \in \Bbbk(C)^*$ are such that $v_P(f_1) \neq v_P(f_2)$ then $v_P(f_1+f_2) = \min\{v_P(f_1), v_P(f_2)\}$.*
4. *Suppose C is defined over $\Bbbk$ and let $P \in C(\overline{\Bbbk})$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then $v_P(f) = v_{\sigma(P)}(\sigma(f))$.*

Proof: Let t_P be a uniformizer at P. Then $v_P(t_P) = 1$, which proves the third property of Definition 7.4.1. The property $v_P(fg) = v_P(f) + v_P(g)$ follows by the same argument as Exercise 7.4.9. Similarly, if$f = t_P^v u_1$ and $g = t_P^w u_2$ with $v \leq w$ and $g \neq -f$ then $f+g = t_P^v(u_1 + t_P^{w-v}u_2)$ so $v_P(f+g) \geq \min\{v_P(f), v_P(g)\}$. Hence v_P satisfies Definition 7.4.1.

We turn to the rest of the proof. The third statement is just a refinement of the above argument. Without loss of generality, $v_P(f_1) < v_P(f_2)$. Then $f_1 = t_P^v u_1$ and $f_2 = t_P^{v+m}u_2$ for some $u_1, u_2 \in \mathcal{O}_P^*$, $v \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then $f_1 + f_2 = t_P^v(u_1 + t_P^m u_2) \neq 0$ and $u_1 + t_P^m u_2 \in \mathcal{O}_P^*$ so $v_P(f_1 + f_2) = v_P(f_1)$.

The first statement follows since $f(P) \neq 0$. Statement 2 is just a special case of statement 3.

For the fourth statement, recall from Lemma 7.3.5 that one can take $t_{\sigma(P)} = \sigma(t_P)$. If $f = t_P^v u$ where $u(P) \neq 0$ then $\sigma(f) = \sigma(t_P)^v \sigma(u)$ and $\sigma(u)(\sigma(P)) = \sigma(u(P)) \neq \sigma(0) = 0$ (see Exercise 5.4.13). The result follows. □

Having shown that every v_P is a discrete valuation on $\Bbbk(C)$ it is natural to ask whether every discrete valuation on $\Bbbk(C)$ is v_P for some point $P \in C(\Bbbk)$. To make this true over fields that are not algebraically closed requires a more general notion of a point of C defined over $\Bbbk$. Instead of doing this, we continue to work with points over $\overline{\Bbbk}$ and show in Theorem 7.5.2 that every discrete valuation on $\overline{\Bbbk}(C)$ is v_P for some $P \in C(\overline{\Bbbk})$. But first we give some examples.

Example 7.4.15. Let $E : y^2 = x(x-1)(x+1)$ over $\Bbbk$ and let $P = (1,0) \in E(\Bbbk)$. We determine $v_P(x), v_P(x-1), v_P(y)$ and $v_P(x+y-1)$.

First, $x(P) = 1$ so $v_P(x) = 0$. For the rest, since $P = \iota(P)$ we take the uniformizer to be $t_P = y$. Hence $v_P(y) = 1$. Since

$$x - 1 = y^2/(x(x+1))$$

and $1/(x(x+1)) \in \mathcal{O}_P$ we have $v_P(x-1) = 2$.

Finally, $f(x,y) = x + y - 1 = y + (x-1)$ so $v_P(f(x,y)) = \min\{v_P(y), v_P(x-1)\} = \min\{1,2\} = 1$. One can see this directly by writing $f(x,y) = y(1 + y/x(x+1))$.

Lemma 7.4.16. *Let E be an elliptic curve. Then $v_{\mathcal{O}_E}(x) = -2$ and $v_{\mathcal{O}_E}(y) = -3$.*

Proof: We consider the projective equation, so that the functions become x/z and y/z then set $y = 1$ so that we are considering x/z and $1/z$ on

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

As in Example 7.3.4 we have $z \in (x^3)$ and so $v_{\mathcal{O}_E}(x) = 1, v_{\mathcal{O}_E}(z) = 3$. This implies $v_{\mathcal{O}_E}(1/z) = -3$ and $v_{\mathcal{O}_E}(x/z) = -2$ as claimed. □

7.5 Valuations and Points on Curves

Let C be a curve over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. We have shown that $v_P(f)$ is a discrete valuation on $\overline{\Bbbk}(C)$. The aim of this section is to show (using the weak Nullstellensatz) that every discrete valuation v on $\overline{\Bbbk}(C)$ arises as v_P for some point $P \in C(\overline{\Bbbk})$.

Lemma 7.5.1. *Let C be a curve over $\Bbbk$ and let v be a discrete valuation on $\Bbbk(C)$. Write $R_v, \mathfrak{m}_v$ for the corresponding valuation ring and maximal ideal (over $\overline{\Bbbk}$). Suppose $C \subset \mathbb{P}^n$ with coordinates $(x_0 : \cdots : x_n)$. Then there exists some $0 \leq i \leq n$ such that $\overline{\Bbbk}[\varphi_i^{-1}(C)]$ is a subring of R_v (where φ_i^{-1} is as in Definition 5.2.24).*

Proof: First we prove there exists some $0 \leq i \leq n$ such that $x_0/x_i, \ldots, x_n/x_i \in R_v$. To do this define $S_i = \{j : 0 \leq j \leq n, x_i/x_j \in R_v\}$. We claim that $S_0 \cap \cdots \cap S_n \neq \varnothing$ and prove this by induction. First, note that $i \in S_i$ so $S_0 \neq \varnothing$. Suppose, that $j \in S_0 \cap \cdots \cap S_k$ for $k \geq 0$. If $j \in S_{k+1}$ then we are done. If $j \notin S_{k+1}$ then we have $x_{k+1}/x_j \notin R_v$ and so $x_j/x_{k+1} \in R_v$. Since $x_i/x_j \in R_v$ for $0 \leq i \leq k$ by the inductive hypothesis it follows that $(x_i/x_j)(x_j/x_{k+1}) = x_i/x_{k+1} \in R_v$ for $0 \leq i \leq k+1$. It follows that $S_0 \cap \cdots \cap S_{k+1} \neq \varnothing$.

To prove the result, suppose i is such that $x_0/x_i, \ldots, x_n/x_i \in R_v$ Then $\overline{\Bbbk}[\varphi_i^{-1}(C)] = \overline{\Bbbk}[x_0/x_i, \ldots, x_n/x_i]$ is a subring of R_v. □

Theorem 7.5.2. *Let C be a curve over $\Bbbk$ and let v be a discrete valuation on $\overline{\Bbbk}(C)$. Then $v = v_P$ for some $P \in C(\overline{\Bbbk})$.*

Proof: (Sketch) Let R_v be the valuation ring of v and $\mathfrak{m}_v$ the maximal ideal. Let i be as in Lemma 7.5.1 so that $R = \overline{\Bbbk}[\varphi_i^{-1}(C)] \subseteq R_v$. Note that R is the affine coordinate ring of an affine curve.

By Lemma A.9.2, $\mathfrak{m} = R \cap \mathfrak{m}_v$ is a prime ideal in R. Furthermore, $\mathfrak{m} \neq \varnothing$ and $\mathfrak{m} \neq R$. Since R has Krull dimension 1, $\mathfrak{m}$ is a maximal ideal.

Theorem 5.1.20 (weak Nullstellensatz) shows that $\mathfrak{m}$ is equal to $\mathfrak{m}_P \cap \overline{\Bbbk}[\varphi_i^{-1}(C)]$ for some point $P \in C(\overline{\Bbbk})$. It follows that the restriction of v to $\overline{\Bbbk}[\varphi_i^{-1}(C)]$ is equal to v_P. Finally, since $\Bbbk(C)$ is the field of fractions of $\overline{\Bbbk}[\varphi_i^{-1}(C)]$ it follows that $v = v_P$.

For full details see Corollary I.6.6 of Hartshorne [278] or Theorem VI.9.1 of Lorenzini [394]. □

7.6 Divisors

A divisor is just a notation for a finite multi-set of points. As always, we work with points over an algebraically closed field $\overline{\Bbbk}$.

Definition 7.6.1. Let C be a curve over $\Bbbk$ (necessarily non-singular and projective). A **divisor** on C is a formal sum

$$D = \sum_{P \in C(\overline{\Bbbk})} n_P(P) \tag{7.7}$$

where $n_P \in \mathbb{Z}$ and only finitely many $n_P \neq 0$. The divisor with all $n_P = 0$ is written 0. The **support** of the divisor D in equation (7.7) is $\mathrm{Supp}(D) = \{P \in C(\overline{\Bbbk}) : n_P \neq 0\}$. Note that many authors use the notation $|D|$ for the support of D. Denote by $\mathrm{Div}_{\overline{\Bbbk}}(C)$ the set of all divisors on C. Define $-D = \sum_P (-n_P)(P)$. If $D' = \sum_{P \in C(\overline{\Bbbk})} n'_P(P)$ then define

$$D + D' = \sum_{P \in C(\overline{\Bbbk})} (n_P + n'_P)(P).$$

Write $D \geq D'$ if $n_P \geq n'_P$ for all P. So $D \geq 0$ if $n_P \geq 0$ for all P, and such a divisor is called **effective**.

Example 7.6.2. Let $E : y^2 = x^3 + 2x - 3$ over $\mathbb{Q}$ and let $P = (2,3), Q = (1,0) \in E(\mathbb{Q})$. Then

$$D = 5(P) - 7(Q)$$

is a divisor on E. The support of D is $\mathrm{Supp}(D) = \{P, Q\}$ and D is not effective.

Definition 7.6.3. The **degree** of a divisor $D = \sum_P n_P(P)$ is the integer

$$\deg(D) = \sum_{P \in C(\overline{\Bbbk})} n_P.$$

(We stress that this is a finite sum.) We write $\mathrm{Div}^0_{\overline{\Bbbk}}(C) = \{D \in \mathrm{Div}_{\overline{\Bbbk}}(C) : \deg(D) = 0\}$.

Lemma 7.6.4. *$\mathrm{Div}_{\overline{\Bbbk}}(C)$ is a group under addition, and $\mathrm{Div}^0_{\overline{\Bbbk}}(C)$ is a subgroup.*

Exercise 7.6.5. Prove Lemma 7.6.4.

Definition 7.6.6. Let C be a curve over $\Bbbk$ and let $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ be a divisor on C. For $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ define $\sigma(D) = \sum_P n_P(\sigma(P))$. Then D is **defined over** $\Bbbk$ if $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Write $\mathrm{Div}_{\Bbbk}(C)$ for the set of divisors on C that are defined over $\Bbbk$.

Since $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ is an enormous and complicated object it is important to realise that testing the field of definition of any specific divisor is a finite task. There is an extension $\Bbbk'/\Bbbk$ of finite degree containing the coordinates of all points in the support of D. Let $\Bbbk''$ be the Galois closure of $\Bbbk'$. Since $\Bbbk''$ is normal over $\Bbbk$, any $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ is such that $\sigma(\Bbbk'') = \Bbbk''$. Hence, it is sufficient to study the behaviour of D under $\sigma \in \mathrm{Gal}(\Bbbk''/\Bbbk)$.

Example 7.6.7. Let $C : x^2 + y^2 = 6$ over $\mathbb{Q}$ and let $P = (1+\sqrt{2}, 1-\sqrt{2}), Q = (1-\sqrt{2}, 1+\sqrt{2}) \in C(\mathbb{Q}(\sqrt{2})) \subseteq C(\overline{\mathbb{Q}})$. Define

$$D = (P) + (Q).$$

It is sufficient to consider $\sigma(D)$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. The only non-trivial element is $\sigma(\sqrt{2}) = -\sqrt{2}$ and one sees that $\sigma(P) = Q$ and $\sigma(Q) = P$. Hence $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ and D is defined over $\mathbb{Q}$. Note that $C(\mathbb{Q}) = \varnothing$, so this example shows it is possible to have $\mathrm{Div}_{\Bbbk}(C) \neq \{0\}$ even if $C(\Bbbk) = \varnothing$.

7.7 Principal Divisors

This section contains an important and rather difficult result, namely that the number of poles of a function on a curve (counted according to multiplicity) is finite and equal to the number of zeros (counted according to multiplicity). The finiteness condition is essential to be able to represent the poles and zeroes of a function as a divisor. The other condition is required to show that the set of all divisors of functions is a subgroup of $\mathrm{Div}^0_{\Bbbk}(C)$.

In this chapter, finite poles and finite zeroes is only proved for plane curves and $\deg(\mathrm{div}(f)) = 0$ is proved only for elliptic curves. The general results are given in Section 8.3 in the next Chapter.

Theorem 7.7.1. *Let C be a curve over $\Bbbk$ and $f \in \Bbbk(C)^*$. Then f has finitely many poles and zeroes.*

Proof: (Special case of plane curves.) Let $C = V(F(x,y,z)) \subseteq \mathbb{P}^2$ where F is irreducible. If $F(x,y,z) = z$ then the result follows from Exercise 5.2.35 (there are only finitely many points at infinity). So we can restrict to the affine case $C = V(F(x,y))$.

Let $f = f_1(x,y)/f_2(x,y)$ with $f_1, f_2 \in \Bbbk[x,y]$. Then f is regular whenever $f_2(P) \neq 0$ so the poles of f are contained in $C \cap V(f_2)$. Without loss of generality, $f_2(x,y)$ contains monomials featuring x. The resultant $R_x(f_2(x,y), F(x,y))$ is a polynomial in y with a finite number of roots hence $C \cap V(f_2)$ is finite.

To show there are finitely many zeroes write $f = f_1/f_2$. The zeroes of f are contained in $C \cap (V(f_1) \cup V(f_2))$ and the argument above applies. □

Definition 7.7.2. Let $f \in \overline{\Bbbk}(C)^*$ and define the **divisor of a function** (this is a divisor by Theorem 7.7.1)

$$\mathrm{div}(f) = \sum_{P \in C(\overline{\Bbbk})} v_P(f)(P).$$

The divisor of a function is also called a **principal divisor**. Note that some authors write $\mathrm{div}(f)$ as (f). Let

$$\mathrm{Prin}_{\Bbbk}(C) = \{\mathrm{div}(f) : f \in \Bbbk(C)^*\}.$$

Exercise 7.7.3. Show that the zero element of $\mathrm{Div}_{\Bbbk}(C)$ lies in $\mathrm{Prin}_{\Bbbk}(C)$.

Lemma 7.7.4. *Let C be a curve over $\Bbbk$ and let $f, f' \in \Bbbk(C)^*$.*

1. $\mathrm{div}(ff') = \mathrm{div}(f) + \mathrm{div}(f')$.
2. $\mathrm{div}(1/f) = -\mathrm{div}(f)$.
3. $\mathrm{div}(f + f') \geq \sum_P \min\{v_P(f), v_P(f')\}(P)$.
4. $\mathrm{div}(f^n) = n\mathrm{div}(f)$ *for* $n \in \mathbb{Z}$.
5. *Let* $f \in \overline{\Bbbk}(C)$ *and let* $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. *Then* $\mathrm{div}(\sigma(f)) = \sigma(\mathrm{div}(f))$.

Exercise 7.7.5. Prove Lemma 7.7.4.

Lemma 7.7.6. *With notation as above,* $\mathrm{Prin}_{\Bbbk}(C)$ *is a subgroup of* $\mathrm{Div}_{\Bbbk}(C)$ *under addition.*

Exercise 7.7.7. Prove Lemma 7.7.6.

Lemma 7.7.8. *In* $\mathbb{P}^1(\Bbbk)$ *every degree 0 divisor is principal.*

Proof: Let $D = \sum_{i=1}^n e_i(x_i : z_i)$ where $\sum_{i=1}^n e_i = 0$. Define

$$f(x, z) = \prod_{i=1}^{n} (xz_i - zx_i)^{e_i}. \tag{7.8}$$

Since $\sum_{i=1}^n e_i = 0$ it follows that $f(x, z)$ is a ratio of homogeneous polynomials of the same degree and therefore a rational function on $\mathbb{P}^1$. Using the uniformizers on $\mathbb{P}^1$ from Example 7.3.3 one can verify that $v_{P_i}(f) = e_i$ when $P_i = (x_i : z_i)$ and hence that $D = \mathrm{div}(f)$. □

Note that if D is defined over $\Bbbk$ then one can show that the function $f(x, z)$ in equation (7.8) is defined over $\Bbbk$.

Exercise 7.7.9. Prove that if $f \in \Bbbk(\mathbb{P}^1)$ then $\deg(\mathrm{div}(f)) = 0$.

Lemma 7.7.10. *Let $E : y^2 + H(x)y = F(x)$ be a Weierstrass equation over $\Bbbk$ and let $P = (x_i, y_i) \in E(\overline{\Bbbk})$ be a non-singular point. Then* $\mathrm{div}(x - x_i) = (P) + (\iota(P)) - 2(\mathcal{O}_E)$.

Proof: There are one or two points $P \in E(\overline{\Bbbk})$ with x-coordinate equal to x_i, namely $P = (x_i, y_i)$ and $\iota(P) = (x_i, -y_i - H(x_i))$ (and these are equal if and only if $2y_i + H(x_i) = 0$). By Example 7.3.4 one can take the uniformizer $t_P = t_{\iota(P)} = (x - x_i)$ unless $(\partial E/\partial y)(P) = 2y_i + H(x_i) = 0$, in which case the uniformizer is $t_P = (y - y_i)$. In the former case we have $v_P(x - x_i) = v_{\iota(P)}(x - x_i) = 1$. In the latter case write

$F(x) = (x-x_i)g(x)+F(x_i) = (x-x_i)g(x)+y_i^2+H(x_i)y_i$ and $H(x) = (x-x_i)a_1+H(x_i)$. Note that $a_1y_i - g(x_i) = (\partial E/\partial x)(P) \neq 0$ and so $g_1(x) := 1/(a_1y - g(x)) \in \mathcal{O}_P$. Then

$$\begin{aligned} 0 &= y^2 + H(x)y - F(x) \\ &= (y-y_i)^2 + 2yy_i - y_i^2 + (x-x_i)a_1y + H(x_i)y - (x-x_i)g(x) - y_i^2 - H(x_i)y_i \\ &= (y-y_i)^2 + (x-x_i)(a_1y - g(x)) + (y-y_i)(2y_i + H(x_i)). \end{aligned}$$

Hence, $x - x_i = (y-y_i)^2 g_1(x)$ and $v_P(x-x_i) = 2$. Finally, the function $(x-x_i)$ corresponds to

$$\frac{x - x_i z}{z} = \frac{x}{z} - x_i$$

on the projective curve E. Since $v_{\mathcal{O}_E}(x/z) = -2$ it follows from part 2 of Lemma 7.4.14 that $v_{\mathcal{O}_E}(x-x_i) = -2$. Hence, if $P = (x_i, y_i)$ then, in all cases, $\mathrm{div}(x-x_i) = (P) + (\iota(P)) - 2(\mathcal{O}_E)$ and $\deg(\mathrm{div}(x-x_i)) = 0$. □

Exercise 7.7.9 and Lemma 7.7.10 determine the divisor of certain functions, and in both cases they turns out to have degree zero. This is not a coincidence. Indeed, we now state a fundamental[6] result which motivates the definition of the divisor class group.

Theorem 7.7.11. *Let C be a curve over $\Bbbk$. Let $f \in \Bbbk(C)^*$. Then* $\deg(\mathrm{div}(f)) = 0$.

Theorem 7.7.11 is proved for general curves in Theorem 8.3.14. Exercise 7.7.9 already proved it for $\mathbb{P}^1$. We prove Theorem 7.7.11 in the case of elliptic curves in this section (essentially, using the same method as Charlap and Robbins [127]). First, we state and prove a lemma.

Lemma 7.7.12. *Let $E : y^2 + H(x)y = F(x)$ be a Weierstrass equation over $\Bbbk$. Recall the morphism $\iota(x,y) = (x, -y-H(x))$ from Exercise 7.2.2. For $f \in \Bbbk(E)$ define $\iota^*(f) = f \circ \iota$. Let $P \in E(\Bbbk)$ be a non-singular point, $Q = \iota(P)$ and let t_Q be a uniformizer at Q. Then $\iota^* t_Q$ is a uniformizer at P and $v_Q(f) = v_P(\iota^*(f))$.*

Proof: One can verify that ι^* is a field automorphism of $\Bbbk(C)$. By definition, $(\iota^* f)(P) = f(\iota(P)) = f(Q)$. and so ι^* gives an isomorphism $\iota^* : \mathcal{O}_Q \to \mathcal{O}_P$. The result follows. □

We can now give a proof of Theorem 7.7.11 for elliptic curves. In some sense, our proof reduces the problem to a polynomial function on $\mathbb{P}^1$ (and the result for $\mathbb{P}^1$ is already known by Exercise 7.7.9). The proof given in Theorem 8.3.14 essentially follows the same logic of reducing to $\mathbb{P}^1$.

Proof: (Proof of Theorem 7.7.11 in the case of elliptic curves.) Write $E(x,y) = y^2 + H(x)y - F(x)$.

First consider a polynomial $a(x) \in \Bbbk[x]$ of degree d as a function on the affine elliptic curve $y^2 + H(x)y = F(x)$ (obtained by taking $z = 1$). The function has no poles on the affine part $E \cap \mathbb{A}^2$. Write $a(x) = \prod_{i=1}^n (x-x_i)^{e_i}$ where all $x_i \in \overline{\Bbbk}$ are distinct, $e_i \in \mathbb{N}$, and $\sum_{i=1}^n e_i = d$. It suffices to compute the divisor of $(x-x_i)$ and show that it has degree 0. The result therefore follows from Lemma 7.7.10.

Now consider a function of the form $a(x) + b(x)y$ on the affine curve $E \cap \mathbb{A}^2$. By Lemma 7.7.12 one has $v_P(a(x)+b(x)y) = v_{\iota(P)}(a(x) + b(x)(-y - H(x)))$ for all points

[6] This innocent-looking fact is actually the hardest result in this chapter to prove. There are several accessible proofs of the general result: Stichtenoth (Theorem I.4.11 of [589]; also see Moreno [439] Lemma 2.2) gives a proof based on "weak approximation" of valuations and this is probably the simplest proof for a reader who has already got this far through the current book; Fulton [216] gives a proof for projective plane curves based on Bézout's theorem; Silverman [564], Shafarevich [543], Hartshorne [278] and Lorenzini [394] all give proofs that boil down to ramification theory of $f : C \to \mathbb{P}^1$, and this is the argument we will give in the next chapter.

$P \in E(\overline{\Bbbk})$. Hence, if $\mathrm{div}(a+by) = \sum_P n_P(P)$ then $\mathrm{div}(a+b(-y-H)) = \sum_P n_P(\iota(P))$ and $\deg(\mathrm{div}(a+by)) = \deg(\mathrm{div}(a+b(-y-H)))$.

Since $(a+by)(a+b(-y-H)) = a^2+ab(y-y-H)+b^2(-y^2-Hy) = a^2-Hab-Fb^2$ is independent of y it follows by the first part of the proof that the affine parts of the divisors of the functions $(a+by)$ and $a+b(-y-H)$ have degree

$$\max\{2\deg(a), \deg(H)+\deg(a)+\deg(b), 3+2\deg(b)\}. \tag{7.9}$$

One can check that the degree in equation (7.9) is $2\deg(a)$ when $\deg(a) \geq \deg(b)+2$ and is $3+2\deg(b)$ when $\deg(a) \leq \deg(b)+1$.

To study the behaviour at infinity consider $(a(x,z)+b(x,z)y)/z^d$ where $d = \max\{\deg(a), \deg(b)+1\}$. By the same argument as before one has $v_{\mathcal{O}_E}(a(x,z)/z^d) = -2\deg(a)$. Similarly, $v_{\mathcal{O}_E}(b(x,z)y/z^d) = v_{\mathcal{O}_E}(b(x,z)/z^{d-1}) + v_{\mathcal{O}_E}(y/z) = -2\deg(b)-3$. It follows by part 3 of Lemma 7.4.14 that $\deg(\mathrm{div}((a(x,z)+b(x,z)y)/z^d)) = 0$.

Finally, consider $f(x,y,z) = f_1(x,y,z)/f_2(x,y,z)$ where f_1 and f_2 are homogeneous of degree d. By the above, $\deg(\mathrm{div}(f_1(x,y,z)/z^d)) = \deg(\mathrm{div}(f_2(x,y,z)/z^d)) = 0$ and the result follows. □

Corollary 7.7.13. *Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)^*$. The following are equivalent:*

1. $\mathrm{div}(f) \geq 0$.
2. $f \in \Bbbk^*$.
3. $\mathrm{div}(f) = 0$.

Proof: Certainly statement 2 implies statement 3 and 3 implies 1. So it suffices to prove 1 implies 2. Let $f \in \Bbbk(C)^*$ be such that $\mathrm{div}(f) \geq 0$. Then f is regular everywhere, so choose some $P_0 \in C(\overline{\Bbbk})$ and define $h = f - f(P_0) \in \overline{\Bbbk}(C)$. Then $h(P_0) = 0$. If $h = 0$ then f is the constant function $f(P_0)$ and, since f is defined over $\Bbbk$, it follows that $f \in \Bbbk^*$. To complete the proof suppose that $h \neq 0$ in $\overline{\Bbbk}(C)$. Since $\deg(\mathrm{div}(h)) = 0$ by Theorem 7.7.11 it follows that h must have at least one pole. But then f has a pole, which contradicts $\mathrm{div}(f) \geq 0$. □

Corollary 7.7.14. *Let C be a curve over $\Bbbk$. Let $f, h \in \Bbbk(C)^*$. Then $\mathrm{div}(f) = \mathrm{div}(h)$ if and only if $f = ch$ for some $c \in \Bbbk^*$.*

Exercise 7.7.15. Prove Corollary 7.7.14.

7.8 Divisor Class Group

We have seen that $\mathrm{Prin}_{\Bbbk}(C) = \{\mathrm{div}(f) : f \in \Bbbk(C)^*\}$ is a subgroup of $\mathrm{Div}^0_{\Bbbk}(C)$. Hence, since all the groups are Abelian, one can define the quotient group; we call this the divisor class group. It is common to use the notation Pic for the divisor class group since the divisor class group of a curve is isomorphic to the Picard group of a curve (even though the Picard group is usually defined differently, in terms of line bundles).

Definition 7.8.1. The (degree zero) **divisor class group** of a curve C over $\Bbbk$ is $\mathrm{Pic}^0_{\Bbbk}(C) = \mathrm{Div}^0_{\Bbbk}(C)/\mathrm{Prin}_{\Bbbk}(C)$.

We call two divisors $D_1, D_2 \in \mathrm{Div}^0_{\Bbbk}(C)$ **linearly equivalent** and write $D_1 \equiv D_2$ if $D_1 - D_2 \in \mathrm{Prin}_{\Bbbk}(C)$. The equivalence class (called a **divisor class**) of a divisor $D \in \mathrm{Div}^0_{\Bbbk}(C)$ under linear equivalence is denoted $\overline{D}$.

Example 7.8.2. By Lemma 7.7.8, $\mathrm{Pic}^0_{\Bbbk}(\mathbb{P}^1) = \{0\}$.

Theorem 7.8.3. *Let C be a curve over $\Bbbk$ and let $f \in \overline{\Bbbk}(C)$. If $\sigma(f) = f$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then $f \in \Bbbk(C)$. If $\mathrm{div}(f)$ is defined over $\Bbbk$ then $f = ch$ for some $c \in \overline{\Bbbk}$ and $h \in \Bbbk(C)$.*

Proof: The first claim follows from Remark 5.4.14 (also see Remark 8.4.11 of Section 8.4).

For the second statement, let $\mathrm{div}(f)$ be defined over $\Bbbk$. Then $\mathrm{div}(f) = \sigma(\mathrm{div}(f)) = \mathrm{div}(\sigma(f))$ where the second equality follows from part 4 of Lemma 7.4.14. Corollary 7.7.14 implies $\sigma(f) = c(\sigma)f$ for some $c(\sigma) \in \overline{\Bbbk}^*$. The function $c : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ is a 1-cocycle (the fact that $c(\sigma\tau) = \sigma(c(\tau))c(\sigma)$ is immediate, the fact that $c : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ is continuous also follows). Hence, Theorem A.7.2 (Hilbert 90) implies that $c(\sigma) = \sigma(\gamma)/\gamma$ for some $\gamma \in \overline{\Bbbk}^*$. In other words, taking $h = f/\gamma \in \overline{\Bbbk}(C)$, we have

$$\sigma(h) = \sigma(f)/\sigma(\gamma) = f/\gamma = h.$$

By the first part of the theorem $h \in \Bbbk(C)$. □

Theorem 7.8.3 has the following important corollary, namely that $\mathrm{Pic}^0_{\Bbbk}(C)$ is a subgroup of $\mathrm{Pic}^0_{\Bbbk'}(C)$ for every extension $\Bbbk'/\Bbbk$.

Corollary 7.8.4. *Let C be a curve over $\Bbbk$ and let $\Bbbk'/\Bbbk$ be an algebraic extension. Then $\mathrm{Pic}^0_{\Bbbk}(C)$ injects into $\mathrm{Pic}^0_{\Bbbk'}(C)$.*

Proof: Suppose a divisor class $\overline{D} \in \mathrm{Pic}^0_{\Bbbk}(C)$ becomes trivial in $\mathrm{Pic}^0_{\Bbbk'}(C)$. Then there is some divisor D on C defined over $\Bbbk$ such that $D = \mathrm{div}(f)$ for some $f \in \Bbbk'(C)^*$. But Theorem 7.8.3 implies $D = \mathrm{div}(h)$ for some $h \in \Bbbk(C)$ and so the divisor class is trivial in $\mathrm{Pic}^0_{\Bbbk}(C)$. □

Corollary 7.8.5. *Let $\Bbbk$ be a finite field. Let C be a curve over $\Bbbk$. Define*

$$\mathrm{Pic}^0_{\overline{\Bbbk}}(C)^{\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)} = \left\{\overline{D} \in \mathrm{Pic}^0_{\overline{\Bbbk}}(C) : \sigma(\overline{D}) = \overline{D} \text{ for all } \sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)\right\}.$$

Then $\mathrm{Pic}^0_{\overline{\Bbbk}}(C)^{\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)} = \mathrm{Pic}^0_{\Bbbk}(C)$.

Proof: (Sketch) Let $G = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Theorem 7.8.3 already showed that $\mathrm{Prin}_{\overline{\Bbbk}}(C)^G = \mathrm{Prin}_{\Bbbk}(C)$ but we re-do the proof in a more explicitly cohomological way, as we need further consequences of the argument.

Take Galois cohomology of the exact sequence

$$1 \to \overline{\Bbbk}^* \to \overline{\Bbbk}(C)^* \to \mathrm{Prin}_{\overline{\Bbbk}}(C) \to 0$$

to get

$$1 \to \Bbbk^* \to (\overline{\Bbbk}(C)^*)^G \to \mathrm{Prin}_{\overline{\Bbbk}}(C)^G \to H^1(G, \overline{\Bbbk}^*) \to H^1(G, \overline{\Bbbk}(C)^*) \to H^1(G, \mathrm{Prin}_{\overline{\Bbbk}}(C)) \to H^2(G, \overline{\Bbbk}^*).$$

Since $(\overline{\Bbbk}(C)^*)^G = \Bbbk(C)$ (Theorem 7.8.3) and $H^1(G, \overline{\Bbbk}^*) = 0$ (Hilbert 90) we have $\mathrm{Prin}_{\overline{\Bbbk}}(C)^G = \mathrm{Prin}_{\Bbbk}(C)$. Further, $H^2(G, \overline{\Bbbk}^*) = 0$ when $\Bbbk$ is finite (see Section X.7 of [542]) and $H^1(G, \overline{\Bbbk}(C)^*) = 0$ (see Silverman Exercise X.10). Hence, $H^1(G, \mathrm{Prin}_{\overline{\Bbbk}}(C)) = 0$.

Now, take Galois cohomology of the exact sequence

$$1 \to \mathrm{Prin}_{\overline{\Bbbk}}(C) \to \mathrm{Div}^0_{\overline{\Bbbk}}(C) \to \mathrm{Pic}^0_{\overline{\Bbbk}}(C) \to 0$$

to get

$$\mathrm{Prin}_{\Bbbk}(C) \to \mathrm{Div}^0_{\overline{\Bbbk}}(C)^G \to \mathrm{Pic}^0_{\overline{\Bbbk}}(C)^G \to H^1(G, \mathrm{Prin}_{\overline{\Bbbk}}(C)) = 0.$$

Now, $\mathrm{Div}^0_{\overline{\Bbbk}}(C)^G = \mathrm{Div}^0_{\Bbbk}(C)$ by definition and so the result follows. □

We minimise the use of the word Jacobian in this book, however we make a few remarks here. We have associated to a curve C over a field $\Bbbk$ the divisor class group $\mathrm{Pic}^0_{\Bbbk}(C)$. This group can be considered as an algebraic group. To be precise, there is a variety J_C (called the **Jacobian variety** of C) that is an algebraic group (i.e., there is a morphism[7] $+ : J_C \times J_C \to J_C$) and such that, for any extension $\mathbb{K}/\Bbbk$, there is a bijective map between $\mathrm{Pic}^0_{\mathbb{K}}(C)$ and $J_C(\mathbb{K})$ that is a group homomorphism.

One can think of Pic^0 as a functor that, given a curve C over $\Bbbk$, associates with every field extension $\Bbbk'/\Bbbk$ a group $\mathrm{Pic}^0_{\Bbbk'}(C)$. The Jacobian variety of the curve is a variety J_C over $\Bbbk$ whose $\Bbbk'$-rational points $J_C(\Bbbk')$ are in one-to-one correspondence with the elements of $\mathrm{Pic}^0_{\Bbbk'}(C)$ for all $\Bbbk'/\Bbbk$. For most applications it is sufficient to work in the language of divisor class groups rather than Jacobians (despite our remarks about algebraic groups in Chapter 4).

7.9 Elliptic Curves

The goal of this section is to show that the 'traditional' **chord-and-tangent rule** for elliptic curves does give a group operation. Our approach is to show that this operation coincides with addition in the divisor class group of an elliptic curve. Hence, elliptic curves are an algebraic group.

First we state the chord-and-tangent rule without justifying any of the claims or assumptions made in the description. The results later in the section will justify these claims (see Remark 7.9.4). For more details about the chord-and-tangent rule see Washington [626], Cassels [122], Reid [497] or Silverman and Tate [567].

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the affine part of an elliptic curve E. Draw the line $l(x, y) = 0$ between P_1 and P_2 (if $P_1 \neq P_2$ then this is called a chord; if $P_1 = P_2$ then let the line be the tangent to the curve at P_1). Denote by R the third point[8] of intersection (counted according to multiplicities) of the line with the curve E. Now draw the line $v(x) = 0$ between $\mathcal{O}_E$ and R (if $R = \mathcal{O}_E$ then this is the "line at infinity" and if R is an affine point this is a vertical line so a function of x only). Denote by S the third point of intersection of this line with the curve E. Then one defines $P_1 + P_2$ to be S. Over the real numbers this operation is illustrated in Figure 7.1.

We now transform the above geometric description into algebra, and show that the points R and S do exist. The first step is to write down the equation of the line between $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. We state the equation of the line as a definition and then show that it corresponds to a function with the correct divisor.

Definition 7.9.1. Let $E(x, y)$ be a Weierstrass equation for an elliptic curve over $\Bbbk$. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\Bbbk) \cap \mathbb{A}^2$. If $P_1 = \iota(P_2)$ then the line between P_1 and P_2 is[9] $v(x) = x - x_1$.

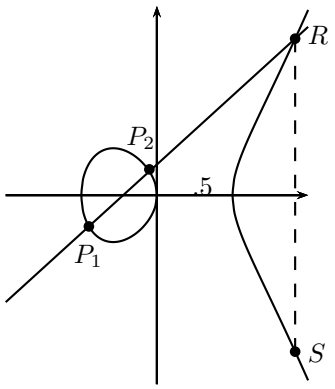
If $P_1 \neq \iota(P_2)$ then there are two subcases. If $P_1 = P_2$ then define $\lambda = (3x_1^2 + 2a_2x_1 + a_4)/(2y_1 + a_1x_1 + a_3)$ and if $P_1 \neq P_2$ then define $\lambda = (y_2 - y_1)/(x_2 - x_1)$. The line between P_1 and P_2 is then

$$l(x, y) = y - \lambda(x - x_1) - y_1.$$

We stress that whenever we write $l(x, y)$ then we are implicitly assuming that it is not a vertical line $v(x)$.

[7] To make this statement precise requires showing that $J_C \times J_C$ is a variety.
[8] Possibly this point is at infinity.
[9] This includes the case $P_1 = P_2 = \iota(P_1)$.

Figure 7.1: Chord and tangent rule for elliptic curve addition.



Warning: Do not confuse the line $v(x)$ with the valuation v_P. The notation $v(P)$ means the line evaluated at the point P. The notation $v_P(x)$ means the valuation of the function x at the point P.

Exercise 7.9.2. Let the notation be as in Definition 7.9.1. Show that if $P_1 = \iota(P_2)$ then $v(P_1) = v(P_2) = 0$ and if $P_1 \neq \iota(P_2)$ then $l(P_1) = l(P_2) = 0$.

Lemma 7.9.3. *Let $P_1 = (x_1, y_1) \in E(\Bbbk)$ and let $P_2 = \iota(P_1)$. Let $v(x) = (x - x_1)$ as in Definition 7.9.1. Then* $\mathrm{div}(v(x)) = (P_1) + (P_2) - 2(\mathcal{O}_E)$.

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\Bbbk)$ be such that $P_1 \neq \iota(P_2)$ and let $l(x, y) = y - \lambda(x - x_1) - y_1$ be as in Definition 7.9.1. Then there exists $x_3 \in \Bbbk$ such that $E(x, \lambda(x - x_1) + y_1) = -\prod_{i=1}^{3}(x - x_i)$ and $\mathrm{div}(l(x, y)) = (P_1) + (P_2) + (R) - 3(\mathcal{O}_E)$ *where $R = (x_3, \lambda(x_3 - x_1) + y_1)$.*

Proof: The first part is just a restatement of Lemma 7.7.10.

For the second part, set $G(x) = -E(x, \lambda(x - x_1) + y_1)$, which is a monic polynomial over $\Bbbk$ of degree 3. Certainly x_1 and x_2 are roots of $G(x)$ over $\Bbbk$ so if $x_1 \neq x_2$ then $G(x)$ has a third root x_3 over $\Bbbk$. In the case $x_1 = x_2$ we have $P_1 = P_2 \neq \iota(P_2)$. Make a linear change of variables so that $(x_1, y_1) = (x_2, y_2) = 0$. The curve equation is $E(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x)$ and $a_3 \neq 0$ since $(0, 0) \neq \iota(0, 0)$. Now, by definition, $l(x, y) = a_4x/a_3$ and one has

$$G(x) = E(x, a_4x/a_3) = (a_4x/a_3)^2 + a_1x(a_4x/a_3) + a_4x - (x^3 + a_2x^2 + a_4x)$$

which is divisible by x^2. Hence $G(x)$ splits completely over $\Bbbk$.

For the final part we consider $l(x, y)$ as a function on the affine curve. By Lemma 7.4.14 and Lemma 7.4.16 we have $v_{\mathcal{O}_E}(l(x, y)) = \min\{v_{\mathcal{O}_E}(y), v_{\mathcal{O}_E}(x), v_{\mathcal{O}_E}(1)\} = -3$. Since $\deg(\mathrm{div}(l(x, y))) = 0$ there are three affine zeroes counted according to multiplicity.

Define $\overline{l}(x, y) = y + (a_1x + a_3) + \lambda(x - x_1) + y_1$. Note that $\overline{l} = -l \circ \iota$ so $v_P(l(x, y)) = v_{\iota(P)}(\overline{l}(x, y))$ (also see Lemma 7.7.12). One can check that

$$l(x, y)\overline{l}(x, y) = -E(x, \lambda(x - x_1) + y_1) = \prod_{i=1}^{3}(x - x_i) \tag{7.10}$$

where the first equality is equivalence modulo $E(x,y)$, not equality of polynomials. Hence, for any point $P \in E(\Bbbk)$,

$$v_P(l(x,y)) + v_P(\overline{l}(x,y)) = v_P\left(\prod_{i=1}^{3}(x-x_i)\right).$$

Write $P_i = (x_i, y_i)$, let e_i be the multiplicity of x_i in the right hand side of equation (7.10) and recall that $v_{P_i}(x - x_i) = 1$ if $P_i \neq \iota(P_i)$ and 2 otherwise. Also note that $l(P_i) = 0$ implies $\overline{l}(P_i) \neq 0$ unless $P_i = \iota(P_i)$, in which case $v_{P_i}(l(x,y)) = v_{P_i}(\overline{l}(x,y))$. It follows that $v_{P_i}(l(x,y)) = e_i$, which proves the result. □

Remark 7.9.4. It follows from the above results that it does make sense to speak of the "third point of intersection" R of $l(x,y)$ with E and to call $l(x,y)$ a tangent line in the case when $P_1 = P_2$. Hence, we have justified the assumptions made in the informal description of the chord-and-tangent rule.

Exercise 7.9.5. Let $E(x,y,z)$ be a Weierstrass equation for an elliptic curve. The line $z = 0$ is called the line at infinity on E. Show that $z = 0$ only passes through $(0,0)$ on the affine curve given by the equation $E(x,1,z) = 0$.

Exercise 7.9.6. Prove that the following algebraic formulae for the chord-and-tangent rule are correct. Let $P_1, P_2 \in E(\Bbbk)$, we want to compute $S = P_1 + P_2$. If $P_1 = \mathcal{O}_E$ then $S = P_2$ and if $P_2 = \mathcal{O}_E$ then $S = P_1$. Hence we may now assume that $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are affine. If $y_2 = -y_1 - H(x_1)$ then $S = \mathcal{O}_E$. Otherwise, set λ to be as in Definition 7.9.1 and compute $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = -\lambda(x_S - x_1) - y_1$. The sum is $S = (x_3, y_3)$.

Before proving the main theorem, we state the following technical result, whose proof is postponed to the next chapter (Corollary 8.6.5).

Theorem 7.9.7. *Let $P_1, P_2 \in E(\Bbbk)$ be a points on an elliptic curve such that $P_1 \neq P_2$. Then $(P_1) - (P_2)$ is not a principal divisor.*

We now consider the divisor class group $\mathrm{Pic}^0_{\Bbbk}(E)$. The following result is usually obtained as a corollary to the Riemann-Roch theorem, but we give an ad-hoc proof for elliptic curves. One can consider this result as the Abel-Jacobi map in the case of genus 1 curves.

Theorem 7.9.8. *There is a one-to-one correspondence between $E(\Bbbk)$ and $\mathrm{Pic}^0_{\Bbbk}(E)$, namely $P \mapsto (P) - (\mathcal{O}_E)$.*

Proof: We first show that the map is injective. Suppose $(P_1) - (\mathcal{O}_E) \equiv (P_2) - (\mathcal{O}_E)$. Then $(P_1) - (P_2)$ is principal, and so Theorem 7.9.7 implies $P_1 = P_2$.

It remains to show that the map is surjective. Let $D = \sum_P n_P(P)$ be any effective divisor on E. We prove that D is equivalent to a divisor of the form

$$(P) + (\deg(D) - 1)(\mathcal{O}_E). \tag{7.11}$$

We will do this by replacing any term $(P_1) + (P_2)$ by a term of the form $(S) + (\mathcal{O}_E)$ for some point S.

The key equations are $(P) + (\iota(P)) = 2(\mathcal{O}_E) + \mathrm{div}(v(x))$ where $v(x)$ is as in Definition 7.9.1, or, if $P_1 \neq \iota(P_2)$, $(P_1) + (P_2) = (S) + (\mathcal{O}_E) + \mathrm{div}(l(x,y)/v(x))$. The first equation allows us to replace any pair $(P) + (\iota(P))$, including the case $P = \iota(P)$, by $2(\mathcal{O}_E)$. The second equation allows us to replace any pair $(P_1) + (P_2)$, where $P_1 \neq \iota(P_2)$

(but including the case $P_1 = P_2$) with $(S)+(\mathcal{O}_E)$. It is clear that any pair of affine points is included in one of these two cases, and so repeating these operations a finite number of times reduces any effective divisor to the form in equation (7.11).

Finally, let D be a degree zero divisor on E. Write $D = D_1 - D_2$ where D_1 and D_2 are effective divisors of the same degree. By the above argument we can write $D_1 \equiv (S_1) + (\deg(D_1) - 1)(\mathcal{O}_E)$ and $D_2 \equiv (S_2) + (\deg(D_1) - 1)(\mathcal{O}_E)$. Hence $D \equiv (S_1) - (S_2)$. Finally, adding the divisor of the vertical line function through S_2 and subtracting the divisor of the line between S_1 and $\iota(S_2)$ gives $D \equiv (S)-(\mathcal{O}_E)$ for some point S as required. □

Since $E(\Bbbk)$ is in bijection with the group $\mathrm{Pic}^0_{\Bbbk}(E)$ it follows that $E(\Bbbk)$ is a group, with the group law coming from the divisor class group structure of E. It remains to show that the group law is just the chord-and-tangent rule. In other words, this result shows that the chord-and-tangent rule is associative. Note that many texts prove that both $E(\Bbbk)$ and $\mathrm{Pic}^0_{\Bbbk}(E)$ are groups and then prove that the map $P \mapsto (P) - (\mathcal{O}_E)$ is a group homomorphism; whereas we use this map to prove that $E(\Bbbk)$ is a group.

Theorem 7.9.9. *Let E be an elliptic curve over a field $\Bbbk$. The group law induced on $E(\Bbbk)$ by pulling back the divisor class group operations via the bijection of Theorem 7.9.8 is the chord-and-tangent rule.*

Proof: Let $P_1, P_2 \in E(\Bbbk)$. To add these points we map them to divisor classes $(P_1)-(\mathcal{O}_E)$ and $(P_2) - (\mathcal{O}_E)$ in $\mathrm{Pic}^0_{\Bbbk}(E)$. Their sum is $(P_1) + (P_2) - 2(\mathcal{O}_E)$, which is reduced to the form $(S) - (\mathcal{O}_E)$ by applying the rules in the proof of Theorem 7.9.8. In other words, we get $(P_1) + (P_2) - 2(\mathcal{O}_E) = (S) - (\mathcal{O}_E) + \mathrm{div}(f(x, y))$ where $f(x, y) = v(x)$ if $P_1 = \iota(P_2)$ or $f(x, y) = l(x, y)/v(x)$ in the general case, where $l(x, y)$ and $v(x)$ are the lines from Definition 7.9.1. Since these are precisely the same lines as in the description of the chord-and-tangent rule it follows that the point S is the same point as produced by the chord-and-tangent rules. □

A succinct way to describe the elliptic curve addition law (since there is a single point at infinity) is that three points sum to zero if they lie on a line. This is simply a restatement of the fact that if P, Q and R line on the line $l(x, y, z) = 0$ then the divisor $(P) + (Q) + (R) - 3(\mathcal{O}_E)$ is a principal divisor.

Exercise 7.9.10. One can choose any $\Bbbk$-rational point $P_0 \in E(\Bbbk)$ and define a group law on $E(\Bbbk)$ such that P_0 is the identity element. The sum of points P and Q is defined as follows: let l be the line through P and Q (taking the tangent if $P = Q$, which uniquely exists since E is non-singular). Then l hits E at a third point (counting multiplicities) R. Draw a line v between P_0 and R. This hits E at a third point (again counting with multiplicities) S. Then $P + Q$ is defined to be the point S. Show that this operation satisfies the axioms of a group.

Chapter 8

Rational Maps on Curves and Divisors

The purpose of this chapter is to develop some tools in the theory of algebraic curves that are needed for the applications (especially, hyperelliptic curve cryptography). The technical machinery in this chapter is somewhat deeper than the previous one and readers can skip this chapter if they wish.

The reader should note that the word "curve" in this chapter always refers to a non-singular curve.

8.1 Rational Maps of Curves and the Degree

Lemma 8.1.1. *Let C be a curve over $\mathbb{k}$ and $f \in \mathbb{k}(C)$. One can associate with f a rational map $\phi : C \to \mathbb{P}^1$ over $\mathbb{k}$ by $\phi = (f : 1)$. (Indeed, this is a morphism by Lemma 7.3.6.) Denote by ∞ the constant map $\infty(P) = (1 : 0)$. Then there is a one-to-one correspondence between $\mathbb{k}(C) \cup \{\infty\}$ and the set of morphisms $\phi : C \to \mathbb{P}^1$.*

Exercise 8.1.2. Prove Lemma 8.1.1.

Note that since $\mathbb{k}(C) \cup \{\infty\}$ is not a field, it does not make sense to interpret the set of rational maps $\phi : C \to \mathbb{P}^1$ as a field.

Lemma 8.1.3. *Let C_1 and C_2 be curves over $\mathbb{k}$ (in particular, non-singular and projective) and let $\phi : C_1 \to C_2$ be a non-constant rational map over $\mathbb{k}$. Then ϕ is a dominant morphism.*

Proof: By Lemma 7.3.6, ϕ is a morphism. By Lemma 5.5.17 and Exercise 5.5.19 we know that the Zariski closure Z of $\phi(C_1)$ is an irreducible algebraic set. Suppose $Z \neq C_2$. We may intersect with an affine space so that $Z \cap \mathbb{A}^n \neq \varnothing$. It follows that $Z \cap \mathbb{A}^n \neq C_2 \cap \mathbb{A}^n$

(otherwise their projective closures are equal and $Z = C_2$). Hence $I_{\overline{\Bbbk}}(C_2) \subsetneq I_{\overline{\Bbbk}}(Z)$. By Theorem 5.6.8 it follows that $\dim(Z) = 0$ and so, by Exercise 5.6.6, $Z = \{P\}$ for some $P \in C_2(\overline{\Bbbk})$. □

The notion of degree of a mapping is fundamental in algebra and topology; a degree d map is "d-to-one on most points".

Example 8.1.4. Let $\Bbbk$ be a field of characteristic not equal to 2. The morphism $\phi : \mathbb{A}^1(\Bbbk) \to \mathbb{A}^1(\Bbbk)$ given by $\phi(x) = x^2$ is clearly two-to-one away from the point $x = 0$. We say that ϕ has degree 2.

Example 8.1.4 suggests several possible definitions for degree: the first in terms of the number of pre-images of a general point in the image; the second in terms of the degrees of the polynomials defining the map. A third definition is to recall the injective field homorphism $\phi^* : \Bbbk(\mathbb{A}^1) \to \Bbbk(\mathbb{A}^1)$. One sees that $\phi^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(x^2) \subseteq \Bbbk(x)$ and that $[\Bbbk(x) : \Bbbk(x^2)] = 2$. This latter formulation turns out to be a suitable definition for degree.

Theorem 8.1.5. *Let C_1, C_2 be curves over $\Bbbk$. Let $\phi : C_1 \to C_2$ be a non-constant rational map over $\Bbbk$. Then $\Bbbk(C_1)$ is a finite algebraic extension of $\phi^*(\Bbbk(C_2))$.*

Proof: By Lemma 8.1.3, ϕ is a dominant morphism and hence by Theorem 5.5.24, $\phi^* : \Bbbk(C_2) \to \Bbbk(C_1)$ is an injective field homorphism. It follows that $\phi^*(\Bbbk(C_2))$ is a subfield of $\Bbbk(C_1)$. Since $\phi^*(\Bbbk(C_2))$ is isomorphic to $\Bbbk(C_2)$ it has transcendence degree 1. Since $\Bbbk(C_1)$ also has transcendence degree 1 it follows from Theorem A.6.5 that $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$ is an algebraic extension. Finally, $\Bbbk(C_1)$ is a finite algebraic extension of $\phi^*(\Bbbk(C_2))$ since $\Bbbk(C_1)$ is finitely generated over $\Bbbk$. □

Definition 8.1.6. Let $\phi : C_1 \to C_2$ be a non-constant rational map of curves over $\Bbbk$. The **degree** of ϕ is $[\Bbbk(C_1) : \phi^*(\Bbbk(C_2))]$.

Let F be a field such that $\phi^*(\Bbbk(C_2)) \subset F \subset \Bbbk(C_1)$ and $\Bbbk(C_1)/F$ is separable and $F/\phi^*(\Bbbk(C_2))$ is purely inseparable (recall the notion of separability from Section A.6). The **separable degree** of ϕ is $\deg_s(\phi) = [\Bbbk(C_1) : F]$ and the **inseparable degree** of ϕ is $\deg_i(\phi) = [F : \phi^*(\Bbbk(C_2))]$.

A non-constant rational map of curves is called **separable** (respectively, **inseparable**) if its inseparable (resp., separable) degree is 1.

Example 8.1.7. Let $\Bbbk = \mathbb{F}_p$. The **Frobenius map** $\pi_p : \mathbb{A}^1(\overline{\Bbbk}) \to \mathbb{A}^1(\overline{\Bbbk})$ is given by $\pi_p(x) = x^p$. Since $\Bbbk(\mathbb{A}^1) = \Bbbk(x)$ and $\pi_p^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(x^p)$ it follows that $\Bbbk(x)/\pi_p^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(x)/\Bbbk(x^p)$ is inseparable of degree p. Hence $\deg_s(\pi_p) = 1$ and $\deg(\pi_p) = \deg_i(\pi_p) = p$. Note that π_p is one-to-one on $\mathbb{A}^1(\overline{\mathbb{F}}_p)$, not p-to-one.

Lemma 8.1.8. *Let $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ be a non-constant morphism over $\Bbbk$ given by $\phi(x) = a(x)$ for some polynomial $a(x) \in \Bbbk[x]$. Then $\deg(\phi) = \deg_x(a(x))$.*

Proof: Let $\theta = a(x)$. We have $\phi^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(\theta) \subseteq \Bbbk(x)$ and we are required to determine $[\Bbbk(x) : \Bbbk(\theta)]$. We claim the minimal polynomial of x over $\Bbbk(\theta)$ is given by

$$F(T) = a(T) - \theta.$$

First, it is clear that $F(x) = 0$. Second, it follows from Eisenstein's criteria (see Proposition III.1.14 of [589], Theorem IV.3.1 of [367] or Theorem III.6.15 of [301]), taking for example the place (i.e., valuation) at infinity in $\Bbbk(\theta)$, that $F(T)$ is irreducible. Since $\deg_T(F(T)) = \deg_x(a(x))$ the result follows. □

Lemma 8.1.9. *Let $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ be a non-constant rational map over $\Bbbk$ given by $\phi(x) = a(x)/b(x)$ where $\gcd(a(x), b(x)) = 1$. Then $\deg(\phi) = \max\{\deg_x(a(x)), \deg_x(b(x))\}$.*

Proof: Let $\theta = a(x)/b(x)$ so that $\phi^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(\theta) \subseteq \Bbbk(x)$. Since $\Bbbk(\theta) = \Bbbk(1/\theta)$ we may assume $\deg_x(a(x)) \geq \deg_x(b(x))$. If these degrees are equal then one can reduce the degree of $a(x)$ by using $\Bbbk(a(x)/b(x)) = \Bbbk((a(x) - cb(x))/b(x))$ for a suitable $c \in \Bbbk$; replacing θ by $1/\theta$ again we may assume that $\deg_x(a(x)) > \deg_x(b(x))$. We may also assume that $a(x)$ and $b(x)$ are monic.

We claim the minimal polynomial of x over $\Bbbk(\theta)$ is given by

$$F(T) = a(T) - \theta b(T).$$

To see this, first note that $F(x) = 0$. Now, $a(T) - \theta b(T)$ is irreducible in $\Bbbk[\theta, T]$ since it is linear in θ. The irreducibility of $F(T)$ in $\Bbbk(\theta)[T]$ then follows from the Gauss Lemma (see, for example, Lemma III.6.13 of Hungerford [301]). □

Exercise 8.1.10. Let $C_1 : y^2 = x^3$ and $C_2 : Y^2 = X$ over a field $\Bbbk$ of characteristic not equal to 2 and consider the map $\phi : C_1 \to C_2$ such that $\phi(x, y) = (x, y/x)$. Show that $\deg(\phi) = 1$.

Exercise 8.1.11. Let $C_1 : y^2 = x^6 + 2x^2 + 1$ and $C_2 : Y^2 = X^3 + 2X + 1$ over a field $\Bbbk$ of characteristic not equal to 2 and consider the map $\phi : C_1 \to C_2$ such that $\phi(x, y) = (x^2, y)$. Show that $\deg(\phi) = 2$.

Exercise 8.1.12. Let C_1, C_2 and C_3 be curves over $\Bbbk$ and let $\psi : C_1 \to C_2$ and $\phi : C_2 \to C_3$ be morphisms over $\Bbbk$. Show that $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$.

Lemma 8.1.13. *Let C_1 and C_2 be curves over $\Bbbk$ (in particular, smooth and projective). Let $\phi : C_1 \to C_2$ be a birational map over $\Bbbk$. Then ϕ has degree 1.*

Proof: Write ϕ^{-1} for the rational map from C_2 to C_1 such that $\phi^{-1} \circ \phi$ is the identity on an open subset of C_1. Then $(\phi^{-1} \circ \phi)^*$ is the identity map on $\Bbbk(C_1)$ and it also factors as $\phi^* \circ (\phi^{-1})^*$. Since $1 = [\Bbbk(C_1) : (\phi^{-1} \circ \phi)^*\Bbbk(C_1)] = [\Bbbk(C_1) : \phi^*\Bbbk(C_2)][\Bbbk(C_2) : (\phi^{-1})^*\Bbbk(C_1)]$ the result follows. □

For Lemma 8.1.15 (and Lemma 8.2.6) we need the following technical result. This is a special case of weak approximation; see Stichtenoth [589] for a presentation that uses similar techniques to obtain most of the results in this chapter.

Lemma 8.1.14. *Let C be a curve over $\Bbbk$ and let $Q, Q' \in C(\overline{\Bbbk})$ be distinct points. Then there is a function $f \in \overline{\Bbbk}(C)$ such that $v_Q(f) = 0$ and $v_{Q'}(f) > 0$.*

Proof: By Lemma 7.1.19 we have $\mathcal{O}_{Q',\overline{\Bbbk}} \not\subseteq \mathcal{O}_{Q,\overline{\Bbbk}}$ (and vice versa). Hence, there exists a function $u \in \mathcal{O}_{Q,\overline{\Bbbk}} - \mathcal{O}_{Q',\overline{\Bbbk}}$. Then $v_Q(u) \geq 0$ while $v_{Q'}(u) < 0$. If $u(Q) = -1$ then set $f = 1/(1 + u^2)$ else set $f = 1/(1 + u)$. Then $v_Q(f) = 0$ and $v_{Q'}(f) > 0$ as required. □

Lemma 8.1.15. *Let C_1 and C_2 be curves over $\Bbbk$ (in particular, smooth and projective). Let $\phi : C_1 \to C_2$ be a rational map over $\Bbbk$ of degree 1. Then ϕ is an isomorphism.*

Proof: Since ϕ has degree 1 it follows that $\phi^*(\Bbbk(C_2)) = \Bbbk(C_1)$ and so $\Bbbk(C_2) \cong \Bbbk(C_1)$. The inverse of ϕ^* induces a rational map $\phi^{-1} : C_2 \to C_1$. Since C_1 and C_2 are non-singular and projective it follows from Lemma 7.3.6 that $\phi : C_1 \to C_2$ and $\phi^{-1} : C_2 \to C_1$ are actually morphisms. It follows that $\phi^{-1} \circ \phi : C_1 \to C_1$ and $\phi \circ \phi^{-1} : C_2 \to C_2$ are morphisms.

It remains to show that these maps are both the identity. Without loss of generality we consider $\psi = \phi^{-1} \circ \phi$. Suppose for contradiction that there are points $P, Q \in C_1(\overline{\Bbbk})$ such that $\psi(P) = Q \neq P$. There exists a function f on C_1 such that $f(P) = 0$ and $f(Q) \neq 0$ (see Lemma 8.1.14). But ψ^* is the identity map on $\Bbbk(C_1)$. Hence $\psi^*(f) = f$. But $\psi^*(f) = f \circ \psi$ and so $0 = f(P) = (f \circ \psi)(P) = f(Q) \neq 0$, which is a contradiction. □

8.2 Extensions of Valuations

Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then $F_1 = \Bbbk(C_1)$ is a finite extension of $F_2 = \phi^*(\Bbbk(C_2))$. We now study the preimages of points $Q \in C_2(\overline{\Bbbk})$ under ϕ and a notion of multiplicity of preimages of Q (namely, ramification indices). The main result is Theorem 8.2.12.

There are several approaches to these results in the literature. One method, which unifies algebraic number theory and the theory of curves, is to note that if U is an open subset of C then $\Bbbk[U]$ is a Dedekind domain. The splitting of the maximal ideal $\mathfrak{m}_Q$ of $\Bbbk[U]$ (for $Q \in U$) in the integral closure of $\phi^*(\Bbbk[U])$ in $\Bbbk(C_1)$ yields the results. Details of this approach are given in Section VII.5 of Lorenzini [394], Section I.4 of Serre [542] (especially Propositions I.10 and I.11), Chapter 1 of Lang [365] and Chapter XII of Lang [367]. An analogous ring-theoretic formulation is used in Proposition II.6.9 of Hartshorne [278]. A different method is to study extensions of valuations directly, for example see Section III.1 of Stichtenoth [589]. Note that, since we consider points over $\overline{\Bbbk}$, the notion of residue degree does not arise, which simplifies the presentation compared with many texts.

Definition 8.2.1. Let F_2 be a field of transcendence degree 1 over $\overline{\Bbbk}$. Let F_1/F_2 be a finite extension. Let v be a discrete valuation on F_2. A valuation v' on F_1 is an **extension** of v (or, v is the **restriction** of v') if $\{f \in F_2 : v(f) \geq 0\} = \{f \in F_2 : v'(f) \geq 0\}$. We write $v' \mid v$ if this is the case.

Note that if v' is an extension of v as above then one does not necessarily have $v'(f) = v(f)$ for all $f \in F_2$ (indeed, we will see later that $v'(f) = ev(f)$ for some $e \in \mathbb{N}$).

Lemma 8.2.2. *Let F_1/F_2 be a finite extension and let $v' \mid v$ be valuations on F_1 and F_2 respectively. Then R_v is a subring of $R_{v'}$, $R_v = R_{v'} \cap F_2$ and $\mathfrak{m}_v = \mathfrak{m}_{v'} \cap F_2$. In particular, for $f \in F_2$, $v(f) = 0$ if and only if $v'(f) = 0$.*

Exercise 8.2.3. Prove Lemma 8.2.2.

Theorem 8.2.4. *Let F_1/F_2 be a finite extension of fields and let v be a valuation on F_2. Then there is at least one (and only finitely many) valuation v' of F_1 such that $v' \mid v$.*

Proof: See Theorem XII.4.1 and Corollary XII.4.9 of Lang [367] or Proposition III.1.7(b) of Stichtenoth [589]. □

Let $\phi : C_1 \to C_2$ be a morphism of curves and let $F_2 = \phi^*(\Bbbk(C_2))$ and $F_1 = \Bbbk(C_1)$. We now explain the relation between extensions of valuations from F_2 to F_1 and pre-images of points under ϕ.

Lemma 8.2.5. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$ (this is short-hand for C_1, C_2 and ϕ all being defined over $\Bbbk$). Let $P \in C_1(\overline{\Bbbk})$ and $Q \in C_2(\overline{\Bbbk})$. Denote by v the valuation on $\phi^*(\Bbbk(C_2)) \subseteq \Bbbk(C_1)$ defined by $v(\phi^*(f)) = v_Q(f)$ for $f \in \Bbbk(C_2)$. If $\phi(P) = Q$ then v_P is an extension of v.*

Proof: Let $f \in \Bbbk(C_2)$. Since $\phi(P) = Q$ we have $\phi^*(f) = f \circ \phi$ regular at P if and only if f is regular at Q. Hence $v_P(\phi^*(f)) \geq 0$ if and only if $v_Q(f) \geq 0$. It follows that $v_P \mid v$. □

Lemma 8.2.6. *Let the notation be as in Lemma 8.2.5. In particular, $P \in C_1(\overline{\Bbbk}), Q \in C_2(\overline{\Bbbk}), v_P$ is the corresponding valuation on $F_1 = \overline{\Bbbk}(C_1)$ and v is the valuation on $\phi^*(\overline{\Bbbk}(C_2))$ corresponding to v_Q on $\overline{\Bbbk}(C_2)$. Then $v_P \mid v$ implies $\phi(P) = Q$.*

Proof: Suppose $\phi(P) = Q' \neq Q$. By Lemma 8.1.14 there is some $f \in \overline{\Bbbk}(C_2)$ such that $f(Q) \neq 0$ and $f(Q') = 0$. Then $0 = v_Q(f) = v(\phi^*(f)) = v_P(\phi^*(f))$ (the last equality

by Lemma 8.2.2 and since $v_P \mid v$). But $\phi^*(f)(P) = f \circ \phi(P) = f(Q') = 0$, which is a contradiction. □

In other words, Lemmas 8.2.5 and 8.2.6 show that $\phi(P) = Q$ if and only if the maximal ideal $\mathfrak{m}_P$ in $\mathcal{O}_P \subseteq \Bbbk(C_1)$ contains $\phi^*(\mathfrak{m}_Q)$ where $\mathfrak{m}_Q$ is the maximal ideal in $\mathcal{O}_Q \subseteq \Bbbk(C_2)$. This is the connection between the behaviour of points under morphisms and the splitting of ideals in Dedekind domains.

We already know that a non-constant morphism of curves is dominant, but the next result makes the even stronger statement that a morphism is surjective.

Theorem 8.2.7. *Let C_1 and C_2 be curves over $\Bbbk$ (in particular, they are projective and non-singular). Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then ϕ is surjective from $C_1(\overline{\Bbbk})$ to $C_2(\overline{\Bbbk})$.*

Proof: Let $Q \in C_2(\overline{\Bbbk})$ and let v be the corresponding valuation on $\phi^*(\overline{\Bbbk}(C_2))$. By Theorem 8.2.4 there is a valuation v' on $\overline{\Bbbk}(C_1)$ that extends v. Theorem 7.5.2 shows that $v' = v_P$ for some $P \in C_1(\overline{\Bbbk})$. Finally, Lemma 8.2.6 shows that $\phi(P) = Q$. □

Definition 8.2.8. Let C_1 and C_2 be curves over $\Bbbk$ and let $\phi : C_1 \to C_2$ be a non-constant rational map over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$. The **ramification index** of ϕ at P is

$$e_\phi(P) = v_P(\phi^*(t_{\phi(P)}))$$

where $t_{\phi(P)}$ is a uniformizer on C_2 at $\phi(P)$. If $e_\phi(P) = 1$ for all $P \in C_1(\overline{\Bbbk})$ then ϕ is **unramified**.

We now show that this definition agrees with Definition III.1.5 of Stichtenoth [589].

Lemma 8.2.9. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$, $Q = \phi(P) \in C_2(\overline{\Bbbk})$ and $f \in \overline{\Bbbk}(C_2)$. Then*

$$v_P(\phi^*(f)) = e_\phi(P) v_Q(f).$$

Proof: Let $v_Q(f) = n$ and write $f = t_Q^n h$ for some $h \in \overline{\Bbbk}(C_2)$ such that $h(Q) \neq 0$. Then $\phi^*(f) = \phi^*(t_Q)^n \phi^*(h)$ and $v_P(\phi^*(h))) = 0$. The result follows since $v_P(\phi^*(t_Q)^n) = n v_P(\phi^*(t_Q))$. □

Exercise 8.2.10. Let $\phi : C_1 \to C_2$ be a non-constant rational map of curves over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$, $Q = \phi(P)$, and suppose $e_\phi(P) = 1$. Show that $t \in \overline{\Bbbk}(C_2)$ is a uniformizer at Q if and only if $\phi^*(t)$ is a uniformizer at P.

Exercise 8.2.11. Let $\phi : C_1 \to C_2$ be an isomorphism of curves over $\Bbbk$. Show that ϕ is unramified.

The following result is of fundamental importance.

Theorem 8.2.12. *Let C_1 and C_2 be curves over $\Bbbk$ and let $\phi : C_1 \to C_2$ be a non-constant rational map over $\Bbbk$. Then for all $Q \in C_2(\overline{\Bbbk})$ we have*

$$\sum_{P \in C_1(\overline{\Bbbk}) : \phi(P) = Q} e_\phi(P) \quad = \quad \deg(\phi).$$

Proof: As mentioned above, one can see this by noting that $\phi^*(\mathcal{O}_Q)$ and $\phi^*(\Bbbk[U])$ (for an open set $U \subseteq C_2$ with $Q \in U$) are Dedekind domains and studying the splitting of $\mathfrak{m}_Q$ in their integral closures in $\Bbbk(C_1)$. For details see any of Proposition 1.10 and 1.11 of Serre [542], Corollary XII.6.3 of Lang [367], Proposition I.21 of Lang [365], Theorem III.3.5 of Lorenzini [394], Proposition II.6.9 of Hartshorne [278], or Theorem III.1.11 of Stichenoth [589]. □

Corollary 8.2.13. *If $\phi : C_1 \to C_2$ is a rational map of degree d and $Q \in C_2(\overline{\Bbbk})$ then there are at most d points $P \in C_1(\overline{\Bbbk})$ such that $\phi(P) = Q$.*

Furthermore, if ϕ is separable then there is an open subset $U \subseteq C_2$ such that for all $Q \in U$ one has $\#\phi^{-1}(Q) = d$.

Proof: The first statement is immediate. The second follows by choosing U to be the complement of points corresponding to factors of the discriminant of $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$; see Proposition VII.5.7 of Lorenzini [394]. □

Example 8.2.14. Consider $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ given by $\phi(x) = x^2$ as in Example 8.1.4. This extends to the morphism $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ given by $\phi((x : z)) = (x^2/z^2 : 1)$, which is regular at $\infty = (1 : 0)$ via the equivalent formula $(1 : z^2/x^2)$. One has $\phi^{-1}((a : 1)) = \{(\sqrt{a} : 1), (-\sqrt{a} : 1)\}$, $\phi^{-1}((0 : 1)) = \{(0 : 1)\}$ and $\phi^{-1}((1 : 0)) = \{(1 : 0)\}$. At a point $Q = (a : 1)$ with $a \neq 0$ one has uniformizer $t_Q = x/z - a$ and

$$\phi^*(t_Q) = x^2/z^2 - a = (x/z - \sqrt{a})(x/z + \sqrt{a}).$$

Writing $P = (\sqrt{a} : 1)$ one has $\phi(P) = Q$ and $e_\phi(P) = 1$. However, one can verify that $e_\phi((0 : 1)) = e_\phi((1 : 0)) = 2$.

Lemma 8.2.15. *Let $\phi : C_1 \to C_2$ and $\psi : C_2 \to C_3$ be non-constant morphisms of curves over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$. Then $e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(\phi(P))$.*

Exercise 8.2.16. Prove Lemma 8.2.15.

Exercise 8.2.17. Let $\phi : C_1 \to C_2$ be defined over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$ and let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Show that $e_\phi(\sigma(P)) = e_\phi(P)$.

8.3 Maps on Divisor Classes

We can now define some important maps on divisors that will be used in several proofs later. In particular, this will enable an elegant proof of Theorem 7.7.11 for general curves.

Definition 8.3.1. Let $\phi : C_1 \to C_2$ be a non-constant morphism over $\Bbbk$. Define the **pullback**

$$\phi^* : \mathrm{Div}_{\overline{\Bbbk}}(C_2) \to \mathrm{Div}_{\overline{\Bbbk}}(C_1)$$

as follows. For $Q \in C_2(\overline{\Bbbk})$ define $\phi^*(Q) = \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P)$ and extend ϕ^* to $\mathrm{Div}_{\overline{\Bbbk}}(C_2)$ by linearity, i.e.,

$$\phi^*\left(\sum_{Q\in C_2(\overline{\Bbbk})} n_Q(Q)\right) = \sum_{Q\in C_2(\overline{\Bbbk})} n_Q\phi^*(Q).$$

Note that, since $\mathrm{Div}_{\overline{\Bbbk}}(C_2)$ and $\mathrm{Div}_{\overline{\Bbbk}}(C_1)$ are not varieties, it does not make sense to ask whether ϕ^* is a rational map or morphism.

Example 8.3.2. Consider $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ given by $\phi(x) = x^2$. Let $D = (0) + (1)$ be a divisor on $\mathbb{A}^1$. Then $\phi^*(D) = 2(0) + (1) + (-1)$.

Let $\phi : C_1 \to C_2$ be a non-constant morphism over $\Bbbk$ and let $P \in C_2(\overline{\Bbbk})$. Then the divisor $\phi^*(P)$ is also called the **conorm** of P with respect to $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$ (see Definition III.1.8 of Stichtenoth [589]).

Lemma 8.3.3. *Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)^*$ be a non-constant rational function. Define the rational map $\phi : C \to \mathbb{P}^1$ by $\phi = (f : 1)$ (in future we will write f instead of ϕ). Then ϕ is a morphism and* $\mathrm{div}(f) = \phi^*((0 : 1) - (1 : 0))$.

Proof: That ϕ is a morphism follows from Lemma 7.3.6. Let $P \in C(\overline{\Bbbk})$ be such that $f(P) = 0$ (i.e., $\phi(P) = (0:1)$). We prove that $v_P(f) = e_\phi(P)$. Recall that $t = x/z$ is a uniformizer at $(0:1)$. By definition, $e_\phi(P) = v_P(t \circ \phi)$. Now $t \circ \phi = x(f:1)/z(f:1) = f/1 = f$. Hence, $e_\phi(P) = v_P(f)$. One handles poles of f analogously using the formula $e_\phi(P) = v_P(1/f)$. □

There is a natural map ϕ_* on divisors that is called the **pushforward** (it is called the **divisor-norm map** in Section VII.7 of Lorenzini [394]).

Definition 8.3.4. Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves. Define the **pushforward**

$$\phi_* : \mathrm{Div}_{\overline{\Bbbk}}(C_1) \to \mathrm{Div}_{\overline{\Bbbk}}(C_2)$$

by $\phi_*(P) = \phi(P)$ and extend to the whole of $\mathrm{Div}_{\overline{\Bbbk}}(C_1)$ by linearity.

It remains to find a map from $\Bbbk(C_1)$ to $\Bbbk(C_2)$ that corresponds (in the sense of property 4 of Theorem 8.3.8) to the pushforward. This is achieved using the norm map with respect to the extension $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$. As we will show in Lemma 8.3.13 this norm satisfies, for $f \in \Bbbk(C_1)$ and $Q \in C_2(\overline{\Bbbk})$, $\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f)(Q) = \prod_{\phi(P)=Q} f(P)^{e_\phi(P)}$.

Definition 8.3.5. Let C_1, C_2 be curves over $\Bbbk$ and let $\phi : C_1 \to C_2$ be a non-constant rational map. Let $N_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}$ be the usual norm map in field theory (see Section A.6). Define

$$\phi_* : \Bbbk(C_1) \to \Bbbk(C_2)$$

by $\phi_*(f) = (\phi^*)^{-1}(\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f))$.

Note that the definition of $\phi_*(f)$ makes sense since $\mathrm{N}_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}(f) \in \phi^*(\Bbbk(C_2))$ and so is of the form $h \circ \phi$ for some $h \in \Bbbk(C_2)$. So $\phi_*(f) = h$.

Example 8.3.6. Let $C_1 = C_2 = \mathbb{A}^1$ and $\phi : C_1 \to C_2$ be given by $\phi(x) = x^2$. Then $\phi^*(\Bbbk(C_2)) = \Bbbk(x^2)$ and $\Bbbk(C_1) = \phi^*(\Bbbk(C_2))(x)$. Let $f(x) = x^2/(x-1)$. Then

$$\mathrm{N}_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}(f) = f(x)f(-x) = \frac{x^2}{(x-1)}\frac{(-x)^2}{(-x-1)} = \frac{x^4}{-x^2+1},$$

which is $h \circ \phi$ for $h(X) = X^2/(1-X)$. Hence $\phi_*(f(x)) = -f(x)$.

Exercise 8.3.7. Let $C_1 = V(y^2 = x^2 + 1) \subseteq \mathbb{A}^2$, $C_2 = \mathbb{A}^1$ and let $\phi : C_1 \to C_2$ be given by $\phi(x, y) = x$. Let $f(x, y) = x/y$. Show that

$$\mathrm{N}_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}(f) = \frac{-x^2}{x^2+1}$$

and so $\phi_*(f) = h(X)$ where $h(X) = -X^2/(X^2+1)$.

We now state the main properties of the pullback and pushforward.

Theorem 8.3.8. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then*

1. $\deg(\phi^*(D)) = \deg(\phi)\deg(D)$ *for all* $D \in \mathrm{Div}(C_2)$.
2. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$ *for all* $f \in \Bbbk(C_2)^*$.
3. $\deg(\phi_*(D)) = \deg(D)$ *for all* $D \in \mathrm{Div}(C_1)$.
4. $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$ *for all* $f \in \Bbbk(C_1)^*$.
5. $\phi_*(\phi^*(D)) = \deg(\phi)D$ *for* $D \in \mathrm{Div}(C_2)$.

6. *If $\psi : C_2 \to C_3$ is another non-constant rational map of curves over $\Bbbk$ then $(\psi\circ\phi)^* = \phi^* \circ \psi^*$ and $(\psi \circ \phi)_* = \psi_* \circ \phi_*$.*

Proof: (Sketch)

1. Follows from Theorem 8.2.12.
2. Follows from Lemma 8.2.9.
3. Follows directly from the definition.
4. First note that

$$\phi_*(\mathrm{div}(f)) = \sum_{P \in C_1(\overline{\Bbbk})} v_P(f)(\phi(P)) = \sum_{Q \in C_2(\overline{\Bbbk})} \left(\sum_{P \in C_1(\overline{\Bbbk}) : \phi(P) = Q} v_P(f) \right) (Q).$$

   To complete the proof it suffices to show that $\sum_{P \in C_1(\overline{\Bbbk}):\phi(P)=Q} v_P(f) = v_Q(\phi_*(f))$. This requires some theory that has not been presented in the book, so we sketch the details here.

   Write $L = \overline{\Bbbk}(C_1)$, $K = \phi^*(\overline{\Bbbk}(C_2)) \subseteq L$. Fix $Q \in C_2(\overline{\Bbbk})$ and write v for the valuation on K corresponding to v_Q on $\overline{\Bbbk}(C_2)$. Write $A = \phi^*(\mathcal{O}_{Q,\overline{\Bbbk}}(C_2)) \subseteq K$, which is a Dedekind domain, and let B be the integral closure of A in L. Write $\mathfrak{m}$ for the maximal ideal of A corresponding to $\mathfrak{m}_{Q,\overline{\Bbbk}}(C_2)$. If $P \in C_1(\overline{\Bbbk})$ is such that $\phi(P) = Q$ then $\mathfrak{m} = \mathfrak{m}_{P,\overline{\Bbbk}}(C_1) \cap A$. Suppose first that L/K is Galois. Then for any B-ideal I one can define the norm $\mathrm{N}_{L/K}(I) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(I)$. Lemma IV.6.4 of Lorenzini [394] implies that $\mathrm{N}_{L/K}(\mathfrak{m}_{P,\overline{\Bbbk}}(C_1)) = \mathfrak{m}$. When L/K is not Galois then one can define $\mathrm{N}_{L/K}$ by $\mathrm{N}_{L/K}(\mathfrak{m}_{P,\overline{\Bbbk}}(C_1)) = \mathfrak{m}$. Proposition IV.6.9 of [394] shows (also see Proposition I.22 of [365] in the case when L/K is separable) that $\mathrm{N}_{L/K}((f)) = (\mathrm{N}_{L/K}(f))$, where (f) denotes the principal B-ideal generated by f and where $\mathrm{N}_{L/K}(f)$ denotes the usual field-theoretic norm. Since

$$\mathrm{N}_{L/K}((f)) = \prod_{\mathfrak{m}_P \supseteq \mathfrak{m}} \mathfrak{m}_P^{v_P(f)} \qquad \text{and} \qquad (\mathrm{N}_{L/K}(f)) = \mathfrak{m}^{v\left(\mathrm{N}_{L/K}(f)\right)}$$

   (where the latter are A-ideals) the result follows.
5. Follows easily from Theorem 8.2.12.
6. The first statement follows from Lemma 8.2.15 and the second is straightforward from the definition.

□

Exercise 8.3.9. Give all the details in the proof of Theorem 8.3.8.

Corollary 8.3.10. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then the induced maps $\phi^* : \mathrm{Pic}^0_{\Bbbk}(C_2) \to \mathrm{Pic}^0_{\Bbbk}(C_1)$ and $\phi_* : \mathrm{Pic}^0_{\Bbbk}(C_1) \to \mathrm{Pic}^0_{\Bbbk}(C_2)$ on divisor class groups are well-defined group homomorphisms.*

Proof: The maps ϕ^* and ϕ_* are well-defined on divisor classes by parts 2 and 4 of Theorem 8.3.8. The homomorphic property follows from the linearity of the definitions. □

Exercise 8.3.11. Show that if $\phi : C_1 \to C_2$ is an isomorphism of curves over $\Bbbk$ then $\mathrm{Pic}^0_{\Bbbk}(C_1) \cong \mathrm{Pic}^0_k(C_2)$ (isomorphic as groups). Give an example to show that the converse is not true.

A further corollary of this result is that a rational map $\phi : E_1 \to E_2$ between elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is automatically a group homomorphism (see Theorem 9.2.1).

Exercise 8.3.12. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be defined by $\phi((x : z)) = (x^2/z^2 : 1)$. Let $D = (-1 : 1) + (1 : 0) - (0 : 1)$. Compute $\phi_*(D)$, $\phi^*(D)$, $\phi_*\phi^*(D)$ and $\phi^*\phi_*(D)$.

We now make an observation that was mentioned when we defined ϕ_* on $\Bbbk(C_1)$.

Lemma 8.3.13. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Let $f \in \Bbbk(C_1)^*$ and $Q \in C_2(\overline{\Bbbk})$. Suppose that $v_P(f) = 0$ for all points $P \in C_1(\overline{\Bbbk})$ such that $\phi(P) = Q$. Then*

$$\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f)(Q) = \prod_{P \in C_1(\overline{\Bbbk}) : \phi(P) = Q} f(P)^{e_\phi(P)}.$$

(Later in the book we will introduce the notation $f(\phi^*(Q))$ for the right hand side.) Another formulation would be "f of conorm of Q equals norm of f at Q".

Proof: (Sketch) This uses similar ideas to the proof of part 4 of Theorem 8.3.8. We work over $\overline{\Bbbk}$.

As always, $\overline{\Bbbk}(C_1)$ is a finite extension of $\phi^*(\overline{\Bbbk}(C_2))$. Let $A = \phi^*(\mathcal{O}_Q(C_2))$ and let B be the integral closure of A in $\Bbbk(C_1)$. Then B is a Dedekind domain and the ideal $\phi^*(\mathfrak{m}_Q)$ splits as a product $\prod_i \mathfrak{m}_{P_i}^{e_\phi(P_i)}$ where $P_i \in C_1(\overline{\Bbbk})$ are distinct points such that $\phi(P_i) = Q$.

By assumption, f has no poles at P_i and so $f \in B$. Note that $f(P_i) = c_i \in \overline{\Bbbk}$ if and only if $f \equiv c_i \pmod{\mathfrak{m}_{P_i}}$. Hence, the right hand side is

$$\prod_i f(P_i)^{e_\phi(P_i)} = \prod_i c_i^{e_\phi(P_i)} = \prod_i (f \pmod{\mathfrak{m}_{P_i}})^{e_\phi(P_i)}.$$

It remains to prove that this is equal to the norm of f evaluated at Q and we sketch this when the extension is Galois and cyclic (the general case is simple linear algebra). The elements $\sigma \in \mathrm{Gal}(\overline{\Bbbk}(C_1)/\phi^*(\overline{\Bbbk}(C_2)))$ permute the $\mathfrak{m}_{P_i}$ and the ramification indices $e_\phi(P_i)$ are all equal. Since $c_i \in \overline{\Bbbk} \subset \phi^*(\Bbbk(C_2))$ we have $f \equiv c_i \pmod{\mathfrak{m}_{P_i}}$ if and only if $\sigma(f) \equiv c_i \pmod{\sigma(\mathfrak{m}_{P_i})}$. Hence

$$\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f) = \prod_{\sigma \in \mathrm{Gal}(\overline{\Bbbk}(C_1)/\phi^*(\overline{\Bbbk}(C_2)))} \sigma(f) \equiv \prod_i c_i^{e_\phi(P_i)} \pmod{\mathfrak{m}_{P_1}}$$

and since $\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f) \in \phi^*(\Bbbk(C_2))$ this congruence holds modulo $\phi^*(\mathfrak{m}_Q)$. The result follows. □

We now give an important application of Theorem 8.3.8, already stated as Theorem 7.7.11.

Theorem 8.3.14. *Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)^*$. Then f has only finitely many zeroes and poles (i.e., $\mathrm{div}(f)$ is a divisor) and $\deg(\mathrm{div}(f)) = 0$.*

Proof: Let $D = (0 : 1) - (1 : 0)$ on $\mathbb{P}^1$. Interpreting f as a rational map $f : C \to \mathbb{P}^1$ as in Lemma 8.1.1 we have $\mathrm{div}(f) = f^*(D)$ and, by part 1 of Theorem 8.3.8, $\deg(f^*(D)) = \deg(f)\deg(D) = 0$. One also deduces that f has, counting with multiplicity, $\deg(f)$ poles and zeroes. □

Exercise 8.3.15. Let $\phi : C_1 \to C_2$ be a rational map over $\Bbbk$. Show that if $D \in \mathrm{Div}_{\Bbbk}(C_1)$ (respectively, $D \in \mathrm{Div}_{\Bbbk}(C_2)$) then $\phi_*(D)$ (resp., $\phi^*(D)$) is defined over $\Bbbk$.

8.4 Riemann-Roch Spaces

Definition 8.4.1. Let C be a curve over $\Bbbk$ and let $D = \sum_P n_P(P)$ be a divisor on C. The **Riemann-Roch space** of D is

$$\mathcal{L}_{\Bbbk}(D) = \{f \in \Bbbk(C)^* : v_P(f) \geq -n_P \text{ for all } P \in C(\overline{\Bbbk})\} \cup \{0\}.$$

We denote $\mathcal{L}_{\overline{\Bbbk}}(D)$ by $\mathcal{L}(D)$.

Lemma 8.4.2. *Let C be a curve over $\Bbbk$ and let D be a divisor on C. Then*

1. *$\mathcal{L}_{\Bbbk}(D)$ is a $\Bbbk$-vector space.*
2. *$D \leq D'$ implies $\mathcal{L}_{\Bbbk}(D) \subseteq \mathcal{L}_{\Bbbk}(D')$.*
3. *$\mathcal{L}_{\Bbbk}(0) = \Bbbk$, $\mathcal{L}_{\Bbbk}(D) = \{0\}$ if $\deg(D) < 0$.*
4. *Let $P_0 \in C(\overline{\Bbbk})$. Then $\dim_{\Bbbk}(\mathcal{L}_{\Bbbk}(D+P_0)/\mathcal{L}_{\Bbbk}(D)) \leq 1$ and if $D' \geq D$ then $\dim_{\Bbbk}(\mathcal{L}_{\Bbbk}(D')/\mathcal{L}_{\Bbbk}(D)) \leq \deg(D') - \deg(D)$.*
5. *$\mathcal{L}_{\Bbbk}(D)$ is finite dimensional and if $D = D_+ - D_-$, where D_+, D_- are effective, then $\dim_{\Bbbk} \mathcal{L}_{\Bbbk}(D) \leq \deg(D_+) + 1$.*
6. *If $D' = D + \operatorname{div}(f)$ for some $f \in \Bbbk(C)^*$ then $\mathcal{L}_{\Bbbk}(D)$ and $\mathcal{L}_{\Bbbk}(D')$ are isomorphic as $\Bbbk$-vector spaces.*

Proof: (Sketch)

1. Straightforward from the definition and part 3 of Lemma 7.4.14.
2. Write $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ and $D' = \sum_P n'_P(P)$. Then $D \leq D'$ implies $n_P \leq n'_P$. If $f \in \mathcal{L}_{\Bbbk}(D)$ then $v_P(f) \geq -n_P \geq n'_P$ and so $f \in \mathcal{L}_{\Bbbk}(D')$.
3. Clearly $\Bbbk \subseteq \mathcal{L}_{\Bbbk}(0)$. The converse follows from Corollary 7.7.13. The second statement follows since $\deg(\operatorname{div}(f)) = 0$.
4. Write $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$. Note that $\mathcal{L}_{\Bbbk}(D)$ is a $\Bbbk$-vector subspace of $\mathcal{L}_{\Bbbk}(D + P_0)$. Let $t \in \Bbbk(C)^*$ be a function such that $v_{P_0}(f) = n_{P_0} + 1$ (e.g., take t to be a power of a uniformizer at P_0). If $f \in \mathcal{L}_{\Bbbk}(D + P_0)$ then $ft \in \mathcal{O}_{P,\Bbbk}(C)$. We therefore have a $\Bbbk$-linear map $\psi : \mathcal{L}_{\Bbbk}(D + P_0) \to \Bbbk$ given by $\psi(f) = (ft)(P_0)$. The kernel of ψ is $\mathcal{L}_{\Bbbk}(D)$ and the first part of the statement follows. The second statement follows by induction.
5. First, note that $\mathcal{L}_{\Bbbk}(D) \subseteq \mathcal{L}_{\Bbbk}(D_+)$. We then compute $\dim_{\Bbbk} \mathcal{L}_{\Bbbk}(D_+) = 1 + \dim_{\Bbbk}(\mathcal{L}_{\Bbbk}(D_+)/\mathcal{L}_{\Bbbk}(0))$. By the previous part this is $\leq 1 + \deg(D_+) - \deg(0) = 1 + \deg(D_+)$.
6. The linear map $\mathcal{L}_{\Bbbk}(D) \to \mathcal{L}_{\Bbbk}(D')$ is given by $h \mapsto h/f$.

□

Exercise 8.4.3. Fill in the gaps in the proof of Lemma 8.4.2.

Exercise 8.4.4. Let $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ be a divisor on C. Explain why $\{f \in \Bbbk(C)^* : v_P(f) = n_P \text{ for all } P \in C(\overline{\Bbbk})\} \cup \{0\}$ is not usually a $\Bbbk$-vector space.

Definition 8.4.5. Let C be a curve over $\Bbbk$ and let D be a divisor on C. Define

$$\ell_{\Bbbk}(D) = \dim_{\Bbbk} \mathcal{L}_{\Bbbk}(D).$$

Write $\ell(D) = \ell_{\overline{\Bbbk}}(D)$.

Exercise 8.4.6. Show that $\ell_{\Bbbk}(0) = 1$ and, for $f \in \Bbbk(C)$, $\ell_{\Bbbk}(\mathrm{div}(f)) = 1$.

Theorem 8.4.7. *(Riemann's theorem) Let C be a curve over $\Bbbk$ (in particular, non-singular and projective) . Then there exists a unique minimal integer g such that, for all divisors D on C over $\overline{\Bbbk}$*

$$\ell_{\overline{\Bbbk}}(D) \geq \deg(D) + 1 - g.$$

Proof: See Proposition I.4.14 of Stichtenoth [589], Section 8.3 (page 196) of Fulton [216] or Theorem 2.3 of Moreno [439]. □

Definition 8.4.8. The number g in Theorem 8.4.7 is called the **genus** of C.

Note that the genus is independent of the model of the curve C and so one can associate the genus with the function field or birational equivalence class of the curve.

Exercise 8.4.9. Show that on $\mathbb{P}^1$ over $\Bbbk$ one has $\ell_{\overline{\Bbbk}}(D) = \deg(D) + 1$ for all divisors D and so the genus of $\mathbb{P}^1$ is zero. Note that if D is defined over $\Bbbk$ then $\ell_{\Bbbk}(D) = \deg(D) + 1$ too. (More results about genus zero are given in Section 8.6.)

Exercise 8.4.10. Let $\Bbbk$ be a field and let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$. Determine the spaces $\mathcal{L}_{\Bbbk}(n\mathcal{O}_E)$ and their dimensions $\ell_{\Bbbk}(n\mathcal{O}_E)$ for $n = 0, 1, 2, 3, 4, 5, 6$.

Remark 8.4.11. We give an alternative justification for Remark 5.4.14. Suppose $f \in \overline{\Bbbk}(C)$ is such that $\sigma(f) = f$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Write $D = \mathrm{div}(f)$. Note that D is defined over $\Bbbk$. Then $f \in \mathcal{L}_{\overline{\Bbbk}}(D)$, which has dimension 1 by Exercise 8.4.6. Now, performing the Brill-Noether proof of Riemann's theorem (e.g., see Section 8.5 of Fulton [216]) one can show that $\mathcal{L}_{\Bbbk}(D)$ contains a function $h \in \Bbbk(C)$. It follows that $\mathrm{div}(h) = D$ and that $f = ch$ for some $c \in \Bbbk$. Hence Theorem 7.8.3 is proved.

8.5 Derivations and Differentials

Differentials arise in differential geometry: a manifold is described by open patches homeomorphic to $\mathbb{R}^n$ (or $\mathbb{C}^n$ for complex manifolds) with coordinate functions $x_1, \ldots, x_n$ and the differentials dx_i arise naturally. It turns out that differentials can be described in a purely formal way (i.e., without reference to limits).

When working over general fields (such as finite fields) it no longer makes sense to consider differentiation as a process defined by limits. But the formal description of differentials makes sense and the concept turns out to be useful.

We first explain how to generalise partial differentiation to functions on curves. We can then define differentials. Throughout this section, if $F(x, y)$ is a polynomial or rational function then $\partial F/\partial x$ denotes standard undergraduate partial differentiation.

Definition 8.5.1. Let C be a curve over $\Bbbk$. A **derivation** on $\Bbbk(C)$ is a $\Bbbk$-linear map (treating $\Bbbk(C)$ as a $\Bbbk$-vector space) $\delta : \Bbbk(C) \to \Bbbk(C)$ such that $\delta(f_1f_2) = f_1\delta(f_2) + f_2\delta(f_1)$.

Lemma 8.5.2. *Let $\delta : \Bbbk(C) \to \Bbbk(C)$ be a derivation. Then*

1. *If $c \in \Bbbk$ then $\delta(c) = 0$.*
2. *If $x \in \Bbbk(C)$ and $n \in \mathbb{Z}$ then $\delta(x^n) = nx^{n-1}\delta(x)$.*
3. *If $\mathrm{char}(\Bbbk) = p$ and $x \in \Bbbk(C)$ then $\delta(x^p) = 0$.*
4. *If $h \in \Bbbk(C)$ then $\delta'(f) = h\delta(f)$ is a derivation.*

5. *If* $x, y \in \Bbbk(C)$ *then* $\delta(x/y) = (y\delta(x) - x\delta(y))/y^2$.
6. *If* $x, y \in \Bbbk(C)$ *and* $F(u, v) \in \Bbbk[u, v]$ *is a polynomial then* $\delta(F(x, y)) = (\partial F/\partial x)\delta(x) + (\partial F/\partial y)\delta(y)$.

Exercise 8.5.3. Prove Lemma 8.5.2.

Definition 8.5.4. Let C be a curve over $\Bbbk$. A function $x \in \Bbbk(C)$ is a **separating element** (or **separating variable**) if $\Bbbk(C)$ is a finite separable extension of $\Bbbk(x)$.

Note that if $x \in \Bbbk(C)$ is such that $x \notin \overline{\Bbbk}$ then $\Bbbk(C)/\Bbbk(x)$ is finite; hence the non-trivial condition is that $\Bbbk(C)/\Bbbk(x)$ is separable.

Example 8.5.5. For $\mathbb{P}^1(\mathbb{F}_p)$, x is a separating element (since $\Bbbk(\mathbb{P}^1) = \Bbbk(x)$) and x^p is not a separating element (since $\Bbbk(\mathbb{P}^1)/\Bbbk(x^p) = \Bbbk(x)/\Bbbk(x^p)$ is not separable). The mapping $\delta(f) = \partial f/\partial x$ is a derivation.

The following exercise shows that separating elements exist for elliptic and hyperelliptic curves. For general curves we need Lemma 8.5.7.

Exercise 8.5.6. Let $\Bbbk$ be any field and let C be a curve given by an equation of the form $y^2 + H(x)y = F(x)$ with $H(x), F(x) \in \Bbbk[x]$. Show that if either $H(x) \neq 0$ or if $\mathrm{char}(\Bbbk) \neq 2$ then x is a separating element of $\Bbbk(C)$.

Lemma 8.5.7. *Let* C *be a curve over* $\Bbbk$*, where* $\Bbbk$ *is a perfect field. Then there exists a separating element* $x \in \Bbbk(C)$.

Proof: Let $L = \Bbbk(x_1, \ldots, x_n)$ be any field extension of transcedence degree 1 of a perfect field $\Bbbk$. We show that L is a separable extension of $\Bbbk(x)$ for some x. First, note that either $\{x_1, \ldots, x_n\}$ is algebraically dependent (and so there is a polynomial $F(x_1, \ldots, x_n) = 0$ of minimal degree, hence irreducible), or else $L = \Bbbk(x_1)$ and we're done. In the former case, write $F = \sum_i f_i m_i$ where $f_i \in \Bbbk$ and m_i are monomials in $x_1, \ldots, x_n$.

We claim that F is separable in at least one variable (i.e., $\partial F/\partial x_i \neq 0$). To show this, suppose F is not separable in any variable. Then all monomials are p-powers, $m_i = n_i^p$. Since $\Bbbk$ is perfect $f_i^{1/p} \in \Bbbk$. Hence $F = (\sum_i f_i^{1/p} n_i)^p$ is not irreducible.

Re-order the variables so that F is separable in x_n. Then $\Bbbk(x_1, \ldots, x_n)/\Bbbk(x_1, \ldots, x_{n-1})$ is a separable extension. Applying the argument inductively to $\Bbbk(x_1, \ldots, x_{n-1})$ proves the result. □

Lemma 8.5.8. *Let* C *be a curve over* $\Bbbk$*, let* $P \in C(\Bbbk)$ *and let* t_P *be a uniformizer at* P*. Then* t_p *is a separating element of* $\Bbbk(C)$.

Proof: Let $p = \mathrm{char}(\Bbbk)$. Then $v_P(t_P) = 1 \not\equiv 0 \pmod{p}$ and so, by Proposition III.9.2(a) of Stichtenoth [589], t_P is a separating element. □

Suppose now that C is a curve over $\Bbbk$ and x is a separating element. We wish to extend $\delta(f) = \partial f/\partial x$ from $\Bbbk(x)$ to the whole of $\Bbbk(C)$. The natural approach is to use property 6 of Lemma 8.5.2: If $f \in \Bbbk(C)$ then $\Bbbk(x, f)/\Bbbk(x)$ is finite and separable; write $F(T)$ for the minimal polynomial of f over $\Bbbk(x)$ in $\Bbbk(C)$; since the extension is separable we have $\partial F/\partial T \neq 0$; as a function on C we have $F(x, f) = 0$ and so

$$0 = \delta(F(x, f)) = \frac{\partial F}{\partial x}\delta(x) + \frac{\partial F}{\partial T}\delta(f). \tag{8.1}$$

This motivates the following definition.

Definition 8.5.9. Let C be a curve over $\Bbbk$ and let $x \in \Bbbk(C)$ be a separating element. Let $y \in \Bbbk(C)$. Let $F(x,T)$ be a rational function such that $F(x,y) = 0$. Define

$$\frac{\partial y}{\partial x} = -(\partial F/\partial x)/(\partial F/\partial T)$$

evaluated at y.

Lemma 8.5.10. *The value $\partial y/\partial x$ in Definition 8.5.9 is well-defined. More precisely, if F and F' are rational functions such that $F(x,y) = F'(x,y) = 0$ then $(\partial F/\partial x)/(\partial F/\partial y) = (\partial F'/\partial x)/(\partial F'/\partial y)$ and if $z \equiv y$ in $\Bbbk(C)$ then $\partial z/\partial x \equiv \partial y/\partial x$.*

Proof: The first claim follows from equation (8.1). For the second claim, if $z = y$ in $\Bbbk(C)$ then they satisfy the same minimal polynomial. □

It remains to show that this construction does give a derivation.

Lemma 8.5.11. *Let C be a curve over $\Bbbk$ and $x \in \Bbbk(C)$ a separating element. The function $\delta : \Bbbk(C) \to \Bbbk(C)$ defined by $\delta(y) = \partial y/\partial x$ as in Definition 8.5.9 is $\Bbbk$-linear and satisfies the product rule.*

Furthermore, if $f = H(y) \in \Bbbk(C)$ is another function, where $H(T) \in \Bbbk(x)[T]$ is a polynomial, then

$$\delta(f) = \frac{\partial H}{\partial x} - (\partial F/\partial x)/(\partial F/\partial T)\frac{\partial H}{\partial T} \tag{8.2}$$

evaluated at y, where F is as in Definition 8.5.9.

Proof: (Sketch; see Proposition IV.1.4 of Stichtenoth for details.)

Consider the two maps $D_1, D_2 : \Bbbk(x)[T] \to \Bbbk(x)[T]$ defined by

$$D_1\left(\sum_i u_i T^i\right) = \sum_i \frac{\partial u_i}{\partial x} T^i \ , \qquad D_2\left(\sum_i u_i T^i\right) = \sum_i i u_i T^{i-1}.$$

(So D_1 corresponds to $\partial/\partial x$ while D_2 will correspond to $\partial/\partial y$.) One can verify that D_1 and D_2 are $\Bbbk$-linear maps. Furthermore, one can verify that if $u, v \in \Bbbk(x)[T]$ then $D_1(uv) = uD_1(v) + vD_1(u)$ and $D_2(uv) = uD_2(v) + vD_2(u)$.

We re-write equation (8.2) as

$$\delta(f) = D_1(H) - D_1(F)/D_2(F)D_2(H) \tag{8.3}$$

evaluated at y. One can show that δ is well-defined, in the sense that if $H(T) = Q(T)F(T) + R(T)$ for $Q, R \in \Bbbk(x)[T]$ then $f = H(y) = R(y)$ and the value of $\delta(f)$ is the same regardless of whether H or R is used to compute it.

Let y be such that $\Bbbk(C) = \Bbbk(x)(y)$ and write $F(T) \in \Bbbk(x)[T]$ for the minimal polynomial of y. For any $f \in \Bbbk(C)$ we have $f = H(y)$ for some polynomial $H(T) \in \Bbbk(x)[T]$ and so define $\delta(f)$ using equation (8.3). We show that δ is a derivation. The $\Bbbk$-linearity of δ is clear. To show that δ satisfies the product rule let $g, h \in \Bbbk(C)$ and write $g = G(y)$ and $h = H(y)$ for $G[T], H[T] \in \Bbbk(x)[T]$. Then note that

$$\begin{aligned}
\delta(gh) &= D_1(GH) - \frac{D_1(F)}{D_2(F)} D_2(GH) \\
&= GD_1(H) + HD_1(G) - \frac{D_1(F)}{D_2(F)}(GD_2(H) + HD_2(G)) \\
&= G\left(D_1(H) - \frac{D_1(F)}{D_2(F)} D_2(H)\right) + H\left(D_1(G) - \frac{D_1(F)}{D_2(F)} D_2(G)\right) \\
&= g\delta(h) + h\delta(g).
\end{aligned}$$

The equivalence of the two definitions (i.e., equations (8.2) and (8.3)) follows from the uniqueness of derivations extending $\Bbbk(x)$ (Lemma IV.1.3 of Stichtenoth [589]). □

Example 8.5.12. Let $C : y^2 = x^3 + x + 1$ over $\mathbb{Q}$. Note that x is a separating element. To compute $\partial y/\partial x$ one uses the fact that $F(x, y) = y^2 - (x^3 + x + 1) = 0$ in $\Bbbk(C)$ and so $\partial y/\partial x = (3x^2 + 1)/(2y)$.

Consider the function $f(x, y) = xy$ and let $\delta(f) = \partial f/\partial x$. Then $\delta(f) = x\delta(y) + y = x(3x^2 + 1)/(2y) + y = (3x^3 + x + 2y^2)/(2y) = (5x^3 + 3x + 2)/(2y)$.

Exercise 8.5.13. Let $\Bbbk(C)$ be as in Example 8.5.12. Show that $\delta(y/x) = (x^3 - x - 2)/(2yx^2)$.

Lemma 8.5.14. *Let C be a curve over $\Bbbk$ and let $x, y \in \Bbbk(C)$ be separating elements. Then the corresponding derivations on $\Bbbk(C)$ satisfy the chain rule, namely*

$$\frac{\partial f}{\partial y} = \frac{\partial f}{\partial x}\frac{\partial x}{\partial y}.$$

In particular, if $x, y \in \Bbbk(C)$ are separating elements then $\partial x/\partial y = 1/(\partial y/\partial x) \neq 0$.

Let $t \in \Bbbk(C)$. Then $\partial t/\partial x = 0$ if and only if t is not a separating element.

Proof: See Lemma IV.1.6 of Stichtenoth [589]. □

Exercise 8.5.15. Let $C = \mathbb{P}^1$ over $\mathbb{F}_p$ with variable x and let $\delta(f) = \partial f/\partial x$. Show that $\delta(x^p) = 0$.

Now we have defined $\partial f/\partial x$ for general $f \in \Bbbk(C)$ we can introduce the differentials on a curve over a field. Our definition is purely formal and the symbol dx is not assumed to have any intrinsic meaning. We essentially follow Section IV.1 of Stichtenoth [589]; for a slightly different approach see Section 8.4 of Fulton [216].

Definition 8.5.16. Let C be a curve over $\Bbbk$. The set of **differentials** $\Omega_{\Bbbk}(C)$ (some authors write $\Omega^1_{\Bbbk}(C)$) is the quotient of the free $\Bbbk(C)$-module on symbols dx for $x \in \Bbbk(C)$ under the relations

1. $dx \neq 0$ if x is a separating element,
2. If x is a separating element and $h_1, h_2 \in \Bbbk(C)$ then $h_1 dx + h_2 dx = (h_1 + h_2)dx$.
3. If x is a separating element and $y \in \Bbbk(C)$ then $dy = (\partial y/\partial x)dx$,

In other words, differentials are equivalence classes of formal symbols

$$\left\{ \sum_{i=1}^{m} h_i dx_i : x_i, h_i \in \Bbbk(C) \right\}$$

where one may assume the x_i are all separating elements.

Lemma 8.5.17. *Let C be a curve over $\Bbbk$ and $x, y \in \Bbbk(C)$ separating elements.*

1. *$dx = 0$ if x is not a separating element.*
2. *$d(x + y) = dx + dy$.*
3. *$d(\lambda x) = \lambda dx$ and $d\lambda = 0$ for all $\lambda \in \Bbbk$.*
4. *$d(xy) = xdy + ydx$.*
5. *If x is a separating element and $y \in \Bbbk(C)$ then $dx + dy = (1 + (\partial y/\partial x))dx$.*

6. *For $n \in \mathbb{Z}$, $d(x^n) = nx^{n-1}dx$.*
7. *$d(x/y) = (ydx - xdy)/y^2$*
8. *If $f \in \Bbbk(C)$ then $d(f(x)) = (\partial f/\partial x)dx$.*
9. *For $i \in \mathbb{Z}$, $d(f(x)y^i) = (\partial f/\partial x)y^i dx + f(x)iy^{i-1}dy$.*
10. *If $F(x,y)$ is a rational function in x and y then $dF(x,y) = (\partial F/\partial x)dx + (\partial F/\partial y)dy$.*

Exercise 8.5.18. Prove Lemma 8.5.17.

Exercise 8.5.19. Let C be a curve over $\Bbbk$. Let $x_1, x_2 \in \Bbbk(C)$ be separating elements and $h_1, h_2 \in \Bbbk(C)$. Show that $h_1 dx_1$ is equivalent to $h_2 dx_2$ if and only if

$$h_2 = h_1 \frac{\partial x_1}{\partial x_2}.$$

Example 8.5.20. We determine $\Omega_{\Bbbk}(\mathbb{P}^1)$. Since $\Bbbk(\mathbb{P}^1) = \Bbbk(x)$ the differentials are $d(f(x)) = (\partial f/\partial x)dx$ for $f(x) \in \Bbbk(x)$. Hence, they are a 1-dimensional vector space over $\Bbbk(C)$.

The following theorem, that all differentials on a curve are multiples of dx where x is a separating element, is a direct consequence of the definition.

Theorem 8.5.21. *Let C be a curve over $\Bbbk$ and let x be a separating element. Let $\omega \in \Omega_{\Bbbk}(C)$. Then $\omega = hdx$ for some $h \in \Bbbk(C)$.*

Exercise 8.5.22. Prove Theorem 8.5.21.

This result shows that $\Omega_{\Bbbk}(C)$ is a $\Bbbk(C)$-vector space of dimension 1 (we know that $\Omega_{\Bbbk}(C) \neq \{0\}$ since $dx \neq 0$ if x is a separating element). Therefore, for any $\omega_1, \omega_2 \in \Omega_{\Bbbk}(C)$ with $\omega_2 \neq 0$ there is a unique function $f \in \Bbbk(C)$ such that $\omega_1 = f\omega_2$. We define ω_1/ω_2 to be f. (See Proposition II.4.3 of Silverman [564]).

We now define the divisor of a differential by using uniformizers. Recall from Lemma 8.5.8 that a uniformizer t_P is a separating element and so $dt_P \neq 0$.

Definition 8.5.23. Let C be a curve over $\Bbbk$. Let $\omega \in \Omega_{\Bbbk}(C)$, $\omega \neq 0$ and let $P \in C(\overline{\Bbbk})$ have uniformizer $t_P \in \overline{\Bbbk}(C)$. Then the **order** of ω at P is $v_P(\omega) := v_P(\omega/dt_P)$. The **divisor of a differential** is

$$\operatorname{div}(\omega) = \sum_{P \in C(\overline{\Bbbk})} v_P(\omega)(P).$$

Lemma 8.5.24. *Let C be a curve over $\Bbbk$ and let ω be a differential on C. Then $v_P(\omega) \neq 0$ for only finitely many $P \in C(\overline{\Bbbk})$ and so $\operatorname{div}(\omega)$ is a divisor.*

Proof: See Proposition II.4.3(e) of Silverman [564]. □

Exercise 8.5.25. Show that $v_P(hdx) = v_P(h) + v_P(dx)$ and $v_P(df) = v_P(\partial f/\partial t_P)$.

Lemma 8.5.26. *The functions $v_P(\omega)$ and $\operatorname{div}(\omega)$ in Definition 8.5.23 are well-defined (both with respect to the choice of representative for ω and choice of t_P).*

Exercise 8.5.27. Prove Lemma 8.5.26.

Lemma 8.5.28. *Let C be a curve over $\Bbbk$ and $\omega, \omega' \in \Omega_{\Bbbk}(C)$. Then*

1. $\deg(\operatorname{div}(\omega)) = \deg(\operatorname{div}(\omega'))$.

2. $\mathrm{div}(\omega)$ *is well-defined up to principal divisors (i.e.,* $\mathrm{div}(\omega) = \mathrm{div}(\omega') + \mathrm{div}(f)$ *for some* $f \in \Bbbk(C)^*$*).*

Exercise 8.5.29. Prove Lemma 8.5.28.

Definition 8.5.30. Any divisor $\mathrm{div}(\omega)$ is called a **canonical divisor**. The set $\{\mathrm{div}(\omega) : \omega \in \Omega_{\Bbbk}(C)\}$ is the **canonical divisor class**.

Example 8.5.31. We determine the canonical class of $C = \mathbb{P}^1$.

Let $\omega = dx$. Since x is a uniformizer at the point 0 we have $v_0(\omega) = v_0(dx/dx) = 0$. More generally, for $P \in \Bbbk$ we have $(x-P)$ a uniformizer and $v_P(\omega) = v_P(dx/d(x-P)) = v_P(1) = 0$. Finally, a uniformizer at ∞ is $t = 1/x$ and $dt = (-x^{-2})dx$ so $v_\infty(\omega) = v_\infty(-x^2) = -2$. Hence $\mathrm{div}(\omega) = -2\infty$ and the degree of $\mathrm{div}(\omega)$ is -2.

Example 8.5.32. We determine the divisor of a differential on an elliptic curve E in Weierstrass form. Rather than computing $\mathrm{div}(dx)$ it is easier to compute $\mathrm{div}(\omega)$ for

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

Let $P \in E(\overline{\Bbbk})$. There are three cases, if $P = \mathcal{O}_E$ then one can take uniformizer $t = x/y$, if $P = (x_P, y_P) = \iota(P)$ then take uniformizer $(y - y_P)$ (and note that $v_P(2y + a_1x + a_3) = 1$ in this case) and otherwise take uniformizer $(x - x_P)$ and note that $v_P(2y + a_1x + a_3) = 0$.

We deal with the general case first. Since $dx/d(x - x_P) = \partial x/\partial(x - x_P) = 1$ it follows that $v_P(\omega) = 0$. For the case, $P = \mathcal{O}_E$ write $x = t^{-2}f$ and $y = t^{-3}h$ for some functions $f, h \in \Bbbk(E)$ regular at $\mathcal{O}_E$ and with $f(\mathcal{O}_E), h(\mathcal{O}_E) \neq 0$. One can verify that

$$\frac{\omega}{dt} = \frac{-2t^{-3}f + t^{-2}f'}{2t^{-3}h + a_1t^{-2}f + a_3} = \frac{-2f + tf'}{2h + a_1tf + a_3t^3}$$

and so $v_{\mathcal{O}_E}(\omega) = 0$. Finally, when $P = \iota(P)$ we must consider

$$\frac{dx}{d(y - y_P)} = \frac{1}{\partial y/\partial x} = \frac{2y + a_1x + a_3}{3x^2 + 2a_2x + a_4}.$$

It follows that $\omega = (1/(3x^2 + 2a_2x + a_4))d(y - y_P)$ and, since P is not a singular point, $3x_P^2 + 2a_2x_P + a_4 \neq 0$ and so $v_P(\omega) = 0$.

In other words, we have shown that $\mathrm{div}(\omega) = 0$. One can verify that

$$\mathrm{div}(dx) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O}_E)$$

where P_1, P_2, P_3 are the three affine points of order 2 in $E(\overline{\Bbbk})$.

Exercise 8.5.33. Show that

$$\frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

on an elliptic curve.

Definition 8.5.34. Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Define the function $\phi^* : \Omega_{\Bbbk}(C_2) \to \Omega_{\Bbbk}(C_1)$ by

$$\phi^*(f dx) = \phi^*(f) d(\phi^*(x)).$$

Lemma 8.5.35. *The function* ϕ^* *of Definition 8.5.34 is* $\Bbbk$*-linear and* ϕ^* *is injective (= non-zero) if and only if* ϕ *is separable.*

Proof: The linearity follows since dx is $\Bbbk$-linear. The second part follows since if x is separating for $\Bbbk(C_2)$ and ϕ is separable then $\Bbbk(C_1)/\phi^*\Bbbk(C_2)$ and $\phi^*\Bbbk(C_2)/\Bbbk(\phi^*(x))$ are separable. Hence, $\phi^*(x)$ is a separating element for $\Bbbk(C_1)$ and $d\phi^*(x) \neq 0$. The reverse implication is also straightforward. □

Lemma 8.5.36. *Let $\phi : C_1 \to C_2$ be an unramified morphism of curves over $\Bbbk$ and let $\omega \in \Omega_{\Bbbk}(C_2)$. Then $\phi^*(\mathrm{div}(\omega)) = \mathrm{div}(\phi^*(\omega))$.*

Proof: Let $P \in C_1(\overline{\Bbbk})$ and $Q = \phi(P)$. Let t_Q be a uniformizer at Q. Since ϕ is unramified it follows that $t_P = \phi^*(t_Q)$ is a uniformizer at P. Let $f \in \Bbbk(C_2)$. It suffices to show that $v_P(\phi^*(df)) = v_Q(df)$.

Recall from Exercise 8.5.25 that $v_Q(df) = v_Q(\partial f/\partial t_Q)$. If $F(x, y)$ is a rational function such that $F(t_Q, f) = 0$ then $0 = F(t_Q, f)\circ\phi = F(t_Q \circ \phi, f \circ \phi) = F(t_P, \phi^*(f)) = 0$. Hence, by definition,

$$\partial\phi^*(f)/\partial t_P = -(\partial F/\partial x)/(\partial F/\partial y) = \partial f/\partial t_Q$$

and so $v_P(d\phi^*(f)) = v_P(\partial\phi^*(f)/\partial t_P) = v_Q(f)$. □

Corollary 8.5.37. *Let $\phi : C_1 \to C_2$ be an isomorphism of curves over $\Bbbk$ and let $\omega \in \Omega_{\Bbbk}(C_2)$. Then $\deg(\mathrm{div}(\omega)) = \deg(\mathrm{div}(\phi^*(\omega)))$.*

8.6 Genus Zero Curves

Theorem 8.6.1. *Let C be a curve over $\Bbbk$ (i.e., projective non-singular). The following are equivalent.*

1. *C is birationally equivalent over $\Bbbk$ to $\mathbb{P}^1$.*
2. *The divisor class group of C over $\Bbbk$ is trivial and $\#C(\Bbbk) \geq 2$.*
3. *There is a point $P \in C(\Bbbk)$ with $\ell_{\Bbbk}(P) \geq 2$.*

Proof: (1 $\Rightarrow$ 2): Let C be birational to $\mathbb{P}^1$ over $\Bbbk$. By Lemma 7.3.6 there is a morphism from $\mathbb{P}^1$ to C and by Lemma 8.2.7 it is surjective. Since $\#\mathbb{P}^1(\Bbbk) \geq 2$ it follows that $\#C(\Bbbk) \geq 2$. Also, since the divisor class group of $\mathbb{P}^1$ is trivial it follows from Exercise 8.3.11 that $\mathrm{Pic}^0_{\Bbbk}(C) = \{0\}$.

(2 $\Rightarrow$ 3): Let $P, Q \in C(\Bbbk)$ be distinct. Since $(Q) - (P)$ is principal there exists a function h with $\mathrm{div}(h) = (Q) - (P)$ and so $\ell_{\Bbbk}(P)$ is spanned by at least $\{1, h\}$ (which is a linearly independent set).

(3 $\Rightarrow$ 1): Let $P_0 \in C(\Bbbk)$ be such that $\ell_{\Bbbk}(P_0) \geq 2$. Then there is some function $h \in \Bbbk(C)$ and a point $P \in C(\Bbbk)$ such that $\mathrm{div}(h) = (P) - (P_0)$. For any $R \in C(\Bbbk)$, $R \neq P_0$, the function $h - h(R)$ has a simple pole at P_0 and a simple zero at R. One can therefore deduce that h gives an injective rational map $h : C \to \mathbb{P}^1$. Unfortunately, it is not trivial to write down the inverse rational map $h' : \mathbb{P}^1 \to C$, so to complete the proof we show that $\Bbbk(C) \cong \Bbbk(\mathbb{P}^1)$.

Let f be any function on C. Then $g = fh^{v_{P_0}(f)}$ has no zero or pole at P_0. Write

$$g' = \prod_{R \in C(\Bbbk)} (h - h(R))^{v_R(g)}.$$

Then $v_R(g) = v_R(g')$ and so $\mathrm{div}(g') = \mathrm{div}(g)$ and $g' = cg$ for some $c \in \Bbbk^*$. In other words, f is a rational function of h, and so $f \in \Bbbk(h)$. Since f was arbitrary, $\Bbbk(C) = \Bbbk(h)$ and so, by Theorem 5.5.28, C is birational to $\mathbb{P}^1$. □

Definition 8.6.2. A curve satisfying any of the above equivalent conditions is called a **genus 0 curve**.

Exercise 8.6.3. Write down a curve C over a field $\Bbbk$ such that the divisor class group $\mathrm{Pic}^0_{\Bbbk}(C)$ is trivial but C is not birationally equivalent over $\Bbbk$ to $\mathbb{P}^1$.

Theorem 8.6.4. *An elliptic curve does not have genus 0.*

Proof: We have seen in Examples 8.5.31 and 8.5.32 that the canonical divisor classes on $\mathbb{P}^1$ and an elliptic curve have different degree. It follows that $\mathbb{P}^1$ is not isomorphic to an elliptic curve. And since a birational map of smooth projective curves is an isomorphism (Lemma 8.1.13 and Lemma 8.1.15) the result follows from Corollary 8.5.37.

There are a number of other proofs of this result: For example, Lemma 11.3 of Washington [626] gives an elementary one; it also follows from the general theorem that a non-singular plane curve of degree d has genus $d(d-1)/2$ or from the Hurwitz genus formula (see below). □

Corollary 8.6.5. *Let E be an elliptic curve and $P_1, P_2 \in E(\Bbbk)$. If $P_1 \neq P_2$ then $(P_1) - (P_2)$ is not a principal divisor.*

8.7 Riemann-Roch Theorem and Hurwitz Genus Formula

In this section we state, without proof, two very important results in algebraic geometry. Neither will play a crucial role in this book.

Lemma 8.7.1. *Let C be a curve over $\Bbbk$ of genus g and let $\omega \in \Omega_{\Bbbk}(C)$. Then*

1. $\deg(\mathrm{div}(\omega)) = 2g - 2$.
2. $\ell_{\Bbbk}(\mathrm{div}(\omega)) = g$.

Proof: See Corollary I.5.16 of Stichtenoth [589] or Corollary 11.16 of Washington [626]. For non-singular plane curves see Sections 8.5 and 8.6 of Fulton [216]. □

Theorem 8.7.2. *(Riemann-Roch) Let C be a non-singular projective curve over $\Bbbk$ of genus g, $\omega \in \Omega_{\Bbbk}(C)$ a differential and D a divisor. Then*

$$\ell_{\Bbbk}(D) = \deg(D) + 1 - g + \ell_{\Bbbk}(\mathrm{div}(\omega) - D).$$

Proof: There are several proofs. Section 8.6 of Fulton [216] gives the Brill-Noether proof for non-singular plane curves. Theorem I.5.15 of Stichtenoth [589] and Theorem 2.5 of Moreno [439] give proofs using repartitions. □

Some standard applications of the Riemann-Roch theorem are to prove that every genus 1 curve with a rational point is birational to an elliptic curve in Weierstrass form, and to prove that every hyperelliptic curve of genus g is birational to an affine curve of the form $y^2 + H(x)y = F(x)$ with $\deg(H(x)) \leq g + 1$ and $\deg(F(x)) \leq 2g + 2$.

Theorem 8.7.3. *(Hurwitz genus formula) Let $\phi : C_1 \to C_2$ be a rational map of curves over $\Bbbk$. Let g_i be the genus of C_i. Suppose that $\Bbbk$ is a field of characteristic zero or characteristic coprime to all $e_\phi(P)$. Then*

$$2g_1 - 2 = \deg(\phi)(2g_2 - 2) + \sum_{P \in C_1(\overline{\Bbbk})} (e_\phi(P) - 1).$$

Proof: See Theorem III.4.12 and Corollary III.5.6 of Stichtenoth [589], Theorem II.5.9 of Silverman [564] or Exercise 8.36 of Fulton [216]. □

A variant of the above formula is known in the case where some of the $e_\phi(P)$ are divisible by $\mathrm{char}(\Bbbk)$.

Chapter 9

Elliptic Curves

This chapter summarises the theory of elliptic curves. Since there are already many outstanding textbooks on elliptic curves (such as Silverman [564] and Washington [626]) we do not give all the details. Our focus is on facts relevant for the cryptographic applications, especially those for which there is not already a suitable reference.

9.1 Group law

Recall that an elliptic curve over a field $\Bbbk$ is given by a non-singular affine Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{9.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \Bbbk$. There is a unique point $\mathcal{O}_E$ on the projective closure that does not lie on the affine curve.

We recall the formulae for the elliptic curve group law with identity element $\mathcal{O}_E$: For all $P \in E(\Bbbk)$ we have $P + \mathcal{O}_E = \mathcal{O}_E + P = P$ so it remains to consider the case where $P_1, P_2 \in E(\Bbbk)$ are such that $P_1, P_2 \neq \mathcal{O}_E$. In other words, P_1 and P_2 are affine points and so write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Recall that Lemma 7.7.10 shows the inverse of $P_1 = (x_1, y_1)$ is $\iota(P_1) = (x_1, -y_1 - a_1x_1 - a_3)$. Hence, if $x_1 = x_2$ and $y_2 = -y_1 - a_1x_1 - a_3$ (i.e., $P_2 = -P_1$) then $P_1 + P_2 = \mathcal{O}_E$. In the remaining cases let

$$\lambda = \begin{cases} \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P_1 = P_2 \\ \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2. \end{cases} \tag{9.2}$$

and set $x_3 = \lambda^2 + a_1\lambda - x_1 - x_2 - a_2$ and $y_3 = -\lambda(x_3 - x_1) - y_1 - a_1x_3 - a_3$. Then $P_1 + P_2 = (x_3, y_3)$.

Exercise 9.1.1. It is possible to "unify" the two cases in equation (9.2). Show that if $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ lie on $y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$ and $y_2 \neq -y_1 - a_1x_1 - a_3$ then $P_1 + P_2$ can be computed using the fomula

$$\lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + a_2(x_1 + x_2) + a_4 - a_1y_1}{y_1 + y_2 + a_1x_2 + a_3} \tag{9.3}$$

instead of equation (9.2).

Definition 9.1.2. Let E be an elliptic curve over a field $\Bbbk$ and let $P \in E(\Bbbk)$. For $n \in \mathbb{N}$ define $[n]P$ to be $P + \cdots + P$ where P appears n times. In particular, $[1]$ is the identity map. Define $[0]P = \mathcal{O}_E$ and $[-n]P = [n](-P)$.

The n**-torsion subgroup** is

$$E[n] = \{P \in E(\overline{\Bbbk}) : [n]P = \mathcal{O}_E\}.$$

We write $E(\Bbbk)[n]$ for $E[n] \cap E(\Bbbk)$.

Exercise 9.1.3. Let $E : y^2 + y = x^3$ be an elliptic curve over $\mathbb{F}_2$. Let $m \in \mathbb{N}$ and $P = (x_P, y_P) \in E(\mathbb{F}_{2^m})$. Show that $[2]P = (x_P^4, y_P^4 + 1)$. (We will show in Example 9.11.6 that this curve is supersingular.)

Exercise 9.1.4. Let $E : y^2 + xy = x^3 + a_2x^2 + a_6$ be an elliptic curve over $\mathbb{F}_{2^m}$ for $m \in \mathbb{N}$. Show that there is a point $P = (x_P, y_P) \in E(\mathbb{F}_{2^m})$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_P + a_2 + a_6/x_P^2) = 0$. Given $Q = (x_Q, y_Q) \in E(\mathbb{F}_{2^m})$ show that the slope of the tangent line to E at Q is $\lambda_Q = x_Q + y_Q/x_Q$. Show that $y_Q = x_Q(\lambda_Q + x_Q)$. Hence show that if $P = [2]Q$ then $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_P) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_2)$, $x_P = x_Q^2 + a_6/x_Q^2$ and $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_6/x_P^2) = 0$. Conversely, show that if $P = (x_P, y_P) \in E(\mathbb{F}_{2^m})$ is such that $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_P) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_2)$ and $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_6/x_P^2) = 0$ then $P = [2]Q$ for some $Q \in E(\mathbb{F}_{2^m})$.

(Point halving) Given $P = (x_P, y_P) \in E(\mathbb{F}_{2^m})$ such that $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_P) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_2)$ show that there are two solutions $\lambda_Q \in \mathbb{F}_{2^m}$ to the equation $\lambda_Q^2 + \lambda_Q = x_P + a_2$. For either solution let $x_Q = \sqrt{x_P(\lambda_P + \lambda_Q + x_P + 1)}$, where $\lambda_P = x_P + y_P/x_P$, and $y_Q = x_Q(\lambda_Q + x_Q)$. Show that $[2](x_Q, y_Q) = P$.

One can consider Weierstrass equations over $\Bbbk$ that have a singular point in the affine plane (recall that there is a unique point at infinity $\mathcal{O}_E$ and it is non-singular). By a change of variable one may assume that the singular point is $(0, 0)$ and the equation is $C : y^2 + a_1xy = x^3 + a_2x^2$. Let $G = C(\Bbbk) \cup \{\mathcal{O}_E\} - \{(0, 0)\}$. It turns out that the elliptic curve group law formulae give rise to a group law on G. There is a morphism over $\overline{\Bbbk}$ from C to $\mathbb{P}^1$ and the group law on G corresponds to either the additive group G_a or the multiplicative group G_m; see Section 9 of [122], Section 2.10 of [626] or Proposition III.2.5 of [564] for details.

Since an elliptic curve is a projective variety it is natural to consider addition formulae on projective coordinates. In the applications there are good reasons to do this (for example, to minimise the number of inversions in fast implementations of elliptic curve cryptography, or in the elliptic curve factoring method).

Exercise 9.1.5. Let $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : y_2 : z_2)$ be points on the elliptic curve $E : y^2z = x^3 + a_4xz^2 + a_6z^3$ over $\Bbbk$. Let

$$u = x_1z_2 - x_2z_1.$$

Show that $(x_3 : y_3 : z_3)$ is a projective representation for $P_1 + P_2$ where

$$\begin{aligned} x_3 &= z_1z_2(y_1z_2 - y_2z_1)^2u - (x_1z_2 + x_2z_1)u^3 && (9.4)\\ y_3 &= -z_1z_2(y_1z_2 - y_2z_1)^3 + (2x_1z_2 + x_2z_1)(y_1z_2 - y_2z_1)u^2 - y_1z_2u^3 && (9.5)\\ z_3 &= z_1z_2u^3 && (9.6) \end{aligned}$$

(as long as the resulting point is not $(0, 0, 0)$).

The elliptic curve addition formula of equations (9.3) and (9.4)-(9.6) are undefined on certain inputs (such as $P = \mathcal{O}_E$ or $P_2 = -P_1$) and so one currently needs to make decisions (i.e., use "if" statements) to compute on elliptic curves. This does not agree with the definition of an algebraic group (informally, that the group operation is given by polynomial equations; formally that there is a morphism $E \times E \to E$). However, it can be shown (see Theorem III.3.6 of Silverman [564]) that elliptic curves are algebraic groups.

To make this concrete let E be an elliptic curve over $\Bbbk$ written projectively. A **complete system of addition laws** for $E(\Bbbk)$ is a set of triples of polynomials

$$\{(f_{i,x}(x_1, y_1, z_1, x_2, y_2, z_2), f_{i,y}(x_1, y_1, z_1, x_2, y_2, z_2), f_{i,z}(x_1, y_1, z_1, x_2, y_2, z_2)) : 1 \leq i \leq k\}$$

such that, for all points $P, Q \in E(\Bbbk)$, at least one of $(f_{i,x}(P, Q), f_{i,y}(P, Q), f_{i,z}(P, Q))$ is defined and all triples defined at (P, Q) give a projective representation of the point $P + Q$.

A rather surprising fact, due to Bosma and Lenstra [92], is that one can give a complete system of addition laws for $E(\overline{\Bbbk})$ using only two triples of polynomials. The resulting equations are unpleasant and not useful for practical computation.

9.2 Morphisms Between Elliptic Curves

The goal of this section is to show that a morphism between elliptic curves is the composition of a group homomorphism and a translation. In other words, all geometric maps between elliptic curves have a group-theoretic interpretation.

Theorem 9.2.1. *Let E_1 and E_2 be elliptic curves over $\Bbbk$ and let $\phi : E_1 \to E_2$ be a morphism of varieties such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. Then ϕ is a group homomorphism.*

Proof: (Sketch) The basic idea is to note that $\phi_* : \mathrm{Pic}^0_{\Bbbk}(E_1) \to \mathrm{Pic}^0_{\Bbbk}(E_2)$ (where $\mathrm{Pic}^0_{\Bbbk}(E_i)$ denotes the degree zero divisor class group of E_i over $\Bbbk$) is a group homomorphism and $\phi_*((P) - (\mathcal{O}_{E_1})) = (\phi(P)) - (\mathcal{O}_{E_2})$. We refer to Theorem III.4.8 of [564] for the details. □

Definition 9.2.2. Let E be an elliptic curve over $\Bbbk$ and let $Q \in E(\Bbbk)$. We define the translation map to be the function $\tau_Q : E \to E$ given by $\tau_Q(P) = P + Q$.

Clearly, τ_Q is a rational map that is defined everywhere on E and so is a morphism. Since τ_Q has inverse map τ_{-Q} it follows that τ_Q is an isomorphism of the curve E to itself (though be warned that in the next section we will define isomorphism for pointed curves and τ_Q will not be an isomorphism in this sense).

Corollary 9.2.3. *Let E_1 and E_2 be elliptic curves over $\Bbbk$ and let $\phi : E_1 \to E_2$ be a rational map. Then ϕ is the composition of a group homomorphism and a translation map.*

Proof: First, by Lemma 7.3.6 a rational map to a projective curve is a morphism. Now let $\phi(\mathcal{O}_{E_1}) = Q \in E_2(\Bbbk)$. The composition $\psi = \tau_{-Q} \circ \phi$ is therefore a morphism. By as in Theorem 9.2.1 it is a group homomorphism. □

Hence, every rational map between elliptic curves corresponds naturally to a map of groups. Theorem 9.6.19 gives a partial converse.

Example 9.2.4. Let $E : y^2 = x^3 + x$ and $Q = (0, 0)$. We determine the map τ_Q on E.

Let $P = (x, y) \in E(\overline{\Bbbk})$ be a point such that P is neither Q nor $\mathcal{O}_E$. To add P and Q to obtain (x_3, y_3) we compute $\lambda = (y - 0)/(x - 0) = y/x$. It follows that

$$x_3 = \lambda^2 - x - 0 = \frac{y^2}{x^2} - x = \frac{y^2 - x^3}{x^2} = \frac{1}{x}$$

and

$$y_3 = -\lambda(x_3 - 0) - 0 = \frac{-y}{x^2}.$$

Hence $\tau_Q(x, y) = (1/x, -y/x^2)$ away from $\{\mathcal{O}_E, Q\}$. It is clear that τ_Q is a rational map of degree 1 and hence an isomorphism of curves by Lemma 8.1.15. Indeed, it is easy to see that the inverse of τ_Q is itself (this is because Q has order 2).

One might wish to write τ_Q projectively (we write the rational map in the form mentioned in Exercise 5.5.2). Replacing x by x/z and y by y/z gives $\tau_Q(x/z, y/z) = (z/x, -yz/x^2)$ from which we deduce

$$\tau_Q(x : y : z) = (xz : -yz : x^2). \tag{9.7}$$

Note that this map is not defined at either $\mathcal{O}_E = (0 : 1 : 0)$ or $Q = (0 : 0 : 1)$, in the sense that evaluating at either point gives $(0 : 0 : 0)$.

To get a map defined at Q one can multiply the right hand side of equation (9.7) through by y to get

$$(xyz : -y^2z : x^2y) = (xyz : -x^3 - xz^2 : x^2y)$$

and dividing by x gives $\tau_Q(x : y : z) = (yz : -x^2 - z^2 : xy)$. One can check that $\tau_Q(0 : 0 : 1) = (0 : -1 : 0) = (0 : 1 : 0)$ as desired. Similarly, to get a map defined at $\mathcal{O}_E$ one can multiply (9.7) by x, re-arrange, and divide by z to get

$$\tau_Q(x : y : z) = (x^2 : -xy : y^2 - xz),$$

which gives $\tau_Q(0 : 1 : 0) = (0 : 0 : 1)$ as desired.

9.3 Isomorphisms of Elliptic Curves

We have already defined isomorphisms of algebraic varieties. It is natural to ask when two Weierstrass equations are isomorphic. Since one can compose any isomorphism with a translation map it is sufficient to restrict attention to isomorphisms $\phi : E \to \widetilde{E}$ such that $\phi(\mathcal{O}_E) = \mathcal{O}_{\widetilde{E}}$.

Formally, one defines a **pointed curve** to be a curve C over a field $\Bbbk$ together with a fixed $\Bbbk$-rational point P_0. An **isomorphism of pointed curves** $\phi : (C, P_0) \to (\widetilde{C}, \widetilde{P}_0)$ is an isomorphism $\phi : C \to \widetilde{C}$ over $\overline{\Bbbk}$ of varieties such that $\phi(P_0) = \widetilde{P}_0$. When one refers to an elliptic curve one usually means the pointed curve $(E, \mathcal{O}_E)$.

Definition 9.3.1. Let $(E, \mathcal{O}_E)$ and $(\widetilde{E}, \mathcal{O}_{\widetilde{E}})$ be elliptic curves over $\Bbbk$. An **isomorphism of elliptic curves** $\phi : E \to \widetilde{E}$ is an isomorphism over $\overline{\Bbbk}$ of algebraic varieties such that $\phi(\mathcal{O}_E) = \mathcal{O}_{\widetilde{E}}$. If there is an isomorphism from E to $\widetilde{E}$ then we write $E \cong \widetilde{E}$.

By Theorem 9.2.1, an isomorphism of elliptic curves is a group homomorphism over $\overline{\Bbbk}$.

Exercise 9.3.2. Let E_1 and E_2 be elliptic curves over $\Bbbk$. Show that if E_1 is isomorphic over $\Bbbk$ to E_2 then $E_1(\Bbbk)$ is isomorphic as a group to $E_2(\Bbbk)$. In particular, if $\Bbbk = \mathbb{F}_q$ is a finite field then $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Note that the translation map τ_Q is not considered to be an isomorphism of the pointed curve $(E, \mathcal{O}_E)$ to itself, unless $Q = \mathcal{O}_E$ in which case τ_Q is the identity map.

Exercise 9.3.3. Exercises 7.2.6 and 7.2.7 give simplified Weierstrass models for elliptic curves when $\mathrm{char}(\Bbbk) \neq 3$. Verify that there are isomorphisms, from a general Weierstrass equation to these models, that fix $\mathcal{O}_E$.

Theorem 9.3.4. *Let $\Bbbk$ be a field and E_1, E_2 elliptic curves over $\Bbbk$. Every isomorphism from E_1 to E_2 defined over $\overline{\Bbbk}$ restricts to an affine isomorphism of the form*

$$\phi(x, y) = (u^2 x + r, u^3 y + s u^2 x + t) \tag{9.8}$$

where $u, r, s, t \in \overline{\Bbbk}$. The isomorphism is defined over $\Bbbk$ if and only if $u, r, s, t \in \Bbbk$.

Proof: See Proposition III.3.1(b) of [564]. □

Definition 9.3.5. Suppose $\mathrm{char}(\Bbbk) \neq 2, 3$ and let $a_4, a_6 \in \Bbbk$ be such that $4a_4^3 + 27a_6^2 \neq 0$. For the short Weierstrass equation $y^2 z = x^3 + a_4 x z^2 + a_6 z^3$, define the **$j$-invariant**

$$j(E) = 1728 \frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

Suppose $\mathrm{char}(\Bbbk) = 2$ and $a_2, a_6 \in \Bbbk$ with $a_6 \neq 0$. For the short Weierstrass equation $y^2 z + xyz = x^3 + a_2 x^2 z + a_6 z^3$ define the j-invariant

$$j(E) = 1/a_6$$

and for $E : y^2 z + y z^2 = x^3 + a_4 x z^2 + a_6 z^3$ (we now allow $a_6 = 0$) define $j(E) = 0$.

We refer to Section III.1 of [564] for the definition of the j-invariant for general Weierstrass equations.

Theorem 9.3.6. *Let $\Bbbk$ be a field and E_1, E_2 elliptic curves over $\Bbbk$. Then there is an isomorphism from E_1 to E_2 defined over $\overline{\Bbbk}$ if and only if $j(E_1) = j(E_2)$.*

Proof: See Proposition III.1.4(b) of [564] or Theorem 2.19 of [626]. □

Exercise 9.3.7. Let $E : y^2 = x^3 + a_4 x + a_6$ be an elliptic curve. Show that $j(E) = 0$ if and only if $a_4 = 0$ and $j(E) = 1728$ if and only if $a_6 = 0$. Suppose $\mathrm{char}(\Bbbk) \neq 2, 3$. Let $j \in \Bbbk$, $j \neq 0, 1728$. Show that the elliptic curve

$$E : y^2 = x^3 + \frac{3j}{1728 - j} x + \frac{2j}{1728 - j}$$

has $j(E) = j$. The discriminant of E is $2^8 \cdot 3^5 / (1728 - j)^3$.

Exercise 9.3.8. Let $E_1 : y^2 + y = x^3$, $E_2 : y^2 + y = x^3 + 1$ and $E_3 : y^2 + y = x^3 + x$ be elliptic curves over $\mathbb{F}_2$. Since $j(E_1) = j(E_2) = j(E_3) = 0$ it follows that there are isomorphisms over $\overline{\mathbb{F}}_2$ from E_1 to E_2 and from E_1 to E_3. Write down such isomorphisms.

Exercise 9.3.9. Let E_1, E_2 be elliptic curves over $\mathbb{F}_q$ that are isomorphic over $\mathbb{F}_q$. Show that the discrete logarithm problem in $E_1(\mathbb{F}_q)$ is equivalent to the discrete logarithm problem in $E_2(\mathbb{F}_q)$. In other words, the discrete logarithm problem on $\mathbb{F}_q$-isomorphic curves has exactly the same security.

To reduce storage in some applications it might be desirable to choose a model for elliptic curves with coefficients as small as possible. Let $p > 3$ be prime. It has been proven (see Section 5 of Banks and Shparlinski [27]) that "almost all" $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ have a model of the form $y^2 = x^3 + a_4x + a_6$ where $1 \leq a_4, a_6 \leq p^{1/2+o(1)}$. Since there are $O(p)$ isomorphism classes this result is optimal. Note that finding such a "small" pair (a_4, a_6) for a given j-invariant may not be easy.

9.4 Automorphisms

Definition 9.4.1. Let E be an elliptic curve over $\Bbbk$. An **automorphism** of E is an isomorphism from $(E, \mathcal{O}_E)$ to itself defined over $\overline{\Bbbk}$. The set of all automorphisms of E is denoted $\mathrm{Aut}(E)$.

We stress that an automorphism maps $\mathcal{O}_E$ to $\mathcal{O}_E$. Under composition, $\mathrm{Aut}(E)$ forms a group, The identity of the group is the identity map.

Example 9.4.2. The map $\phi(P) = -P$ is an automorphism that is not the identity map. On $y^2 = x^3 + 1$ over $\Bbbk$ the map $\rho(x, y) = (\zeta_3 x, y)$ is an automorphism where $\zeta_3 \in \overline{\Bbbk}$ satisfies $\zeta_3^3 = 1$.

Exercise 9.4.3. Show that if E_1 and E_2 are elliptic curves over $\Bbbk$ that are isomorphic over $\overline{\Bbbk}$ then $\mathrm{Aut}(E_1) \cong \mathrm{Aut}(E_2)$.

Theorem 9.4.4. *Let E be an elliptic curve over $\Bbbk$. Then $\#\mathrm{Aut}(E)$ is even and $\#\mathrm{Aut}(E) \mid 24$. More precisely*

- $\#\mathrm{Aut}(E) = 2$ *if* $j(E) \neq 0, 1728$,
- $\#\mathrm{Aut}(E) = 4$ *if* $j(E) = 1728$ *and* $\mathrm{char}(\Bbbk) \neq 2, 3$,
- $\#\mathrm{Aut}(E) = 6$ *if* $j(E) = 0$ *and* $\mathrm{char}(\Bbbk) \neq 2, 3$,
- $\#\mathrm{Aut}(E) = 12$ *if* $j(E) = 0$ *and* $\mathrm{char}(\Bbbk) = 3$,
- $\#\mathrm{Aut}(E) = 24$ *if* $j(E) = 0$ *and* $\mathrm{char}(\Bbbk) = 2$.

(Note that when $\mathrm{char}(\Bbbk) = 2$ *or* 3 *then* $0 = 1728$ *in* $\Bbbk$*.)*

Proof: See Theorem III.10.1 and Proposition A.1.2 of [564]. □

Exercise 9.4.5. Consider $E : y^2 + y = x^3$ over $\mathbb{F}_2$. Let $u \in \overline{\mathbb{F}}_2$ satisfy $u^3 = 1$, $s \in \overline{\mathbb{F}}_2$ satisfy $s^4 + s = 0$ and $t \in \overline{\mathbb{F}}_2$ satisfy $t^2 + t = s^6$. Show that $u, s \in \mathbb{F}_{2^2}$, $t \in \mathbb{F}_{2^4}$ and that

$$\phi(x, y) = (u^2x + s^2, y + u^2sx + t)$$

is an automorphism of E. Note that one can replace u^2 by u and/or swap s and s^2. Show that every automorphism arises this way and so $\#\mathrm{Aut}(E) = 24$. Show that if $\phi \in \mathrm{Aut}(E)$ then either $\phi^2 = \pm 1$ or $\phi^3 = \pm 1$. Show that $\mathrm{Aut}(E)$ is non-Abelian.

9.5 Twists

Twists of elliptic curves have several important applications such as point compression in pairing-based cryptography (see Section 26.6.2), and efficient endomorphisms on elliptic curves (see Exercise 11.3.24).

Definition 9.5.1. Let E be an elliptic curve over $\Bbbk$. A **twist** of E is an elliptic curve $\widetilde{E}$ over $\Bbbk$ such that there is an isomorphism $\phi : E \to \widetilde{E}$ over $\overline{\Bbbk}$ of pointed curves (i.e., such that $\phi(\mathcal{O}_E) = \mathcal{O}_{\widetilde{E}}$). Two twists $\widetilde{E}_1$ and $\widetilde{E}_2$ of E are **equivalent** if there is an isomorphism from $\widetilde{E}_1$ to $\widetilde{E}_2$ defined over $\Bbbk$. A twist $\widetilde{E}$ of E is called a **trivial twist** if $\widetilde{E}$ is equivalent to E. Denote by $\mathrm{Twist}(E)$ the set of equivalence classes of twists of E.

Example 9.5.2. Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2$. Let $E : y^2 = x^3 + a_4x + a_6$ over $\Bbbk$ and let $d \in \Bbbk^*$. Define the elliptic curve $E^{(d)} : y^2 = x^3 + d^2a_4x + d^3a_6$. The map $\phi(x, y) = (dx, d^{3/2}y)$ is an isomorphism from E to $E^{(d)}$. Hence $E^{(d)}$ is a twist of E. Note that $E^{(d)}$ is a trivial twist if $\sqrt{d} \in \Bbbk^*$.

If $\Bbbk = \mathbb{Q}$ then there are infinitely many non-equivalent twists $E^{(d)}$, since one can let d run over the square-free elements in $\mathbb{N}$.

Exercise 9.5.3. Let q be an odd prime power and let $E : y^2 = x^3 + a_4x + a_6$ over $\mathbb{F}_q$. Let $d \in \mathbb{F}_q^*$. Show that the twist $E^{(d)}$ of E by d is not isomorphic over $\mathbb{F}_q$ to E if and only if d is a non-square (i.e., the equation $u^2 = d$ has no solution in $\mathbb{F}_q$). Show also that if d_1 and d_2 are non-squares in $\mathbb{F}_q^*$ then $E^{(d_1)}$ and $E^{(d_2)}$ are isomorphic over $\mathbb{F}_q$. Hence, there is is a unique $\mathbb{F}_q$-isomorphism class of elliptic curves arising in this way. Any curve in this isomorphism class is called a **quadratic twist** of E.

Exercise 9.5.4. Show that if $E : y^2 = x^3 + a_4x + a_6$ over $\mathbb{F}_q$ has $q + 1 - t$ points then a quadratic twist of E has $q + 1 + t$ points over $\mathbb{F}_q$.

Exercise 9.5.5. Let $F(x) = x^3 + a_2x^2 + a_4x + a_6$ and let $E : y^2 + (a_1x + a_3)y = F(x)$ be an elliptic curve over $\mathbb{F}_{2^n}$. Let $\alpha \in \mathbb{F}_{2^n}$ be such that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha) = 1$. Define $\widetilde{E} : y^2 + (a_1x + a_3)y = F(x) + \alpha(a_1x + a_3)^2$. For the special case (see Exercise 7.2.7) $E : y^2 + xy = x^3 + a_2x^2 + a_6$ this is $\widetilde{E} : y^2 + xy = x^3 + (a_2 + \alpha)x^2 + a_6$.

Show that $\widetilde{E}$ is isomorphic to E over $\mathbb{F}_{2^{2n}}$ but not over $\mathbb{F}_{2^n}$. Hence, it makes sense to call $\widetilde{E}$ a **quadratic twist** of E. Show, using Exercise 2.14.7, that $\#E(\mathbb{F}_{2^n}) + \#\widetilde{E}(\mathbb{F}_{2^n}) = 2(2^n + 1)$. Hence, if $\#E(\mathbb{F}_{2^n}) = 2^n + 1 - t$ then $\#\widetilde{E}(\mathbb{F}_{2^n}) = 2^n + 1 + t$.

Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$. Let $\phi : E \to \widetilde{E}$ be an isomorphism that is not defined over $\Bbbk$. Then $\phi^{-1} : \widetilde{E} \to E$ is also an isomorphism that is not defined over $\Bbbk$. One can therefore consider $\sigma(\phi^{-1}) : \widetilde{E} \to E$ for any $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. The composition $\psi(\sigma) = \sigma(\phi^{-1}) \circ \phi$ is therefore an automorphism of E.

Exercise 9.5.6. Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$. Show that if $\phi : E \to \widetilde{E}$ is an isomorphism that is not defined over $\Bbbk$ then there exists some $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ such that $\sigma(\phi^{-1}) \circ \phi$ is not the identity.

One can show that $\sigma \mapsto \sigma(\phi^{-1}) \circ \phi$ is a 1-cocycle with values in $\mathrm{Aut}(E)$. We refer to Section X.2 of Silverman [564] for further discussion of this aspect of the theory (note that Silverman considers twists for general curves C and his definition of $\mathrm{Twist}(C)$ is not for pointed curves).

Lemma 9.5.7. *Let E be an elliptic curve over a finite field $\Bbbk$ where $\mathrm{char}(\Bbbk) \neq 2, 3$ and $j(E) \neq 0, 1728$. Then $\#\mathrm{Twist}(E) = 2$.*

Proof: Let $\widetilde{E}/\Bbbk$ be isomorphic to E. Without loss of generality E and $\widetilde{E}$ are given in short Weierstrass form $y^2 = x^3 + a_4x + a_6$ and $Y^2 = X^3 + a_4'X + a_6'$ with $a_4, a_4', a_6, a_6' \neq 0$. Since $\widetilde{E} \cong E$ over $\overline{\Bbbk}$ it follows from Theorem 9.3.4 that $a_4' = u^4 a_4$ and $a_6' = u^6 a_6$ for some $u \in \overline{\Bbbk}^*$. Hence $u^2 = a_6' a_4 / (a_6 a_4') \in \Bbbk^*$. Since $\Bbbk$ is finite and $\mathrm{char}(\Bbbk) \neq 2$ the result follows from the fact that $[\Bbbk^* : (\Bbbk^*)^2] = 2$. □

An immediate consequence of Lemma 9.5.7 is that the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ is approximately $2q$.

Exercise 9.5.8. ★ Let $\Bbbk$ be a finite field such that $\mathrm{char}(\Bbbk) \geq 5$ and let E be an elliptic curve over $\Bbbk$. Show that $\#\mathrm{Twist}(E) = \#(\Bbbk^*/(\Bbbk^*)^d)$ where $d = 2$ if $j(E) \neq 0, 1728$, $d = 4$ if $j(E) = 1728$, $d = 6$ if $j(E) = 0$.

Due to Theorem 9.4.4 one might be tempted to phrase Lemma 9.5.7 and Exercise 9.5.8 as $\#\mathrm{Twist}(E) = \#\mathrm{Aut}(E)$, but the following example shows that this statement is not true in general.

Exercise 9.5.9. Let $E : y^2 + y = x^3$ over $\mathbb{F}_2$. Show that the number of non-equivalent twists of E over $\mathbb{F}_2$ is 4, whereas $\#\mathrm{Aut}(E) = 24$.

Exercise 9.5.10. Let $E : y^2 = x^3 + x$ over $\mathbb{F}_{19}$ (note that $j(E) = 1728$). Show that $\#\mathrm{Twist}(E) = 2$. Now consider the same curve over $\mathbb{F}_{19^2}$. Show that $\#\mathrm{Twist}(E) = 4$. Show that the group orders of the twists are $19^2 + 1$ (twice) and $(19 \pm 1)^2$.

9.6 Isogenies

We now return to more general maps between elliptic curves. Recall from Theorem 9.2.1 that a morphism $\phi : E_1 \to E_2$ of elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is a group homomorphism. Hence, isogenies are group homomorphisms. Chapter 25 discusses isogenies in further detail. In particular, Chapter 25 describes algorithms to compute isogenies efficiently.

Definition 9.6.1. Let E_1 and E_2 be elliptic curves over $\Bbbk$. An **isogeny** over $\Bbbk$ is a morphism $\phi : E_1 \to E_2$ over $\Bbbk$ such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. The **zero isogeny** is the constant map $\phi : E_1 \to E_2$ given by $\phi(P) = \mathcal{O}_{E_2}$ for all $P \in E_1(\overline{\Bbbk})$. If $\phi(x, y) = (\phi_1(x, y), \phi_2(x, y))$ is an isogeny then define $-\phi$ by $(-\phi)(x, y) = -(\phi_1(x, y), \phi_2(x, y))$. where $-(X, Y)$ denotes, as always, the inverse for the group law. The **kernel** of an isogeny is $\ker(\phi) = \{P \in E_1(\overline{\Bbbk}) : \phi(P) = \mathcal{O}_{E_2}\}$. The **degree** of a non-zero isogeny is the degree of the morphism. The degree of the zero isogeny is 0. If there is an isogeny (respectively, isogeny of degree d) between two elliptic curves E_1 and E_2 then we say that E_1 and E_2 are **isogenous** (respectively, **d-isogenous**). A non-zero isogeny is **separable** if it is separable as a morphism (see Definition 8.1.6). Denote by $\mathrm{Hom}_{\Bbbk}(E_1, E_2)$ the set of isogenies from E_1 to E_2 defined over $\Bbbk$. Denote by $\mathrm{End}_{\Bbbk}(E_1)$ the set of isogenies from E_1 to E_1 defined over $\Bbbk$; this is called the **endomorphism ring** of the elliptic curve.

Exercise 9.6.2. Show that if $\phi : E_1 \to E_2$ is an isogeny then so is $-\phi$.

Theorem 9.6.3. *Let E_1 and E_2 be elliptic curves over $\Bbbk$. If $\phi : E_1 \to E_2$ is a non-zero isogeny over $\overline{\Bbbk}$ then $\phi : E_1(\overline{\Bbbk}) \to E_2(\overline{\Bbbk})$ is surjective.*

Proof: This follows from Theorem 8.2.7. □

We now relate the degree to the number of points in the kernel. First we remark the standard group theoretical fact that, for all $Q \in E_2(\overline{\Bbbk})$, $\#\phi^{-1}(Q) = \#\ker(\phi)$ (this is just the fact that all cosets have the same size).

Lemma 9.6.4. *A non-zero separable isogeny $\phi : E_1 \to E_2$ over $\Bbbk$ of degree d has $\#\ker(\phi) = d$.*

Proof: It follows from Corollary 8.2.13 that a separable degree d map ϕ has $\#\phi^{-1}(Q) = d$ for a generic point $Q \in E_2(\overline{\Bbbk})$. Hence, by the above remark, $\#\phi^{-1}(Q) = d$ for all points Q and $\#\ker(\phi) = d$. (Also see Proposition 2.21 of [626] for an elementary proof.) □

A morphism of curves $\phi : C_1 \to C_2$ is called **unramified** if $e_\phi(P) = 1$ for all $P \in C_1(\overline{\Bbbk})$. Let $\phi : E_1 \to E_2$ be a separable isogeny over $\Bbbk$ and let $P \in E_1(\overline{\Bbbk})$. Since $\phi(P) = \phi(P+R)$ for all $R \in \ker(\phi)$ it follows that a separable morphism of elliptic curves is unramified (this also follows from the Hurwitz genus formula).

Exercise 9.6.5. Let E_1 and E_2 be elliptic curves over $\Bbbk$ and suppose $\phi : E_1 \to E_2$ is an isogeny over $\Bbbk$. Show that $\ker(\phi)$ is defined over $\Bbbk$ (in the sense that $P \in \ker(\phi)$ implies $\sigma(P) \in \ker(\phi)$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$).

Lemma 9.6.6. *Let E_1 and E_2 be elliptic curves over $\Bbbk$. Then $\mathrm{Hom}_\Bbbk(E_1, E_2)$ is a group with addition defined by $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$. Furthermore, $\mathrm{End}_\Bbbk(E_1) = \mathrm{Hom}_\Bbbk(E_1, E_1)$ is a ring with addition defined in the same way and with multiplication defined by composition.*

Proof: The main task is to show that if $\phi_1, \phi_2 : E_1 \to E_2$ are morphisms then so is $(\phi_1 + \phi_2)$. The case $\phi_2 = -\phi_1$ is trivial, so assume $\phi_2 \neq -\phi_1$. Let U be an open set such that: ϕ_1 and ϕ_2 are regular on U; $P \in U$ implies $\phi_1(P) \neq \mathcal{O}_{E_2}$ and $\phi_2(P) \neq \mathcal{O}_{E_2}$; $\phi_1(P) \neq -\phi_2(P)$. That such an open set exists is immediate for all but the final requirement; but one can also show that the points such that $\phi_1(x, y) = -\phi_2(x, y)$ form a closed subset of E_1 as long as $\phi_1 \neq -\phi_2$. Then using equation (9.3) one obtains a rational map $(\phi_1 + \phi_2) : E_1 \to E_2$. Finally, since composition of morphisms is a morphism it is easy to check that $\mathrm{End}_\Bbbk(E_1)$ is a ring. □

By Exercise 8.1.12, if $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_3$ are non-constant isogenies then $\deg(\phi_2 \circ \phi_1) = \deg(\phi_2)\deg(\phi_1)$. This fact will often be used.

An important example of an isogeny is the multiplication by n map.

Exercise 9.6.7. Show that $[n]$ is an isogeny.

Example 9.6.8. Let $E : y^2 = x^3 + x$. Then the map $[2] : E \to E$ is given by the rational function

$$[2](x, y) = \left(\frac{(x^2-1)^2}{4(x^3+x)}, \frac{y(x^6+5x^4-5x^2-1)}{8(x^3+x)^2} \right).$$

The kernel of $[2]$ is $\mathcal{O}_E$ together with the three points $(x_P, 0)$ such that $x_P^3 + x_P = 0$. In other words, the kernel is the set of four points of order dividing 2.

We now give a simple example of an isogeny that is not $[n]$ for some $n \in \mathbb{N}$. The derivation of a special case of this example is given in Example 25.1.5.

Example 9.6.9. Let $A, B \in \Bbbk$ be such that $B \neq 0$ and $D = A^2 - 4B \neq 0$. Consider the elliptic curve $E : y^2 = x(x^2 + Ax + B)$ over $\Bbbk$, which has the point $(0, 0)$ of order 2. There is an elliptic curve $\widetilde{E}$ and an isogeny $\phi : E \to \widetilde{E}$ such that $\ker(\phi) = \{\mathcal{O}_E, (0, 0)\}$. One can verify that

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(B-x^2)}{x^2} \right) = \left(\frac{x^2+Ax+B}{x}, y\frac{B-x^2}{x^2} \right)$$

has the desired kernel, and the image curve is $\widetilde{E} : Y^2 = X(X^2 - 2AX + D)$.

Before proving the next result we need one exercise (which will also be used later).

Exercise 9.6.10. Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$. Show that if $\mathrm{char}(\Bbbk) = 2$ and $a_1 = 0$ then there are no points (x, y) of order 2. Show that if $\mathrm{char}(\Bbbk) = 2$ and $a_1 \neq 0$ then (x, y) has order 2 if and only if $x = a_3/a_1$. Hence, if $\mathrm{char}(\Bbbk) = 2$ then $\#E[2] \in \{1, 2\}$.

Show that if $\mathrm{char}(\Bbbk) \neq 2$ then (x, y) has order 2 if and only if $2y + a_1x + a_3 = 0$. Show that this is also equivalent to

$$4x^3 + (a_1^2 + 4a_2)x^2 + (2a_1a_3 + 4a_4)x + (a_3^2 + 4a_6) = 0. \tag{9.9}$$

Note that when $a_1 = a_3 = 0$ this polynomial is simply 4 times the right hand side of the elliptic curve equation. Show that this polynomial has distinct roots and so if $\mathrm{char}(\Bbbk) \neq 2$ then $\#E[2] = 4$.

Lemma 9.6.11. *Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$. If $n \in \mathbb{N}$ then $[n]$ is not the zero isogeny. Further, $\mathrm{Hom}_{\Bbbk}(E, \widetilde{E})$ is torsion-free as a $\mathbb{Z}$-module (i.e., if $\phi \in \mathrm{Hom}_{\Bbbk}(E, \widetilde{E})$ is non-zero then $[n] \circ \phi$ is non-zero for all $n \in \mathbb{Z}$, $n \neq 0$) and $\mathrm{End}_{\Bbbk}(E)$ has no zero divisors.*

Proof: First, suppose $\phi_1, \phi_2 : E \to E$ are non-zero isogenies such that $[0] = \phi_1 \circ \phi_2$. By Theorem 9.6.3, ϕ_1, ϕ_2 and hence $\phi_1 \circ \phi_2$ are surjective over $\overline{\Bbbk}$. Since the zero isogeny is not surjective it follows that there are no zero divisors in $\mathrm{End}_{\Bbbk}(E)$.

Now, consider any $n \in \mathbb{N}$ and note that $n = 2^k m$ for some $k \in \mathbb{Z}_{\geq 0}$ and some odd $m \in \mathbb{N}$. By Exercise 9.6.10 we know that $[2]$ is not zero over $\overline{\Bbbk}$ (when $\mathrm{char}(\Bbbk) \neq 2$ this is immediate since there are at most 3 points of order 2; when $\mathrm{char}(\Bbbk) = 2$ one must show that if equation (9.9) is identically zero then the Weierstrass equation is singular). It follows that $[2^k] = [2] \circ [2] \circ \cdots \circ [2]$ is not zero either (since if $[2]$ is non-zero then it is surjective on $E(\overline{\Bbbk})$). Finally, since there exists $P \in E(\overline{\Bbbk})$ such that $P \neq \mathcal{O}_E$ but $[2]P = \mathcal{O}_E$ we have $[m]P = P \neq \mathcal{O}_E$ and so $[m]$ is not the zero isogeny. It follows that $[n] = [m] \circ [2^k]$ is not the zero isogeny.

Similarly, if $[0] = [n]\phi$ for $\phi \in \mathrm{Hom}_{\Bbbk}(E, \widetilde{E})$ then either $[n]$ or ϕ is the zero isogeny. □

Lemma 9.6.12. *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $\widetilde{E} : Y^2 + \widetilde{a}_1XY + \widetilde{a}_3Y = X^3 + \widetilde{a}_2X^2 + \widetilde{a}_4X + \widetilde{a}_6$ be elliptic curves over $\Bbbk$. Let $\phi : E \to \widetilde{E}$ be an isogeny of elliptic curves over $\Bbbk$. Then ϕ may be expressed by a rational function in the form*

$$\phi(x, y) = (\phi_1(x), y\phi_2(x) + \phi_3(x))$$

where

$$2\phi_3(x) = -\widetilde{a}_1\phi_1(x) - \widetilde{a}_3 + (a_1x + a_3)\phi_2(x).$$

In particular, if $\mathrm{char}(\Bbbk) \neq 2$ and $a_1 = a_3 = \widetilde{a}_1 = \widetilde{a}_3 = 0$ then $\phi_3(x) = 0$, while if $\mathrm{char}(\Bbbk) = 2$ then $\phi_2(x) = (\widetilde{a}_1\phi_1(x) + \widetilde{a}_3)/(a_1x + a_3)$.

Proof: Certainly, ϕ may be written as $\phi(x, y) = (\phi_1(x) + yf(x), y\phi_2(x) + \phi_3(x))$ where $\phi_1(x), f(x), \phi_2(x)$ and $\phi_3(x)$ are rational functions.

Since ϕ is a group homomorphism it satisfies $\phi(-P) = -\phi(P)$. Writing $P = (x, y)$ the left hand side is

$$\begin{aligned} \phi(-(x, y)) &= \phi(x, -y - a_1x - a_3) \\ &= (\phi_1(x) + (-y - a_1x - a_3)f(x), (-y - a_1x - a_3)\phi_2(x) + \phi_3(x)) \end{aligned}$$

while the right hand side is

$$-\phi(P) \quad = \quad (\phi_1(x) + yf(x), -y\phi_2(x) - \phi_3(x) - \widetilde{a}_1(\phi_1(x) + yf(x)) - \widetilde{a}_3).$$

It follows that $(2y + a_1x + a_3)f(x)$ is a function that is zero for all points $(x, y) \in E(\overline{\Bbbk})$. Since $2y + a_1x + a_3$ is not the zero function (if it was zero then $\Bbbk(E) = \Bbbk(x, y) = \Bbbk(y)$, which contradicts Theorem 8.6.4) it follows that $f(x) = 0$.

It then follows that

$$2\phi_3(x) = -\widetilde{a}_1\phi_1(x) - \widetilde{a}_3 + (a_1x + a_3)\phi_2(x).$$

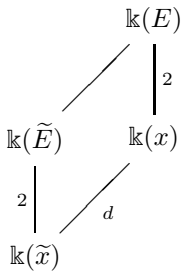
□

Lemma 9.6.12 will be refined in Theorem 9.7.5.

Lemma 9.6.13. *Let $\phi : E \to \widetilde{E}$ be as in Lemma 9.6.12 where $\phi_1(x) = a(x)/b(x)$. Then the degree of ϕ is* $\max\{\deg_x(a(x)), \deg_x(b(x))\}$.

Corollary 25.1.8 will give a more precise version of this result in a special case.

Proof: We have $\Bbbk(E) = \Bbbk(x, y)$ being a quadratic extension of $\Bbbk(x)$, and $\Bbbk(\widetilde{E}) = \Bbbk(\widetilde{x}, \widetilde{y})$ being a quadratic extension of $\Bbbk(\widetilde{x})$. Now $\phi_1(x)$ gives a morphism $\phi_1 : \mathbb{P}^1 \to \mathbb{P}^1$ and this morphism has degree $d = \max\{\deg_x(a(x)), \deg_x(b(x))\}$ by Lemma 8.1.9. It follows that $\Bbbk(x)$ is a degree d extension of $\phi_1^*\Bbbk(\widetilde{x})$. We therefore have the following diagram of field extensions



and it follows that $[\Bbbk(E) : \phi^*\Bbbk(\widetilde{E})] = d$. □

Example 9.6.14. Let p be a prime and let $q = p^m$ for some $m \in \mathbb{N}$. Let E be an elliptic curve over $\mathbb{F}_q$. The q-power **Frobenius map** is the rational map $\pi_q : E \to E$ such that $\pi_q(\mathcal{O}_E) = \mathcal{O}_E$ and $\pi_q(x, y) = (x^q, y^q)$. Since π_q is a morphism that fixes $\mathcal{O}_E$ it is an isogeny (this can also be easily seen by explicit computation). If E has equation $y^2 = F(x)$ (and so q is odd) then one can write π_q in the form of Lemma 9.6.12 as $\pi_q(x, y) = (x^q, yF(x)^{(q-1)/2})$. Note that π_q is the identity map on $E(\mathbb{F}_q)$ but is not the identity on $E(\overline{\mathbb{F}}_q)$.

Corollary 9.6.15. *Let the notation be as in Example 9.6.14. The q-power Frobenius map is inseparable of degree q.*

Exercise 9.6.16. Prove Corollary 9.6.15.

Theorem 9.6.17. *Let p be a prime and $E, \widetilde{E}$ elliptic curves over $\overline{\mathbb{F}}_p$. Let $\psi : E \to \widetilde{E}$ be a non-zero isogeny. Then there is an integer m and an elliptic curve $E^{(q)}$ (namely, the curve obtained by applying the $q = p^m$-power Frobenius map to the coefficients of E; the reader should not confuse the notation $E^{(q)}$ with the quadratic twist $E^{(d)}$) and a separable isogeny $\phi : E^{(q)} \to \widetilde{E}$ of degree* $\deg(\psi)/q$ *such that $\psi = \phi \circ \pi_q$ where $\pi_q : E \to E^{(q)}$ is the q-power Frobenius morphism.*

Proof: See Corollary II.2.12 of [564]. □

The following result is needed to obtain many useful results in this chapter and in Chapter 25.

Theorem 9.6.18. *Let E_1, E_2, E_3 be elliptic curves over $\Bbbk$ and $\phi : E_1 \to E_2$, $\psi : E_1 \to E_3$ isogenies over $\Bbbk$. Suppose $\ker(\phi) \subseteq \ker(\psi)$ and that ψ is separable. Then there is a unique isogeny $\lambda : E_2 \to E_3$ defined over $\Bbbk$ such that $\psi = \lambda \circ \phi$.*

Proof: (Sketch) See Corollary III.4.11 of [564] for the case where $\Bbbk$ is algebraically closed. The proof uses the fact that $\overline{\Bbbk}(E_1)$ is a Galois extension of $\phi^*(\overline{\Bbbk}(E_2))$ (with Galois group isomorphic to $\ker(\phi)$). Furthermore, one has $\psi^*(\overline{\Bbbk}(E_3)) \subseteq \phi^*(\overline{\Bbbk}(E_2)) \subseteq \overline{\Bbbk}(E_1)$. The existence and uniqueness of the morphism λ follows from the Galois extension $\phi^*(\overline{\Bbbk}(E_2))/\psi^*(\overline{\Bbbk}(E_3))$ and Theorem 5.5.27. The uniqueness of λ implies it is actually defined over $\Bbbk$, since

$$\psi = \sigma(\psi) = \sigma(\lambda) \circ \sigma(\phi) = \sigma(\lambda) \circ \phi.$$

for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. □

Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$. Not every group homomorphism $E(\Bbbk) \to \widetilde{E}(\Bbbk)$ is an isogeny. In particular, a non-zero isogeny has finite degree and hence finite kernel, whereas one can have groups such as $E(\mathbb{Q}) \cong \mathbb{Z}$ and $\widetilde{E}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ for which there is a non-zero group homomorphism $E(\mathbb{Q}) \to \widetilde{E}(\mathbb{Q})$ whose kernel is infinite. It is natural to ask whether every group homomorphism with finite kernel is an isogeny. The following result shows that this is the case (the condition of being defined over $\Bbbk$ can be ignored by taking a field extension).

Theorem 9.6.19. *Let E be an elliptic curve over $\Bbbk$. Let $G \subseteq E(\overline{\Bbbk})$ be a finite group that is defined over $\Bbbk$ (i.e., $\sigma(P) \in G$ for all $P \in G$ and $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$). Then there is a unique (up to isomorphism over $\overline{\Bbbk}$) elliptic curve $\widetilde{E}$ over $\Bbbk$ and a (not necessarily unique) isogeny $\phi : E \to \widetilde{E}$ over $\Bbbk$ such that $\ker(\phi) = G$.*

Proof: See Proposition III.4.12 and Exercise 3.13(e) of [564]. We will give a constructive proof (Vélu's formulae) in Section 25.1.1, which also proves that the isogeny is defined over $\Bbbk$. □

The elliptic curve $\widetilde{E}$ in Theorem 9.6.19 is sometimes written E/G. As noted, the isogeny in Theorem 9.6.19 is not necessarily unique, but Exercise 9.6.20 shows the only way that non-uniqueness can arise.

Exercise 9.6.20. Let the notation be as in Theorem 9.6.19. Let $\psi : E \to \widetilde{E}$ be another isogeny over $\Bbbk$ such that $\ker(\psi) = G$. Show that $\psi = \lambda \circ \phi$ where λ is an automorphism of $\widetilde{E}$ (or, if $\Bbbk$ is finite, the composition of an isogeny and a Frobenius map). Similarly, if $\psi : E \to E_2$ is an isogeny over $\Bbbk$ with $\ker(\psi) = G$ then show that $\psi = \lambda \circ \phi$ where $\lambda : \widetilde{E} \to E_2$ is an isomorphism over $\Bbbk$ of elliptic curves.

We now present the dual isogeny. Let $\phi : E \to \widetilde{E}$ be an isogeny over $\Bbbk$. Then there is a group homomorphism $\phi^* : \mathrm{Pic}^0_{\Bbbk}(\widetilde{E}) \to \mathrm{Pic}^0_{\Bbbk}(E)$. Since $\mathrm{Pic}^0_{\Bbbk}(E)$ is identified with $E(\overline{\Bbbk})$ in a standard way (and similarly for $\widetilde{E}$) one gets a group homomorphism from $\widetilde{E}(\overline{\Bbbk})$ to $E(\overline{\Bbbk})$. Indeed, the next result shows that this is an isogeny of elliptic curves; this is not trivial as ϕ^* is defined set-theoretically and it is not possible to interpret it as a rational map in general.

Theorem 9.6.21. *Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$. Let $\phi : E \to \widetilde{E}$ be a non-zero isogeny over $\Bbbk$ of degree m. Then there is a non-zero isogeny $\widehat{\phi} : \widetilde{E} \to E$ over $\Bbbk$ such that*

$$\widehat{\phi} \circ \phi = [m] : E \to E.$$

Indeed, $\widehat{\phi}$ is unique (see Exercise 9.6.22).

Proof: Let $\alpha_1 : E(\Bbbk) \to \mathrm{Pic}^0_{\Bbbk}(E)$ be the canonical map $P \mapsto (P) - (\mathcal{O}_E)$ and similarly for $\alpha_2 : \widetilde{E} \to \mathrm{Pic}^0_{\Bbbk}(\widetilde{E})$. We have $\widehat{\phi} = \alpha_1^{-1} \circ \phi^* \circ \alpha_2$ as above. We refer to Theorem III.6.1 of [564] (or Section 21.1 of [626] for elliptic curves over $\mathbb{C}$) for the details. □

Exercise 9.6.22. Suppose as in Theorem 9.6.21 that $\phi : E \to \widetilde{E}$ is a non-zero isogeny over $\Bbbk$ of degree m. Show that if $\psi : \widetilde{E} \to E$ is any isogeny such that $\psi \circ \phi = [m]$ then $\psi = \widehat{\phi}$.

Definition 9.6.23. Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$ and let $\phi : E \to \widetilde{E}$ be a non-zero isogeny over $\Bbbk$. The isogeny $\widehat{\phi} : \widetilde{E} \to E$ of Theorem 9.6.21 is called the **dual isogeny**.

Example 9.6.24. Let E be an elliptic curve over $\mathbb{F}_q$ and $\pi_q : E \to E$ the q-power Frobenius map. The dual isogeny $\widehat{\pi_q}$ is called the **Verschiebung**. Since $\widehat{\pi_q} \circ \pi_q = [q]$ it follows that $\widehat{\pi_q}(x, y) = [q](x^{1/q}, y^{1/q})$. Example 9.10.2 gives another way to write the Verschiebung.

Exercise 9.6.25. Let $E : y^2 = x^3 + a_6$ over $\Bbbk$ with $\mathrm{char}(\Bbbk) \neq 2, 3$. Let $\zeta_3 \in \overline{\Bbbk}$ be such that $\zeta_3^2 + \zeta_3 + 1 = 0$ and define the isogeny $\rho(\mathcal{O}_E) = \mathcal{O}_E$ and $\rho(x, y) = (\zeta_3 x, y)$. Show that $\widehat{\rho} = \rho^2$ (where ρ^2 means $\rho \circ \rho$).

Exercise 9.6.26. Recall E, $\widetilde{E}$ and ϕ from Example 9.6.9. Show that $\widehat{\phi} : \widetilde{E} \to E$ is given by

$$\widehat{\phi}(X, Y) = \left(\frac{Y^2}{4X^2}, \frac{Y(D - X^2)}{8X^2} \right)$$

and that $\widehat{\phi} \circ \phi(x, y) = [2](x, y)$.

We list some properties of the dual isogeny.

Theorem 9.6.27. *Let $\phi : E \to \widetilde{E}$ be a non-zero isogeny of elliptic curves over $\Bbbk$.*

1. *Let $d = \deg(\phi)$. Then $\deg(\widehat{\phi}) = d$, $\widehat{\phi} \circ \phi = [d]$ on E and $\phi \circ \widehat{\phi} = [d]$ on $\widetilde{E}$.*
2. *Let $\psi : \widetilde{E} \to E_3$ be an isogeny. Then $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}$.*
3. *Let $\psi : E \to \widetilde{E}$ be an isogeny. Then $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.*
4. *$\widehat{\widehat{\phi}} = \phi$.*

Proof: See Theorem III.6.2 of [564]. □

Corollary 9.6.28. *Let E be an elliptic curve over $\Bbbk$ and let $m \in \mathbb{Z}$. Then $\widehat{[m]} = [m]$ and $\deg([m]) = m^2$.*

Proof: The first claim follows by induction from part 3 of Theorem 9.6.27. The second claim follows from part 1 of Theorem 9.6.27 and since $\widehat{[1]} = [1]$: write $d = \deg([m])$ and use $[d] = \widehat{[m]}[m] = [m^2]$; since $\mathrm{End}_{\Bbbk}(E)$ is torsion-free (Lemma 9.6.11) it follows that $d = m^2$. □

An important consequence of Corollary 9.6.28 is that it determines the possible group structures of elliptic curves over finite fields. We return to this topic in Theorem 9.8.2.

We end this section with another example of an isogeny.

Exercise 9.6.29. Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2, 3$. Let E be an elliptic curve over $\Bbbk$ with a subgroup of order 3 defined over $\Bbbk$. Show that, after a suitable change of variable, one has a point $P = (0, v)$ such that $[2]P = (0, -v)$ and $v^2 \in \Bbbk$. Show that E is $\Bbbk$-isomorphic to a curve of the form

$$y^2 = x^3 + \tfrac{1}{a_6}\left(\tfrac{a_4}{2}x + a_6\right)^2$$

Show that there is a $\overline{\Bbbk}$-isomorphism to a curve of the form

$$Y^2 = X^3 + A(X+1)^2$$

where $A \neq 0, \frac{27}{4}$.

Exercise 9.6.30. (Doche, Icart and Kohel [183]) Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2, 3$. Let $u \in \Bbbk$ be such that $u \neq 0, \frac{9}{4}$. Consider the elliptic curve $E : y^2 = x^3 + 3u(x+1)^2$ as in Exercise 9.6.29. Then $(0, \sqrt{3u})$ has order 3 and $G = \{\mathcal{O}_E, (0, \pm\sqrt{3u})\}$ is a $\Bbbk$-rational subgroup of $E(\overline{\Bbbk})$. Show that

$$\phi(x, y) = \left(\frac{x^3 + 4ux^2 + 12u(x+1)}{x^2}, y\left(1 - 12u\frac{x+2}{x^3}\right)\right)$$

is an isogeny from E to $\widetilde{E} : Y^2 = X^3 - u(3X - 4u + 9)^2$ with $\ker(\phi) = G$. Determine the dual isogeny to ϕ and show that $\widehat{\phi} \circ \phi = [3]$.

Exercise 9.6.31. Let $\phi_1, \phi_2 : E \to E'$ be isogenies of degree d such that $\ker(\widehat{\phi_1}) = \ker(\widehat{\phi_2})$. Show that there exists $\lambda \in \mathrm{Aut}(E)$ such that $\phi_2 = \phi_1 \circ \lambda$.

[Hint: Use Exercise 9.6.20.]

9.7 The Invariant Differential

Let E over $\Bbbk$ be an elliptic curve. Recall the differential

$$\omega_E = \frac{dx}{2y + a_1x + a_3} \tag{9.10}$$

on the Weierstrass equation for E, which was studied in Example 8.5.32. We showed that the divisor of ω_E is 0. Let $Q \in E(\Bbbk)$ and τ_Q be the translation map. Then $\tau_Q^*(\omega_E) \in \Omega_{\Bbbk}(E)$ and so, by Theorem 8.5.21, $\tau_Q^*(\omega_E) = f\omega_E$ for some $f \in \Bbbk(E)$. Lemma 8.5.36 implies $\tau_Q^*(\mathrm{div}(\omega_E)) = 0$ and so $\mathrm{div}(f) = 0$. It follows that $\tau_Q^*(\omega_E) = c\omega_E$ for some $c \in \Bbbk^*$. The following result shows that $c = 1$ and so ω_E is fixed by translation maps. This explains why ω_E is called the **invariant differential**.

Theorem 9.7.1. *Let E be an elliptic curve in Weierstrass form and let ω_E be the differential in equation (9.10). Then $\tau_Q^*(\omega_E) = \omega_E$ for all $Q \in E(\overline{\Bbbk})$.*

Proof: See Proposition III.5.1 of [564]. □

An important fact is that the action of isogenies on differentials is linear.

Theorem 9.7.2. *Let $E, \widetilde{E}$ be elliptic curves over $\Bbbk$ and $\omega_{\widetilde{E}}$ the invariant differential on $\widetilde{E}$. Suppose $\phi, \psi : E \to \widetilde{E}$ are isogenies. Then*

$$(\phi + \psi)^*(\omega_{\widetilde{E}}) = \phi^*(\omega_{\widetilde{E}}) + \psi^*(\omega_{\widetilde{E}}).$$

Proof: See Theorem III.5.2 of [564]. □

A crucial application is to determine when certain isogenies are separable. In particular, if E is an elliptic curve over $\mathbb{F}_{p^n}$ then $[p]$ is inseparable on E while $\pi_{p^n} - 1$ is separable (where π_{p^n} is the p^n-power Frobenius).

Corollary 9.7.3. *Let E be an elliptic curve over $\Bbbk$. Let $m \in \mathbb{Z}$. Then $[m]$ is separable if and only if m is coprime to the characteristic of $\Bbbk$. Let $\Bbbk = \mathbb{F}_q$ and π_q be the q-power Frobenius. Let $m, n \in \mathbb{Z}$. Then $m + n\pi_q$ is separable if and only if m is coprime to q.*

Proof: (Sketch) Theorem 9.7.2 implies $[m]^*(\omega_E) = m\omega_E$. So $[m]^*$ maps $\Omega_{\Bbbk}(E)$ to $\{0\}$ if and only if the characteristic of $\Bbbk$ divides m. The first part then follows from Lemma 8.5.35. The second part follows by the same argument, using the fact that π_q is inseparable and so $\pi_q^*(\omega_E) = 0$. For full details see Corollaries III.5.3 to III.5.5 of [564]. □

This result has the following important consequence.

Theorem 9.7.4. *Let E and $\widetilde{E}$ be elliptic curves over a finite field $\mathbb{F}_q$. If $\phi : E \to \widetilde{E}$ is an isogeny over $\mathbb{F}_q$ then $\#E(\mathbb{F}_q) = \#\widetilde{E}(\mathbb{F}_q)$.*

Proof: Let π_q be the q-power Frobenius map on E. For $P \in E(\overline{\mathbb{F}}_q)$ we have $\pi_q(P) = P$ if and only if $P \in E(\mathbb{F}_q)$. Hence, $E(\mathbb{F}_q) = \ker(\pi_q - 1)$. Since $\pi_q - 1$ is separable it follows that $\#E(\mathbb{F}_q) = \deg(\pi_q - 1)$. Since $\pi_q - 1$ is separable it follows that $\#E(\mathbb{F}_q) = \deg(\pi_q - 1)$.

Now, returning to the problem of the Theorem, write π_q and $\widehat{\pi}_q$ for the q-power Frobenius maps on E and $\widetilde{E}$ respectively. Since ϕ is defined over $\mathbb{F}_q$ it follows that $\widehat{\pi}_q \circ \phi = \phi \circ \pi_q$. Hence, $(\widehat{\pi}_q - 1) \circ \phi = \phi \circ (\pi_q - 1)$ and so (applying Exercise 8.1.12 twice) $\deg(\widehat{\pi}_q - 1) = \deg(\pi_q - 1)$. The result follows since $\#E(\mathbb{F}_q) = \deg(\pi_q - 1)$ and $\#\widetilde{E}(\mathbb{F}_q) = \deg(\widehat{\pi}_q - 1)$. □

The converse (namely, if E and $\widetilde{E}$ are elliptic curves over $\mathbb{F}_q$ and $\#E(\mathbb{F}_q) = \#\widetilde{E}(\mathbb{F}_q)$ then there is an isogeny from E to $\widetilde{E}$ over $\mathbb{F}_q$) is Tate's isogeny theorem [601]. This can be proved for elliptic curves using the theory of complex multiplication (see Remark 25.3.10).

We now give a refinement of Lemma 9.6.12. This result shows that a separable isogeny is determined by $\phi_1(x)$ when $\mathrm{char}(\Bbbk) \neq 2$.

Theorem 9.7.5. *Let the notation be as in Lemma 9.6.12. Let $\phi : E \to \widetilde{E}$ be a separable isogeny over $\Bbbk$. Then ϕ may be expressed by a rational function in the form*

$$\phi(x, y) = (\phi_1(x), cy\phi_1(x)' + \phi_3(x))$$

where $\phi_1(x)' = d\phi_1(x)/dx$ is the (formal) derivative of the rational function $\phi_1(x)$, where $c \in \overline{\Bbbk}^*$ is a non-zero constant, and where

$$2\phi_3(x) = -\widetilde{a}_1\phi_1(x) - \widetilde{a}_3 + c(a_1x + a_3)\phi_1(x)'.$$

Proof: Let $\omega_E = dx/(2y + a_1x + a_3)$ be the invariant differential on E and $\omega_{\widetilde{E}} = dX/(2Y + \widetilde{a}_1X + \widetilde{a}_3)$ be the invariant differential on $\widetilde{E}$. Since ϕ is separable, then $\phi^*(\omega_{\widetilde{E}})$ is non-zero. Furthermore, since ϕ is unramified, Lemma 8.5.36 implies that $\mathrm{div}(\phi^*(\omega_{\widetilde{E}})) = \phi^*(\mathrm{div}(\omega_{\widetilde{E}})) = 0$. Hence, $\phi^*(\omega_{\widetilde{E}})$ is a multiple of ω_E and so

$$dx/(2y + a_1x + a_3) = c\phi^*(dX/(2Y + \widetilde{a}_1X + \widetilde{a}_3)).$$

for some non-zero constant $c \in \overline{\Bbbk}$.

By Lemma 9.6.12, $X = \phi_1(x)$, $Y = y\phi_2(x) + \phi_3(x)$ and

$$2\phi_3(x) = -\widetilde{a}_1\phi_1(x) - \widetilde{a}_3 + (a_1x + a_3)\phi_2(x).$$

Now, since $dX/dx = \phi_1(x)'$,

$$\phi^*(dX/(2Y + \widetilde{a}_1 X + \widetilde{a}_3)) = \phi_1(x)' dx/(2(y\phi_2(x) + \phi_3(x)) + \widetilde{a}_1\phi_1(x) + \widetilde{a}_3).$$

Hence, substituting for $\phi_3(x)$,

$$\begin{aligned} \phi^*(dX/(2Y + \widetilde{a}_1 X + \widetilde{a}_3)) &= \phi_1(x)' dx/((2y + a_1 x + a_3)\phi_2(x)) \\ &= (\phi_1(x)'/\phi_2(x))dx/(2y + a_1 x + a_3). \end{aligned}$$

It follows that $\phi_2(x) = c\phi_1(x)'$ for some $c \in \overline{\Bbbk}^*$, which proves the result. □

In Section 25.1.1 we will make use of Theorem 9.7.5 in the case $c = 1$.

Exercise 9.7.6. Let the notation be as in Theorem 9.7.5 and suppose $\mathrm{char}(\Bbbk) = 2$. Show that there are only two possible values for the rational function $\phi_3(x)$.

9.8 Multiplication by n and Division Polynomials

Corollary 9.6.28 showed the fundamental fact that $\deg([m]) = m^2$ and so there are at most m^2 points of order dividing m on an elliptic curve. There are several other explanations for this fact. One explanation is to consider elliptic curves over $\mathbb{C}$: as a Riemann surface they are a complex torus $\mathbb{C}/L$ where L is a rank 2 lattice (see Chapter 5 of Silverman [564], especially Proposition 5.4) and it follows that there are m^2 points of order m (this argument generalises immediately to Abelian varieties).

Another reason for this fact is because the group law is given by rational functions whose denominators are essentially quadratic polynomials in each variable. For comparison, see Exercise 9.8.1 which shows that a group law given by linear polynomials only has m points of order m.

Exercise 9.8.1. Consider the multiplicative group $\mathbb{G}_m(\Bbbk) = \Bbbk^*$. The group operation $(x_1, x_2) \mapsto x_1 x_2$ is linear in each of x_1 and x_2. The elements of order m are the roots of the polynomial $x^m - 1$. Show that there are m points of order m if $\gcd(m, \mathrm{char}(\Bbbk)) = 1$, and if $p = \mathrm{char}(\Bbbk)$ then there is 1 point of order p.

It follows from Corollary 9.6.28 that $\#E[m] \leq m^2$, and elementary group theory implies $\#E[m]$ is therefore a divisor of m^2. Theorem 9.8.2 follows. A more precise version of this result is Theorem 9.10.13.

Theorem 9.8.2. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then $E(\mathbb{F}_q)$ is isomorphic as a group to a product of cyclic groups of order n_1 and n_2 such that $n_1 \mid n_2$.*

Proof: (Sketch) Since $E(\mathbb{F}_q)$ is a finite Abelian group we apply the classification of finite Abelian groups (e.g., Theorem II.2.1 of [301]). Then use the fact that there are at most m^2 points in $E(\mathbb{F}_q)$ of order m for every $m \in \mathbb{N}$. □

Since $\#E[m] \leq m^2$ (and, by Corollary 9.7.3, is equal to m^2 when m is coprime to the characteristic) it is natural to seek polynomials whose roots give the (affine) points of order dividing m. We already saw such polynomials in Exercise 9.6.10 for the case $m = 2$ (and this gave an alternative proof that, in general, there are three points (x, y) over $\overline{\Bbbk}$ of order 2 on an elliptic curve; namely the points $(x, 0)$ where x is a root of the polynomial in equation (9.9)). Since $[m]P = \mathcal{O}_E$ if and only if $[m](-P) = \mathcal{O}_E$ one might expect to use polynomials in $\Bbbk[x]$, but when m is even it turns out to be more convenient to have polynomials that feature the variable y (one reason being that this leads to polynomials of lower degree). When m is odd the polynomials will be univariate and of degree $(m^2-1)/2$ as expected. We now determine these polynomials, first for the cases $m = 3$ and $m = 4$.

Exercise 9.8.3. Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$ (with $\mathrm{char}(\Bbbk) \neq 2$). Show that if $\mathrm{char}(\Bbbk) = 3$, $a_2 = 0$ and $a_4 \neq 0$ then there is no point (x, y) of order 3. Show that if $\mathrm{char}(\Bbbk) = 3$ and $a_2 \neq 0$ then (x, y) has order 3 if and only if $x^3 = a_6 - a_4^2/(4a_2)$. Hence if $\mathrm{char}(\Bbbk) = 3$ then $\#E[3] \in \{1, 3\}$.

Show that if $\mathrm{char}(\Bbbk) \neq 3$ then (x, y) has order 3 if and only if

$$3x^4 + 4a_2x^3 + 6a_4x^2 + 12a_6x + (4a_2a_6 - a_4^2) = 0.$$

Exercise 9.8.4. Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve over $\Bbbk$ with $\mathrm{char}(\Bbbk) \neq 2$. Show that if $P = (x, y) \in E(\overline{\Bbbk})$ satisfies $P \in E[4]$ and $P \notin E[2]$ then $[2]P$ is of the form $(x_2, 0)$ for some $x_2 \in \Bbbk$. Hence show that x satisfies

$$x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - (a_4^3 + 8a_6^2).$$

We now state the polynomials whose roots give affine points of order dividing m for the case of elliptic curves in short Weierstrass form. The corresponding polynomials for elliptic curves over fields of characteristic 2 are given in Section 4.4.5.a of [16] and Section III.4.2 of [65]. Division polynomials for elliptic curves in general Weierstrass form are discussed in Section III.4 of [65].

Definition 9.8.5. Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve over $\Bbbk$ with $\mathrm{char}(\Bbbk) \neq 2$. The **division polynomials** are defined by

$$\begin{aligned}
\psi_1(x, y) &= 1 \\
\psi_2(x, y) &= 2y \\
\psi_3(x, y) &= 3x^4 + 6a_4x^2 + 12a_6x - a_4^2 \\
\psi_4(x, y) &= 4y(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - (a_4^3 + 8a_6^2)) \\
\psi_{2m+1}(x, y) &= \psi_{m+2}(x, y)\psi_m(x, y)^3 - \psi_{m-1}(x, y)\psi_{m+1}(x, y)^3 \ , \quad (m \geq 2) \\
\psi_{2m}(x, y) &= \tfrac{1}{2y}\psi_m(x, y)(\psi_{m+2}(x, y), \psi_{m-1}(x, y)^2 - \psi_{m-2}(x, y)\psi_{m+1}(x, y)^2) \ , \quad (m \geq 3).
\end{aligned}$$

Lemma 9.8.6. *Let E be an elliptic curve in short Weierstrass form over $\Bbbk$ with* $\mathrm{char}(\Bbbk) \neq 2$. *Let $m \in \mathbb{N}$. Then $\psi_m(x, y) \in \Bbbk[x, y]$. If m is odd then $\psi_m(x, y)$ is a polynomial in x only and $\psi_m(x, y) = mx^{(m^2-1)/2} + \cdots \in \Bbbk[x]$. If m is even then $\psi_m(x, y) = yh(x)$ where $h(x) = mx^{(m^2-4)/2} + \cdots \in \Bbbk[x]$.*

Proof: The cases $m = 2, 3$ and 4 are clear by inspection. The rest are easily proved by induction. □

Theorem 9.8.7. *Let E be an elliptic curve in short Weierstrass form over $\Bbbk$ with* $\mathrm{char}(\Bbbk) \neq 2, 3$. *Let $m \in \mathbb{N}$ and $\psi_m(x, y)$ as above. Then $P = (x_P, y_P) \in E(\overline{\Bbbk})$ satisfies $[m]P = \mathcal{O}_E$ if and only if $\psi_m(x_P, y_P) = 0$. Furthermore, there are polynomials $A_m(x) \in \Bbbk[x]$ and $B_m(x, y) \in \Bbbk[x, y]$ such that*

$$[m](x, y) = \left(\frac{A_m(x)}{\psi_m(x, y)^2}, \frac{B_m(x, y)}{\psi_m(x, y)^3} \right).$$

Proof: The first claim has already been proved for $m = 3$ and $m = 4$ in Exercises 9.8.3 and 9.8.4. The general result can be proved in various ways: Section 9.5 of Washington [626] gives a proof for elliptic curves over $\mathbb{C}$ and then deduces the result for general fields of characteristic not equal to 2, Charlap and Robbins [127] give a proof (Sections 7 to 9) using considerations about divisors and functions, other sources (such as Exercise 3.7 of [564]) suggest a (tedious) verification by induction. □

9.9 Endomorphism Structure

The aim of this section is to discuss the structure of the ring $\mathrm{End}_{\Bbbk}(E)$. Note that $\mathbb{Z} \subseteq \mathrm{End}_{\Bbbk}(E)$ and that, by Lemma 9.6.11, $\mathrm{End}_{\Bbbk}(E)$ is a torsion-free $\mathbb{Z}$-module. For an isogeny $\phi : E \to E$ and an integer $m \in \mathbb{Z}$ we write $m\phi$ for the isogeny $[m] \circ \phi$.

To understand the endomorphism rings of elliptic curves one introduces the **Tate module** $T_l(E)$. This is defined, for any prime $l \neq \mathrm{char}(\Bbbk)$, to be the inverse limit of the groups $E[l^i]$ (this is the same process as used to construct the p-adic ($= l$-adic) numbers $\mathbb{Z}_l$ as the inverse limit of the rings $\mathbb{Z}/l^i\mathbb{Z}$). More precisely, for each $i \in \mathbb{N}$ fix a pair $\{P_{i,1}, P_{i,2}\}$ of generators for $E[l^i]$ such that $P_{i-1,j} = [l]P_{i,j}$ for $i > 1$ and $j \in \{1, 2\}$. Via this basis we can identify $E[l^i]$ with $(\mathbb{Z}/l^i\mathbb{Z})^2$. Indeed, this is an isomorphism of $(\mathbb{Z}/l^i\mathbb{Z})$-modules. It follows that $T_l(E)$ is a $\mathbb{Z}_l$-module that is isomorphic to $\mathbb{Z}_l^2$ as a $\mathbb{Z}_l$-module. Hence, the set $\mathrm{End}_{\mathbb{Z}_l}(T_l(E))$ of $\mathbb{Z}_l$-linear maps from $T_l(E)$ to itself is isomorphic as a $\mathbb{Z}_l$-module to $M_2(\mathbb{Z}_l)$. We refer to Section III.7 of Silverman [564] for the details.

An isogeny $\phi : E \to \widetilde{E}$ gives rise to a linear map from $E[l^i]$ to $\widetilde{E}[l^i]$ for each i. Writing $\phi(P_{i,1}) = [a]\widetilde{P}_{i,1} + [b]\widetilde{P}_{i,2}$ and $\phi(P_{i,2}) = [c]\widetilde{P}_{i,1} + [d]\widetilde{P}_{i,2}$ (where $\{\widetilde{P}_{i,1}, \widetilde{P}_{i,2}\}$ is a basis for $\widetilde{E}[l^i]$) we can represent ϕ as a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}/l^i\mathbb{Z})$. It follows that ϕ corresponds to an element $\phi_l \in M_2(\mathbb{Z}_l)$.

Write $\mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$ for the set of $\mathbb{Z}_l$-module homomorphisms from $T_l(E_1)$ to $T_l(E_2)$. Since $T_l(E)$ is isomorphic to $M_2(\mathbb{Z}_l)$ it follows that $\mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$ is a $\mathbb{Z}_l$-module of rank 4. An important result is that

$$\mathrm{Hom}_{\Bbbk}(E_1, E_2) \otimes \mathbb{Z}_l \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$$

is injective (Theorem III.7.4 of [564]). It follows that $\mathrm{Hom}_{\Bbbk}(E_1, E_2)$ is a $\mathbb{Z}$-module of rank at most 4.

The map $\phi \mapsto \widehat{\phi}$ is an involution in $\mathrm{End}_{\Bbbk}(E)$ and $\phi \circ \widehat{\phi} = [d]$ where $d > 0$. This constrains what sort of ring $\mathrm{End}_{\Bbbk}(E)$ can be (Silverman [564] Theorem III.9.3). The result is as follows (for the definitions of orders in quadratic fields see Section A.12 and for quaternion algebras see Vignéras [622]).

Theorem 9.9.1. *Let E be an elliptic curve over a field $\Bbbk$. Then $\mathrm{End}_{\Bbbk}(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a definite quaternion algebra.*

Proof: See Corollary III.9.4 of [564]. □

When $\Bbbk$ is a finite field then the case $\mathrm{End}_{\overline{\Bbbk}}(E) = \mathbb{Z}$ is impossible (see Theorem V.3.1 of [564]).

Example 9.9.2. Let $E : y^2 = x^3 + x$ over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$ is prime. Then $\xi(x, y) = (-x, iy)$ is an isogeny where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. One can verify that $\xi^2 = \xi \circ \xi = [-1]$. One can show that $\#E(\mathbb{F}_p) = p + 1$ (Exercise 9.10.5) and then Theorem 9.10.3 implies that the Frobenius map $\pi_p(x, y) = (x^p, y^p)$ satisfies $\pi_p^2 = [-p]$. Finally, we have $\xi \circ \pi_p(x, y) = (-x^p, iy^p) = -\pi_p \circ \xi(x, y)$. Hence, $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is not a commutative ring. Indeed, it is isomorphic to a subring of the quaternion algebra (be warned that we are recycling the symbol i here) $\mathbb{Q}[i, j]$ with $i^2 = -1, j^2 = -p, ij = -ji$. Note that $\mathrm{End}_{\mathbb{F}_p}(E)$ is isomorphic to an order, containing $\mathbb{Z}[\sqrt{-p}]$, in the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Every endomorphism on an elliptic curve satisfies a quadratic characteristic polynomial with integer coefficients.

Theorem 9.9.3. *Let E be an elliptic curve over $\mathbb{k}$ and $\phi \in \mathrm{End}_{\mathbb{k}}(E)$ be a non-zero isogeny. Let $d = \deg(\phi)$. Then there is an integer t such that $\phi^2 - t\phi + d = 0$ in $\mathrm{End}_{\mathbb{k}}(E)$. In other words, for all $P \in E(\overline{\mathbb{k}})$,*

$$\phi(\phi(P)) - [t]\phi(P) + [d]P = \mathcal{O}_E.$$

Proof: (Sketch) Choose an auxiliary prime $l \neq \mathrm{char}(\mathbb{k})$. Then ϕ acts on the Tate module $T_l(E)$ and so corresponds to a matrix $M \in \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E), T_l(E))$. Such a matrix has a determinant d and a trace t. The trick is to show that $d = \deg(\phi)$ and $t = 1 + \deg(\phi) - \deg(1 - \phi)$ (which are standard facts for 2×2 matrices when deg is replaced by det). These statements are independent of l. Proposition V.2.3 of Silverman [564] gives the details (this proof uses the Weil pairing). A slightly simpler proof is given in Lemma 24.4 of [122]. □

Definition 9.9.4. The integer t in Theorem 9.9.3 is called the **trace** of the endomorphism.

Exercise 9.9.5. Show that if $\phi \in \mathrm{End}_{\mathbb{k}}(E)$ satisfies the equation $T^2 - tT + d = 0$ then so does $\widehat{\phi}$.

Lemma 9.9.6. *Suppose $\phi \in \mathrm{End}_{\overline{\mathbb{k}}}(E)$ has characteristic polynomial $P(T) = T^2 - tT + d \in \mathbb{Z}[T]$. Let $\alpha, \beta \in \mathbb{C}$ be the roots of $P(T)$. Then, for $n \in \mathbb{N}$, ϕ^n satisfies the polynomial $(T - \alpha^n)(T - \beta^n) \in \mathbb{Z}[T]$.*

Proof: This is a standard result: let M be a matrix representing ϕ (or at least, representing the action of ϕ on the Tate module for some l) in Jordan form $M = \left(\begin{smallmatrix} \alpha & \gamma \\ 0 & \beta \end{smallmatrix}\right)$. Then M^n has Jordan form $\left(\begin{smallmatrix} \alpha^n & * \\ 0 & \beta^n \end{smallmatrix}\right)$ and the result follows by the previous statements. □

9.10 Frobenius map

We have seen that the q-power Frobenius on an elliptic curve over $\mathbb{F}_q$ is a non-zero isogeny of degree q (Corollary 9.6.15) and that isogenies on elliptic curves satisfy a quadratic characteristic polynomial. Hence there is an integer t such that

$$\pi_q^2 - t\pi_q + q = 0. \tag{9.11}$$

Definition 9.10.1. The integer t in equation (9.11) is called the **trace of Frobenius**. The polynomial $P(T) = T^2 - tT + q$ is the **characteristic polynomial of Frobenius**.

Note that $\mathrm{End}_{\mathbb{F}_q}(E)$ always contains the order $\mathbb{Z}[\pi_q]$, which is an order of discriminant $t^2 - 4q$.

Example 9.10.2. Equation (9.11) implies

$$([t] - \pi_q) \circ \pi_q = [q]$$

and so we have $\widehat{\pi_q} = [t] - \pi_q$.

Theorem 9.10.3. *Let E be an elliptic curve over $\mathbb{F}_q$ and let $P(T)$ be the characteristic polynomial of Frobenius. Then $\#E(\mathbb{F}_q) = P(1)$.*

Proof: We have $E(\mathbb{F}_q) = \ker(\pi_q - 1)$ and, since $\pi_q - 1$ is separable, $\#E(\mathbb{F}_q) = \deg(\pi_q - 1)$. Now, $P(1) = 1 + q - t$ where, as noted in the proof of Theorem 9.9.3, $t = 1 + \deg(\pi_q) - \deg(1 - \pi_q)$. □

Exercise 9.10.4. Let $p \equiv 2 \pmod 3$. Show that the elliptic curve $E : y^2 = x^3 + a_6$ for $a_6 \in \mathbb{F}_p^*$ has $p+1$ points over $\mathbb{F}_p$.
[Hint: re-arrange the equation.]

Exercise 9.10.5. Let $p \equiv 3 \pmod 4$ and $a_4 \in \mathbb{F}_p^*$. Show that $E : y^2 = x^3 + a_4 x$ over $\mathbb{F}_p$ has $\#E(\mathbb{F}_p) = p+1$.
[Hint: Write the right hand side as $x(x^2 + a_4)$ and use the fact that $(\frac{-1}{p}) = -1$.]

We now give an example where the Frobenius map, as an endomorphism, is the same as the map $[n]$ for some integer n.

Example 9.10.6. Let $p \equiv 3 \pmod 4$ be prime, let $g \in \mathbb{F}_{p^2}$ be a primitive root and $E : y^2 = x^3 + g^2 x$. Let $u = 1/\sqrt{g} \in \mathbb{F}_{p^4}$. Consider the map $\phi(x, y) = (u^2 x, u^3 y)$ that maps E to $\widetilde{E} : Y^2 = X^3 + (u^4 g^2)X = X^3 + X$. By Exercise 9.10.5, $\#\widetilde{E}(\mathbb{F}_p) = p+1$ and the p-power Frobenius map $\widetilde{\pi}_p$ on $\widetilde{E}$ satisfies $(\widetilde{\pi}_p)^2 = -p$.

Define $\psi \in \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ by $\psi = \phi^{-1} \circ \widetilde{\pi}_p \circ \phi$. Then $\psi(x, y) = (w_1 x^p, w_2 y^p)$ where $w_1 = u^{2p}/u^2$ and $w_2 = u^{3p}/u^3$. One can verify that $w_1, w_2 \in \mathbb{F}_{p^2}$ (just show that $w_i^{p^2} = w_i$) and that $w_1^{p+1} = 1$ and $w_2^{p+1} = -1$. Finally, one has $\psi(\psi(x, y)) = \psi(w_1 x^p, w_2 y^p) = (w_1^{p+1} x^{p^2}, w_2^{p+1} y^{p^2}) = (x^{p^2}, -y^{p^2}) = -\pi_{p^2}(x, y)$ on E. On the other hand, by definition

$$\psi^2 = \phi^{-1} \circ (\widetilde{\pi}_p)^2 \circ \phi = \phi^{-1} \circ [-p] \circ \phi = [-p]$$

on E. Hence we have shown that $\pi_{p^2} = [p]$ on E. The characteristic polynomial of π_{p^2} is therefore $(T-p)^2$ and so $\#E(\mathbb{F}_{p^2}) = p^2 - 2p + 1$.

As we will see in Section 9.11, this curve is supersingular and so $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is an order in a quaternion algebra. Since $\pi_{p^2} \in \mathbb{Z}$ in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ the quaternion algebra structure comes from other endomorphisms. We already met $\psi \in \mathrm{End}_{\mathbb{F}_{p^2}}(E)$ such that $\psi^2 = -p$. The endomorphism ring also contains the map $\xi(x, y) = (-x, iy)$ where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. One can verify that $\xi^2 = -1$ and $\xi\psi = -\psi\xi$ (since $i^p = -i$ as $p \equiv 3 \pmod 4$); as was seen already in Example 9.9.2.

Theorem 9.10.7. *(Hasse) Let E be an elliptic curve over $\mathbb{F}_q$ and denote by t the trace of the q-power Frobenius map. Then $|t| \leq 2\sqrt{q}$.*

Proof: (Sketch) The idea is to use the fact that $\deg : \mathrm{End}(E) \to \mathbb{Z}$ is a positive definite quadratic form. See Theorem V.1.1 of [564], Theorem 4.2 of [626], Theorem 1 of Chapter 25 of [122] or Theorem 13.4 of [127]. □

In other words, the number of points on an elliptic curve over $\mathbb{F}_q$ lies in the **Hasse interval** $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$.

Corollary 9.10.8. *Let E be an elliptic curve over $\mathbb{F}_q$ and let $P(T)$ be the characteristic polynomial of Frobenius. Let $\alpha, \beta \in \mathbb{C}$ be such that $P(T) = (T - \alpha)(T - \beta)$. Then $\beta = q/\alpha = \overline{\alpha}$ and $|\alpha| = |\beta| = \sqrt{q}$.*

Proof: It follows from the proof of Theorem 9.10.7 that if $P(T) \in \mathbb{Z}[T]$ has a real root then it is a repeated root (otherwise, the quadratic form is not positive definite). Obviously, if the root α is not real then $\beta = \overline{\alpha}$. Since the constant coefficient of $P(T)$ is q it follows that $q = \alpha\beta = \alpha\overline{\alpha} = |\alpha|^2$ and similarly for β. □

The case of repeated roots of $P(T)$ only happens when $\alpha = \pm\sqrt{q} \in \mathbb{Z}$ and $P(T) = (T \pm \sqrt{q})^2$. The condition $|\alpha| = |\beta| = \sqrt{q}$ is known as the **Riemann hypothesis for elliptic curves**. This concept has been generalised to general varieties over finite fields as part of the Weil conjectures (proved by Deligne).

Corollary 9.10.9. *Let E be an elliptic curve over $\mathbb{F}_q$ and let $P(T) = (T-\alpha)(T-\beta)$ be the characteristic polynomial of Frobenius. Let $n \in \mathbb{N}$. Then $\#E(\mathbb{F}_{q^n}) = (1-\alpha^n)(1-\beta^n)$.*

Proof: We have $E(\mathbb{F}_{q^n}) = \ker(\pi_{q^n} - 1) = \ker(\pi_q^n - 1)$. The result follows from Lemma 9.9.6. □

Corollary 9.10.9 shows that for practical calculations we can identify the isogeny π_q with a complex number α that is one of the roots of $P(T)$. The name "complex multiplication" for endomorphisms of elliptic curves that are not in $\mathbb{Z}$ comes from this identification. When working with elliptic curves over $\mathbb{C}$ the analogy is even stronger, see Theorem 5.5 of [564].

Exercise 9.10.10. Let E be an elliptic curve over $\mathbb{F}_q$. Write $\#E(\mathbb{F}_{q^n}) = q^n - t_n + 1$ for $n \in \mathbb{N}$. Show that for $i, j \in \mathbb{N}$ with $i < j$ we have $t_i t_j = t_{i+j} + q^i t_{j-i}$. Some special cases are

$$t_{2n} = t_n^2 - 2q^n \ , \quad t_{n+1} = t_n t_1 - q t_{n-1}.$$

Hence give an algorithm to efficiently compute t_n for any value n, given q and t_1.

Exercise 9.10.11. Let $E_a : y^2 + xy = x^3 + ax^2 + 1$ over $\mathbb{F}_2$ where $a \in \{0, 1\}$. Show that $\#E_a(\mathbb{F}_2) = 2 + (-1)^a + 1$ so $P(T) = T^2 + (-1)^a T + 2$. These curves are called **Koblitz curves** (Koblitz called them **anomalous binary curves**). Show that if n is composite then $\#E_a(\mathbb{F}_{2^n})$ is not of the form $2r$ or $4r$ where r is prime. Hence, find all $3 < n < 200$ such that $\#E_0(\mathbb{F}_{2^n}) = 2r$ or $\#E_1(\mathbb{F}_{2^n}) = 4r$ where r is prime.

We have seen that the number of points on an elliptic curve over a finite field lies in the Hasse interval. An important result of Waterhouse [627] specifies exactly which group orders arise.

Theorem 9.10.12. *(Waterhouse) Let $q = p^m$ where p is prime and let $t \in \mathbb{Z}$ be such that $|t| \leq 2\sqrt{q}$. Then there is an elliptic curve over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q - t + 1$ if and only if one of the following conditions holds:*

1. $\gcd(t, p) = 1$;
2. *m is even and $t = \pm 2\sqrt{q}$;*
3. *m is even, $p \not\equiv 1 \pmod 3$ and $t = \pm\sqrt{q}$;*
4. *m is odd, $p = 2, 3$ and $t = \pm p^{(m+1)/2}$;*
5. *Either m is odd or (m is even and $p \not\equiv 1 \pmod 4$) and $t = 0$.*

Proof: The proof given by Waterhouse relies on Honda-Tate theory; one shows that the above cases give precisely the polynomials $T^2 - tT + q$ with roots being Weil numbers. See Theorem 4.1 of [627]. □

In the cases $\gcd(t, p) \neq 1$ (i.e., $p \mid t$) the elliptic curve is said to be **supersingular**. This case is discussed further in Section 9.11.

We know from Theorem 9.8.2 that the group structure of an elliptic curve over a finite field $\mathbb{F}_q$ is of the form $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ for some integers n_1, n_2 such that $n_1 \mid n_2$. It follows from the Weil pairing (see Exercise 26.2.5 or Section 3.8 of [564]) that $n_1 \mid (q-1)$.

The following result gives the group structures of elliptic curves.[1]

[1] This result has been discovered by several authors. Schoof determined the group structures of supersingular elliptic curves in his thesis. The general statement was given by Tsfasman [610] in 1985, Rück [505] in 1987 and Voloch [623] in 1988.

Theorem 9.10.13. *Let $q = p^m$ where p is prime, let $t \in \mathbb{Z}$ be such that $|t| \leq 2\sqrt{q}$ and let $N = q - t + 1$ be a possible group order for an elliptic curve as in Theorem 9.10.12. Write $N = \prod_l l^{h_l}$ for the prime factorisation of N. Then the possible group structures of elliptic curves over $\mathbb{F}_q$ with N points are (i.e., only these cases are possible, and every case does arise for every q)*

$$\mathbb{Z}/p^{h_p}\mathbb{Z} \times \prod_{l \neq p} \left(\mathbb{Z}/l^{a_l}\mathbb{Z} \times \mathbb{Z}/l^{h_l - a_l}\mathbb{Z} \right)$$

where

1. *if $\gcd(t, p) = 1$ then $0 \leq a_l \leq \min\{v_l(q-1), \lfloor h_l/2 \rfloor\}$ where $v_l(q-1)$ denotes the integer b such that $l^b \| (q-1)$,*
2. *if $t = \pm 2\sqrt{q}$ then $a_l = h_l/2$ (i.e., the group is $(\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z})^2$),*
3. *if $t = \pm\sqrt{q}$ or $t = \pm p^{(m+1)/2}$ then the group is cyclic (i.e., all $a_l = 0$),*
4. *if $t = 0$ then either the group is cyclic (i.e., all $a_l = 0$) or is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/((q+1)/2)\mathbb{Z}$ (i.e., all $a_l = 0$ except $a_2 = 1$).*

Proof: See Voloch [623] or Theorem 3 of Rück [505] (note that it is necessary to prove that Rück's conditions imply those written above by considering possible divisors $d \mid (q-1)$ and $d \mid (q - t + 1)$ in the supersingular cases). □

Exercise 9.10.14. Let q be a prime power, $\gcd(t, q) = 1$, and $N = q + 1 - t$ a possible value for $\#E(\mathbb{F}_q)$. Show that there exists an elliptic curve over $\mathbb{F}_q$ with N points and which is cyclic as a group.

If E is an elliptic curve defined over $\mathbb{F}_q$ and ℓ is a prime such that $\gcd(\ell, q) = 1$, then π_q acts linearly on $E[\ell]$. Considering $E[\ell]$ as a 2-dimensional vector space over $\mathbb{F}_\ell$ we can represent π_q as a 2×2 matrix with entries in $\mathbb{F}_\ell$. Since $(\pi_q^2 - t\pi_q + q)(Q) = \mathcal{O}_E$ for all $Q \in E[\ell]$, it follows that the matrix satisfies the characteristic polynomial $P(T) \pmod{\ell}$. If $E[\ell]$ contains a cyclic subgroup $\langle Q \rangle$ defined over $\mathbb{F}_q$ then $\pi_q(Q) = [\lambda]Q$ for some $\lambda \in \mathbb{Z}$. Hence, $\mathcal{O}_E = (\pi_q^2 - t\pi_q + q)(Q) = [\lambda^2 - t\lambda + q]Q$ and so $P(\lambda) \equiv 0 \pmod{\ell}$. Conversely, if $P(T) \equiv (T - \lambda)(T - \mu) \pmod{\ell}$ then, for any $Q \in E[\ell]$ we have $(\pi_q - \lambda)(\pi_q - \mu)(Q) = \mathcal{O}_E$. Writing $Q' = \pi_q(Q) - [\mu]Q$ we have either $Q' = \mathcal{O}_E$ (in which case $\langle Q \rangle$ is a cyclic subgroup fixed by π_q), or $\pi_q(Q') - [\lambda]Q' = \mathcal{O}_E$ (in which case $\langle Q' \rangle$ is such a group).

Atkin classified the splitting of the ℓ-division polynomials in $\mathbb{F}_q[X]$ in terms of the Frobenius map and its characteristic polymomial modulo ℓ. We refer to Proposition 6.2 of Schoof [530] for the details.

Another useful result, which relates group structures and properties of the endomorphism ring, is Theorem 9.10.16. Exercise 9.10.15 shows that the final condition makes sense.

Exercise 9.10.15. Let E be an elliptic curve over $\mathbb{F}_q$ and let $t = q + 1 - \#E(\mathbb{F}_q)$. Show that if $n^2 \mid (q + 1 - t)$ and $n \mid (q - 1)$ then $n^2 \mid (t^2 - 4q)$.

Theorem 9.10.16. *Let p be a prime, $q = p^m$, E an elliptic curve over $\mathbb{F}_q$, and $t = q + 1 - \#E(\mathbb{F}_q)$. Let $n \in \mathbb{N}$ be such that $p \nmid n$. Then $E[n] \subseteq E(\mathbb{F}_q)$ if and only if $n^2 \mid (q + 1 - t)$, $n \mid (q - 1)$, and (either $t = \pm 2\sqrt{q}$ (equivalently, $\pi_q \in \mathbb{Z}$) or $\mathrm{End}_{\mathbb{F}_q}(E)$ contains the order of discriminant $(t^2 - 4q)/n^2$).*

Proof: If the kernel of $\pi_q - 1$ contains the kernel of $[n]$ then, by Theorem 9.6.18, there is an isogeny $\psi \in \mathrm{End}_{\mathbb{F}_q}(E)$ such that $\pi_q - 1 = \psi \circ [n]$. We write $\psi = (\pi_q - 1)/n$. The result follows easily; see Proposition 3.7 of Schoof [529] for the details. □

Exercise 9.10.17. Let E be an elliptic curve over $\mathbb{F}_q$ with[2] $\gcd(q,t)=1$, where $\#E(\mathbb{F}_q) = q+1-t$. Deduce from Theorem 9.10.16 that if $\mathrm{End}_{\overline{\mathbb{F}}_q}(E) = \mathbb{Z}[\pi_q]$ then $E(\mathbb{F}_q)$ is a cyclic group.

9.10.1 Complex Multiplication

A lot of information about the numbers of points on elliptic curves arises from the theory of complex multiplication. We do not have space to develop this theory in detail. Some crucial tools are the lifting and reduction theorems of Deuring (see Sections 13.4 and 13.5 of Lang [366] or Chapter 10 of Washington [626]). We summarise some of the most important ideas in the following theorem.

Theorem 9.10.18. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Then there is a number field L containing K (called the ring class field) and an elliptic curve E over L with $\mathrm{End}_{\overline{L}}(E) \cong \mathcal{O}$.*

Let p be a rational prime that splits completely in L, and let $\wp$ be a prime of $\mathcal{O}_L$ above p (so that $\mathcal{O}_L/\wp \cong \mathbb{F}_p$). If E has good reduction modulo $\wp$ (this holds if $\wp$ does not divide the discriminant of E), write $\overline{E}$ for the elliptic curve over $\mathbb{F}_p$ obtained as the reduction of E modulo $\wp$. Then $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \cong \mathcal{O}$ and there is an element $\pi \in \mathcal{O}$ such that $p = \pi\overline{\pi}$ (where the overline denotes complex conjugation). Furthermore,

$$\#\overline{E}(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}). \tag{9.12}$$

Conversely, every elliptic curve $\overline{E}$ over $\mathbb{F}_p$ such that $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \cong \mathcal{O}$ arises in this way as a reduction modulo $\wp$ of an elliptic curve over L.

Proof: This is Theorem 14.16 of Cox [157]; we refer to the books [157, 366] for much more information about complex multiplication and elliptic curves. □

Remark 9.10.19. An important consequence of the theory of complex multiplication is that the weighted number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with number of points equal to $q+1-t$ is the Hurwitz class number[3] $H(t^2-4q)$ (see Theorem 14.18 of Cox [157], Section 1.5 of Lenstra [377] or Schoof [529]). The Hurwitz class number is the sum of the (weighted) class numbers of the orders containing the order of discriminant t^2-4q (see the references mentioned or Section 5.3.2 of Cohen [136]).

These results imply that the number of elliptic curves over $\mathbb{F}_q$ with $q+1-t$ points is $O(u\log(u)\log(\log(u)))$, where $u = \sqrt{4q-t^2}$. The bound $h(-D) < \sqrt{D}\log(D)$ for fundamental discriminants is Exercise 5.27 of Cohen [136]; the case of general discriminants was discussed by Lenstra [377] and the best result is due to McKee [413].

Example 9.10.20. Let $p \equiv 1 \pmod 4$ be prime and let $a_4 \in \mathbb{Z}$ be such that $p \nmid a_4$. Let $E : y^2 = x^3 + a_4 x$ be an elliptic curve over $\mathbb{Q}$ and denote by $\overline{E}$ the elliptic curve over $\mathbb{F}_p$ obtained as the reduction of E modulo p. We will determine $\#\overline{E}(\mathbb{F}_p)$.

The curve E has the endomorphism $\psi(x,y) = (-x, iy)$ (where $i \in \overline{\mathbb{Q}}$ satisfies $i^2 = -1$) satisfying $\psi^2(x,y) = (x,-y) = [-1](x,y)$ and so $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ contains $\mathbb{Z}[\psi] \cong \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a maximal order it follows that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}[i]$.

Note that every prime $p \equiv 1 \pmod 4$ can be written as $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ (see Theorem 1.2 of Cox [157]). Note that there are eight choices for the pair (a,b) in $p = a^2+b^2$, namely $(\pm a, \pm b), (\pm b, \pm a)$ with all choices of sign independent (note that $a \neq b$ since p is odd).

[2] In fact, if $\gcd(q,t) \neq 1$ then the condition $\mathrm{End}_{\overline{\mathbb{F}}_q}(E) = \mathbb{Z}[\pi_q]$ never holds.

[3] Lenstra and Schoof call it the Kronecker class number.

In other words $p = (a+bi)(a-bi)$ where $i^2 = -1$. By Theorem 9.10.18 the reduction modulo p of E has $\#\overline{E}(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi})$ where $\pi\overline{\pi} = p$. Hence $\pi = a + bi$ for one of the pairs (a, b) and $\#\overline{E}(\mathbb{F}_p) = p + 1 - t$ where

$$t \in \{2a, -2a, 2b, -2b\}.$$

The correct value can usually be determined by testing whether $[p + 1 - t]P = \mathcal{O}_E$ for a random point $P \in E(\mathbb{F}_p)$. Section 4.4 of Washington [626] gives much more detail about this case.

In practice, one uses the Cornacchia algorithm to compute the integers a and b such that $p = a^2 + b^2$ and so it is efficient to compute $\#E(\mathbb{F}_p)$ for elliptic curves of the form $y^2 = x^3 + a_4 x$ for very large primes p. This idea can be extended to many other curves and is known as the **complex multiplication method** or **CM method**.

Exercise 9.10.21. Determine the number of points on $E : y^2 = x^3 + a_4 x$ modulo $p = 1429 = 23^2 + 30^2$ for $a_4 = 1, 2, 3, 4$.

Exercise 9.10.22. Let p be an odd prime such that $p \equiv 1 \pmod 3$. Then there exist integers a, b such that $p = a^2 + ab + b^2$ (see Chapter 1 of [157] and note that $p = x^2 + 3y^2$ implies $p = (x-y)^2 + (x-y)(2y) + (2y)^2$). Show that the number of points on $y^2 = x^3 + a_6$ over $\mathbb{F}_p$ is $p + 1 - t$ where

$$t \in \{\pm(2a + b), \pm(2b + a), \pm(b - a)\}.$$

Example 9.10.23. The six values $a_6 = 1, 2, 3, 4, 5, 6$ all give distinct values for $\#E(\mathbb{F}_7)$ for the curve $E : y^2 = x^3 + a_6$, namely $12, 9, 13, 3, 7, 4$ respectively.

9.10.2 Counting Points on Elliptic Curves

A computational problem of fundamental importance is to compute $\#E(\mathbb{F}_q)$ where E is an elliptic curve over a finite field $\mathbb{F}_q$. Due to lack of space we are unable to give a full treatment of this topic.

We know that $\#E(\mathbb{F}_q)$ lies in the Hasse interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$. In many cases, to determine $\#E(\mathbb{F}_q)$ it suffices to determine the order n of a random point $P \in E(\mathbb{F}_q)$. Determining all multiples of n that lie in the Hasse interval for a point in $E(\mathbb{F}_q)$ can be done using the baby-step-giant-step algorithm in $\tilde{O}(q^{1/4})$ bit operations (see Exercise 13.3.11). If there is only one multiple of n in the Hasse interval then we have determined $\#E(\mathbb{F}_q)$. This process will not determine $\#E(\mathbb{F}_q)$ uniquely if $n \leq 4\sqrt{q}$. Mestre suggested determining the order of points on both $E(\mathbb{F}_q)$ and its quadratic twist. This leads to a randomised algorithm to compute $\#E(\mathbb{F}_q)$ in $\tilde{O}(q^{1/4})$ bit operations. We refer to Section 3 of Schoof [530] for details.

A polynomial-time algorithm to compute $\#E(\mathbb{F}_q)$ was given by Schoof [528, 530]. Improvements have been given by numerous authors, especially Atkin and Elkies. The crucial idea is to use equation (9.11). Indeed, the basis of Schoof's algorithm is that if P is a point of small prime order l then one can compute $t \pmod l$ by solving the (easy) discrete logarithm problem

$$\pi_q(\pi_q(P)) + [q]P = [t \pmod l]\pi_q(P).$$

One finds a point P of order l using the division polynomials $\psi_l(x, y)$ (in fact, Schoof never writes down an explicit P, but rather works with a "generic" point of order l by performing polynomial arithmetic modulo $\psi_l(x, y)$). Note that, when l is odd, $\psi_l(x, y)$

is a polynomial in x only. Repeating this idea for different small primes l and applying the Chinese remainder theorem gives t. We refer to [530], Chapters VI and VII of [64], Chapter VI of [65] and Chapter 17 of [16] for details and references.

Exercise 9.10.24. Let $E : y^2 = F(x)$ over $\mathbb{F}_q$. Show that one can determine $t \pmod 2$ by considering the number of roots of $F(x)$ in $\mathbb{F}_q$.

There are a number of point counting algorithms using p-adic ideas. We do not have space to discuss these algorithms. See Chapter VI of [65] and Chapter IV of [16] for details and references.

9.11 Supersingular Elliptic Curves

This section is about a particular class of elliptic curves over finite fields that have quite different properties to the general case. For many cryptographic applications these elliptic curves are avoided, though in pairing-based cryptography they have some desirable features.

Exercise 9.11.1. Let $q = p^m$ where p is prime and let E be an elliptic curve over $\mathbb{F}_q$. Show using Exercise 9.10.10 that if $\#E(\mathbb{F}_q) \equiv 1 \pmod p$ then $\#E(\mathbb{F}_{q^n}) \equiv 1 \pmod p$ for all $n \in \mathbb{N}$. Hence, show that $E[p] = \{\mathcal{O}_E\}$ for such an elliptic curve.

Theorem 9.11.2. *Let E be an elliptic curve over $\mathbb{F}_{p^m}$ where p is prime. The following are equivalent:*

1. $\#E(\mathbb{F}_{p^m}) = p^m + 1 - t$ *where* $p \mid t$;
2. $E[p] = \{\mathcal{O}_E\}$;
3. $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ *is not commutative (hence, by Theorem 9.9.1, it is an order in a quaternion algebra);*
4. *The characteristic polynomial of Frobenius $P(T) = T^2 - tT + p^m$ factors over $\mathbb{C}$ with roots α_1, α_2 such that $\alpha_i/\sqrt{p^m}$ are roots of unity. (Recall that a root of unity is a complex number z such that there is some $n \in \mathbb{N}$ with $z^n = 1$.)*

Proof: The equivalence of Properties 1, 2 and 3 is shown in Theorem 3.1 of Silverman [564]. Property 4 is shown in Proposition 13.6.2 of Husemöller [302]. □

Definition 9.11.3. An elliptic curve E over $\mathbb{F}_{p^m}$ is **supersingular** if it satisfies any of the conditions of Theorem 9.11.2. An elliptic curve is **ordinary** if it does not satisfy any of the conditions of Theorem 9.11.2.

We stress that a supersingular curve is not singular as a curve. The name "supersingular" originates from the theory of "singular invariants" in the theory of modular functions.

Example 9.11.4. Let $p \equiv 2 \pmod 3$ be prime and let $a_6 \in \mathbb{F}_p^*$. The elliptic curve $E : y^2 = x^3 + a_6$ is supersingular since, by Exercise 9.10.4, it has $p + 1$ points. Another way to show supersingularity for this curve is to use the endomorphism $\rho(x, y) = (\zeta_3 x, y)$ as in Exercise 9.6.25 (where $\zeta_3 \in \mathbb{F}_{p^2}$ is such that $\zeta_3^2 + \zeta_3 + 1 = 0$). Since ρ does not commute with the p-power Frobenius map π_p (specifically, $\pi_p \rho = \rho^2 \pi_p$, since $\zeta_3 \notin \mathbb{F}_p$) the endomorphism ring is not commutative.

To determine the quaternion algebra one can proceed as follows. First show that ρ satisfies the characteristic polynomial $T^2 + T + 1 = 0$ (since $\rho^3(P) = P$ for all $P \in E(\overline{\mathbb{F}}_p)$).

Then consider the isogeny $\phi = [1] - \rho$, which has dual $\widehat{\phi} = [1] - \rho^2$. The degree d of ϕ satisfies $[d] = \phi\widehat{\phi} = (1-\rho)(1-\rho^2) = 1 - \rho - \rho^2 + 1 = 3$. Hence ϕ has degree 3. The trace of ϕ is $t = 1 + \deg(\phi) - \deg(1-\phi) = 1 + 3 - \deg(\rho) = 3$. One can show that $(\rho\phi)^2 = [-3]$ and so the quaternion algebra is $\mathbb{Q}[i,j]$ with $i^2 = -3$ and $j^2 = -p$.

Example 9.11.5. Let $p \equiv 3 \pmod 4$ be prime and $a_4 \in \mathbb{F}_p^*$. Exercise 9.10.5 implies that $E : y^2 = x^3 + a_4 x$ is supersingular. An alternative proof of supersingularity follows from Example 9.9.2; since $\xi(x,y) = (-x, iy)$ does not commute with the p-power Frobenius.

Example 9.11.6. Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $F(x) \in \mathbb{F}_q[x]$ a monic polynomial of degree 3. Then $E : y^2 + y = F(x)$ is supersingular. This follows from the fact that $(x,y) \in E(\mathbb{F}_{q^n})$ if and only if $(x, y+1) \in E(\mathbb{F}_{q^n})$ and hence $\#E(\mathbb{F}_{q^n})$ is odd for all n. It follows that there are no points of order 2 in $E(\overline{\mathbb{F}}_2)$ and so E is supersingular.

Exercise 9.11.7. Use Waterhouse's theorem to show that, for every prime p and $m \in \mathbb{N}$, there exists a supersingular curve over $\mathbb{F}_{p^m}$.

Bröker [107] has given an algorithm to construct supersingular elliptic curves over finite fields using the CM method. The basic algorithm also appeared as Algorithm A2 in Sakai, Ohgishi and Kasahara [509]. The method has expected polynomial-time complexity, assuming a generalisation of the Riemann hypothesis is true.

Property 4 of Theorem 9.11.2 implies that if E is a supersingular curve then $\pi_q^m = [p^M]$ for some $m, M \in \mathbb{N}$. In other words, $\pi_q^m \in \mathbb{Z}$. In examples we have seen $\pi^2 = [-q]$. A natural question is how large the integer m can be.

Lemma 9.11.8. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$ and let $P(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of Frobenius. Then every non-square factor of $\frac{1}{q}P(T\sqrt{q})$ divides $\Phi_m(T^2)$ in $\mathbb{R}[T]$ for some $m \in \{1,2,3,4,6\}$, where $\Phi_m(x)$ is the m-th cyclotomic polynomial (see Section 6.1).*

Proof: Waterhouse's theorem gives the possible values for the characteristic polynomial $P(T) = T^2 - tT + q$ of Frobenius. The possible values for t are 0, $\pm\sqrt{q}$, $\pm 2\sqrt{q}$, $\pm\sqrt{2q}$ (when q is a power of 2) or $\pm\sqrt{3q}$ (when q is a power of 3).

By part 4 of Theorem 9.11.2, every root α of $P(T)$ is such that $\alpha/\sqrt{q}$ is a root of unity. If $P(T) = (T-\alpha)(T-\beta)$ then

$$(T - \alpha/\sqrt{q})(T - \beta/\sqrt{q}) = \tfrac{1}{q}P(T\sqrt{q}).$$

So, write $Q(T) = P(T\sqrt{q})/q \in \mathbb{R}[T]$. The first three values for t in the above list give $Q(T)$ equal to $T^2 + 1$, $T^2 \pm T + 1$ and $T^2 \pm 2T + 1 = (T \pm 1)^2$ respectively. The result clearly holds in these cases (the condition about "non-square factors" is needed since $(T \pm 1)$ divides $\Phi_1(T^2) = (T-1)(T+1)$ but $(T \pm 1)^2$ does not divide any cyclotomic polynomial).

We now deal with the remaining two cases. Let $t = \pm 2^{(m+1)/2}$ where $q = 2^m$. Then $Q(T) = T^2 \pm \sqrt{2}T + 1$ and we have

$$(T^2 + \sqrt{2}T + 1)(T^2 - \sqrt{2}T + 1) = T^4 + 1 = \Phi_4(T^2).$$

Similarly, when $t = \pm 3^{(m+1)/2}$ and $q = 3^m$ then $Q(T) = T^2 \pm \sqrt{3}T + 1$ and

$$(T^2 + \sqrt{3}T + 1)(T^2 - \sqrt{3}T + 1) = T^4 - T^2 + 1 = \Phi_6(T^2).$$

□

Corollary 9.11.9. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$. Then there is an integer $m \in \{1,2,3,4,6\}$ such that $\pi_q^m \in \mathbb{Z}$ and the exponent of the group $E(\mathbb{F}_q)$ divides (q^m-1). Furthermore, the cases $m = 3,4,6$ only occur when q is a square, a power of 2, or a power of 3 respectively.*

Exercise 9.11.10. Prove Corollary 9.11.9.

Lemma 9.11.11. *Let $p > 3$ be prime, let $E/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve and let $\mathcal{O} = \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$. Then $j(E) \in \mathbb{F}_p$ if and only if $\sqrt{-p} \in \mathcal{O}$.*

Proof: ($\Rightarrow$) $j(E) \in \mathbb{F}_p$ implies E is defined over $\mathbb{F}_p$ and so $\mathcal{O}$ contains a Frobenius element π satisfying (by Theorem 9.10.12, since $p > 3$) the characteristic polynomial $\pi^2 + p = 0$.

($\Leftarrow$) Let $\psi \in \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ satisfy $\psi^2 = [-p]$. Then ψ is an isogeny of degree p and $\widehat{\psi} \circ \psi = [p]$. Since E is supersingular it follows that ψ has trivial kernel and so is inseparable. Hence, by Theorem 9.6.17, ψ composes as

$$E \xrightarrow{\pi} E^{(p)} \xrightarrow{\lambda} E$$

where π is the p-power Frobenius map and $E^{(p)}$ is the image curve of Frobenius. Now $\deg(\lambda) = 1$ and so λ is an isomorphism. Hence, $j(E) = j(E^{(p)}) = j(E)^p$. Hence, $j(E) \in \mathbb{F}_p$. □

In general, the endomorphism ring of a supersingular elliptic curve is generated over $\mathbb{Z}$ by the Frobenius map and some "complex multiplication" isogeny. However, as seen in Example 9.10.6, the Frobenius can lie in $\mathbb{Z}$, in which case two independent "complex multiplications" are needed (though, as in Example 9.10.6, one of them will be very closely related to a Frobenius map on a related elliptic curve).

It is known that the endomorphism ring $\mathrm{End}_{\overline{\mathbb{k}}}(E)$ of a supersingular elliptic curve E over a finite field $\mathbb{k}$ is a **maximal order** in a quaternion algebra (see Theorem 4.2 of Waterhouse [627]) and that the quaternion algebra is ramified at exactly p and ∞. Indeed, [627] (Theorem 4.1) shows that when $t = \pm 2\sqrt{q}$ then all endomorphisms are defined over $\mathbb{F}_q$ and every maximal order arises. In other cases not all endomorphisms are defined over $\mathbb{F}_q$ and the maximal order is an order that contains π_q and is maximal at p (i.e., the index is not divisible by p).

We now present some results on the number of supersingular curves over finite fields.

Theorem 9.11.12. *Let $\mathbb{F}_q$ be a field of characteristic p and $E/\mathbb{F}_q$ a supersingular elliptic curve. Then $j(E) \in \mathbb{F}_{p^2}$. Furthermore:*

1. *The number of $\overline{\mathbb{F}}_q$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is 1 if $p = 2,3$ and $\lfloor p/12 \rfloor + \epsilon_p$ where $\epsilon_p = 0,1,1,2$ respectively if $p \equiv 1,5,7,11 \pmod{12}$.*

2. *The number of $\overline{\mathbb{F}}_q$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ is 1 if $p = 2,3$ and is equal to the Hurwitz class number $H(-4p)$ if $p > 3$. Furthermore,*

$$H(-4p) = \begin{cases} \frac{1}{2}h(-4p) & \text{if } p \equiv 1 \pmod 4, \\ h(-p) & \text{if } p \equiv 7 \pmod 8, \\ 2h(-p) & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

where $h(d)$ is the usual ideal class number of the quadratic field $\mathbb{Q}(\sqrt{d})$.

Proof: The claim that $j(E) \in \mathbb{F}_{p^2}$ is Theorem V.3.1(a)(iii) of [564] or Theorem 5.6 of [302]. The formula for the number of supersingular j-invariants in $\mathbb{F}_{p^2}$ is Theorem 4.1(c)

of [564] or Section 13.4 of [302]. The statement about the number of supersingular j-invariants in $\mathbb{F}_p$ is given in Theorem 14.18 of Cox [157] (the supersingular case is handled on page 322). The precise formula for $H(-4p)$ is equation (1.11) of Gross [268]. (Gross also explains the relation between isomorphism classes of supersingular curves and Brandt matrices.) □

Lemma 9.11.13. *Let E_1, E_2 be elliptic curves over $\mathbb{F}_q$. Show that if E_1 and E_2 are ordinary, $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ and $j(E_1) = j(E_2)$ then they are isomorphic over $\mathbb{F}_q$.*

Proof: (Sketch) Since $j(E_1) = j(E_2)$ the curves are isomorphic over $\overline{\mathbb{F}}_q$. If $\#E_1(\mathbb{F}_q) = q + 1 - t$ and E_2 is not isomorphic to E_1 over $\mathbb{F}_q$, then E_2 is a non-trivial twist of E_1. If $j(E_1) \neq 0, 1728$ then $\#E_2(\mathbb{F}_q) = q + 1 + t \neq \#E_1(\mathbb{F}_q)$, since $t \neq 0$ (this is where we use the fact that E_1 is ordinary). In the cases $j(E_1) = 0, 1728$ one needs to use the formulae of Example 9.10.20 and Exercise 9.10.22 and show that these group orders are distinct when $t \neq 0$.

An alternative proof, using less elementary methods, is given in Proposition 14.19 (page 321) of Cox [157]. □

Exercise 9.11.14. Give an example of supersingular curves E_1, E_2 over $\mathbb{F}_p$ such that $j(E_1) = j(E_2)$, $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ and E_1 is not isomorphic to E_2 over $\mathbb{F}_p$.

9.12 Alternative Models for Elliptic Curves

We have introduced elliptic curves using Weierstrass equations, but there are many different models and some of them have computational advantages. We present the Montgomery model and the twisted Edwards model. A mathematically important model, which we do not discuss directly, is the intersection of two quadratic surfaces; see Section 2.5 of Washington [626] for details. It is not the purpose of this book to give an implementation guide, so we refrain from providing the optimised addition algorithms. Readers are advised to consult Sections 13.2 and 13.3 of [16] or the Explicit Formulas Database [51].

9.12.1 Montgomery Model

This model, for elliptic curves over fields of odd characteristic, was introduced by Montgomery [436] in the context of efficient elliptic curve factoring using $(x : z)$ coordinates. It is a very convenient model for arithmetic in (a projective representation of) the algebraic group quotient $E(\Bbbk)$ modulo the equivalence relation $P \equiv -P$. Versions of the Montgomery model have been given in characteristic 2 but they are not so successful; we refer to Stam [578] for a survey.

Definition 9.12.1. Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2$. Let $A, B \in \Bbbk$, $B \neq 0$. The **Montgomery model** is

$$By^2 = x^3 + Ax^2 + x. \tag{9.13}$$

According to Definition 7.2.8, when $B \neq 1$, the Montgomery model is not an elliptic curve. However, the theory all goes through in the more general case, and so we refer to curves in Montgomery model as elliptic curves.

Exercise 9.12.2. Show that the Montgomery model is non-singular if and only if $B(A^2 - 4) \neq 0$.

Exercise 9.12.3. Show that there is a unique point at infinity on the Montgomery model of an elliptic curve. Show that this point is not singular, and is always $\Bbbk$-rational.

Lemma 9.12.4. *Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2$. Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$ in Weierstrass form. There is an isomorphism over $\Bbbk$ from E to a Montgomery model if and only if $F(x) = x^3 + a_2x^2 + a_4x + a_6$ has a root $x_P \in \Bbbk$ such that $(3x_P^2 + 2a_2x_P + a_4)$ is a square in $\Bbbk$. This isomorphism maps $\mathcal{O}_E$ to the point at infinity on the Montgomery model and is a group homomorphism.*

Proof: Let $P = (x_P, 0) \in E(\Bbbk)$. First move P to $(0, 0)$ by the change of variable $X = x - x_P$. The map $(x, y) \mapsto (x - x_P, y)$ is an isomorphism to $y^2 = X^3 + a_2'X^2 + a_4'X$ where $a_2' = 3x_P + a_2$ and $a_4' = 3x_P^2 + 2a_2x_P + a_4$. Let $w = \sqrt{a_4'}$, which lies in $\Bbbk$ by the assumption of the Lemma. Consider the isomorphism $(X, y) \mapsto (U, V) = (X/w, y/w)$ that maps to

$$(1/w)V^2 = U^3 + (a_2'/w)U^2 + U.$$

Taking $A = a_2'/w, B = 1/w \in \Bbbk$ gives the result.

Conversely, suppose $By^2 = x^3 + Ax^2 + x$ is a Montgomery model of an elliptic curve over $\Bbbk$. Multiplying though by B^3 gives $(B^2y)^2 = (Bx)^3 + AB(Bx)^2 + B^2(Bx)$ and so $(U, V) = (Bx, B^2y)$ satisfies the Weierstrass equation $V^2 = U^3 + ABU^2 + B^2U$. Taking $a_2 = AB, a_4 = B^2$ and $a_6 = 0$ one can check that the conditions in the statement of the Lemma hold (the polynomial $F(x)$ has the root 0, and $a_4' = B^2$ is a square).

The maps extend to the projective curves and map $(0 : 1 : 0)$ to $(0 : 1 : 0)$. The fact that they are group homomorphisms follows from a generalisation of Theorem 9.2.1. □

When the conditions of Lemma 9.12.4 hold we say that the elliptic curve E can be written in Montgomery model. Throughout this section, when we refer to an elliptic curve E in Montgomery model, we assume that E is specified by an affine equation as in equation (9.13).

Lemma 9.12.5. *Let $P_1 = (x_1, y_2), P_2 = (x_2, y_2)$ be points on the elliptic curve $By^2 = x^3 + Ax^2 + x$ such that $x_1 \neq x_2$ and $x_1x_2 \neq 0$. Then $P_1 + P_2 = (x_3, y_3)$ where*

$$x_3 = B(x_2y_1 - x_1y_2)^2/(x_1x_2(x_2 - x_1)^2).$$

Writing $P_1 - P_2 = (x_4, y_4)$ one finds

$$x_3x_4 = (x_1x_2 - 1)^2/(x_1 - x_2)^2.$$

For the case $P_2 = P_1$ we have $[2](x_1, y_1) = (x_3, y_3)$ where

$$x_3 = (x_1^2 - 1)^2/(4x_1(x_1^2 + Ax_1 + 1)).$$

Proof: The standard addition formula gives $x_3 = B((y_2 - y_1)/(x_2 - x_1))^2 - (A + x_1 + x_2)$, which yields

$$\begin{aligned} x_3(x_2 - x_1)^2 &= By_1^2 + By_2^2 - 2By_1y_2 - (A + x_1 + x_2)(x_2 - x_1)^2 \\ &= -2By_1y_2 + 2Ax_1x_2 + x_1^2x_2 + x_1x_2^2 + x_1 + x_2 \\ &= \tfrac{x_2}{x_1}By_1^2 + \tfrac{x_1}{x_2}By_2^2 - 2By_1y_2 \\ &= B(x_2y_1 - x_1y_2)^2/(x_1x_2). \end{aligned}$$

Replacing P_2 by $-P_2$ gives $P_1-P_2=(x_4,y_4)$ with $x_4(x_2-x_1)^2=B(x_2y_1+x_1y_2)^2/(x_1x_2)$. Multiplying the two equations gives

$$\begin{aligned} x_3x_4(x_2-x_1)^4 &= B^2(x_2y_1-x_1y_2)^2(x_2y_1+x_1y_2)^2/(x_1x_2)^2 \\ &= \left(\frac{x_2By_1^2}{x_1}-\frac{x_1By_2^2}{x_2}\right)^2 \\ &= (x_1x_2(x_1-x_2)+(x_2-x_1))^2 \end{aligned}$$

from which we deduce that $x_3x_4(x_2-x_1)^2=(x_1x_2-1)^2$. In the case $P_1=P_2$ we have $x_34By_1^2=(3x_1^2+2Ax_1+1)^2-(A+2x_1)4By_1^2$, which implies $4x_1x_3(x_1^2+Ax_1+1)=(x_1^2-1)^2$. □

In other words, one can compute the x-coordinate of $[2]P$ using only the x-coordinate of P. Similarly, given the x-coordinates of P_1, P_2 and P_1-P_2 (i.e., x_1, x_2 and x_4) one can compute the x-coordinate of P_1+P_2. The next exercise shows how to do this projectively.

Exercise 9.12.6. Let $P=(x_P,y_P)\in E(\mathbb{F}_q)$ be a point on an elliptic curve given in a Montgomery model. Define $X_1=x_P, Z_1=1$, $X_2=(X_1^2-1)^2, Z_2=4x_1(x_1^2+Ax_1+1)$. Given $(X_n,Z_n),(X_m,Z_m),(X_{m-n},Z_{m-n})$ define

$$\begin{aligned} X_{n+m} &= Z_{m-n}(X_nX_m-Z_nZ_m)^2 \\ Z_{n+m} &= X_{m-n}(X_nZ_m-X_mZ_n)^2 \end{aligned}$$

and

$$\begin{aligned} X_{2n} &= (X_n^2-Z_n^2)^2 \\ Z_{2n} &= 4X_nZ_n(X_n^2+AX_nZ_n+Z_n^2). \end{aligned}$$

Show that the x-coordinate of $[m]P$ is X_m/Z_m.

Exercise 9.12.7.★ Write a "double and add" algorithm to compute the x-coordinate of $[n]P$ using the projective Montgomery addition formula. Give alternative versions of the Montgomery addition formulae that show that each iteration of your algorithm requires only 7 multiplications and 4 squarings in $\mathbb{F}_q$.

The most efficient formulae for exponentiation using a ladder algorithm on Montgomery curves are given in Section 6.2 of Gaudry and Lubicz [247] (also see [51]).

Exercise 9.12.8. Let $E: By^2=x(x^2+a_2x+a_4)$ be an elliptic curve over $\Bbbk$ (where $\mathrm{char}(\Bbbk)\neq 2$). Show that the solutions $(x,y)\in E(\overline{\Bbbk})$ to $[2](x,y)=(0,0)$ are the points $(\sqrt{a_4},\pm\sqrt{a_4(a_2+2\sqrt{a_4})/B})$ and $(-\sqrt{a_4},\pm\sqrt{a_4(a_2-2\sqrt{a_4})/B})$.

Lemma 9.12.9. *(Suyama) If E is an elliptic curve given by a Montgomery model then $4\mid \#E(\mathbb{F}_q)$.*

Proof: If $A^2-4=(A-2)(A+2)$ is a square then the full 2-torsion is over $\mathbb{F}_q$. If $(A-2)(A+2)$ is not a square then one of $(A\pm 2)$ is a square in $\mathbb{F}_q$ and the other isn't. If $B(A+2)$ is a square then $(1,\sqrt{(A+2)/B})$ is defined over $\mathbb{F}_q$ and, by Exercise 9.12.8, has order 4. Similarly, if $B(A-2)$ is a square then $(-1,\sqrt{(A-2)/B})$ is defined over $\mathbb{F}_q$ and has order 4. □

Let $E: By^2=x^3+Ax^2+x$ be an elliptic curve over $\Bbbk$ in Montgomery model. If $u\in\Bbbk^*$ then E is isomorphic to $E^{(u)}: (uB)Y^2=X^3+AX^2+X$ where the corresponding isomorphism $\phi: E\to E^{(u)}$ is $\phi(x,y)=(x,y/\sqrt{u})$. If u is not a square in $\Bbbk$ then ϕ is not defined over $\Bbbk$ and so $E^{(u)}$ is the **quadratic twist** of E.

Exercise 9.12.10. Show that every elliptic curve E in Montgomery model over a finite field $\mathbb{F}_q$ is such that either E or its quadratic twist $E^{(d)}$ has a point of order 4.

Theorem 9.12.11. *Let E be an elliptic curve over $\mathbb{F}_q$ ($\mathrm{char}(\mathbb{F}_q) \neq 2$) such that $4 \mid \#E(\mathbb{F}_q)$. Then E is either isomorphic or 2-isogenous over $\mathbb{F}_q$ to an elliptic curve in Montgomery model.*

Proof: Suppose $P \in E(\mathbb{F}_q)$ has order 4. Write $P_0 = [2]P$ and change coordinates so that $P_0 = (0,0)$. By Exercise 9.12.8 it follows that a_4 is a square in $\mathbb{F}_q$ and so by Lemma 9.12.4 is isomorphic to an elliptic curve in Montgomery model.

Suppose now that there is no point of order 4 in $E(\mathbb{F}_q)$. Then $\#E(\mathbb{F}_q)[2] = 4$ and so all points of order 2 are defined over $\mathbb{F}_q$. In other words, one can write E as $y^2 = x(x-a)(x-b) = x(x^2-(a+b)x+ab)$ where $a, b \in \mathbb{F}_q$. Now take the 2-isogeny as in Example 9.6.9. This maps E to $E' : Y^2 = X(X^2+2(a+b)X+(a-b)^2)$. By Lemma 9.12.4 it follows that E' is isomorphic to an elliptic curve in Montgomery model. □

We have already seen the quadratic twist of a Montgomery model. It is natural to consider whether there are other twists.

Theorem 9.12.12. *Let $q = p^n$ where $p > 3$ is prime. If $E/\mathbb{F}_q$ is an ordinary elliptic curve admitting a Montgomery model then only one non-trivial twist also admits a Montgomery model. Furthermore, this twist is the quadratic twist.*

Proof: When $j(E) \neq 0, 1728$ then the quadratic twist is the only non-trivial twist, so there is nothing to prove. So we consider $j(E) = 1728$ and $j(E) = 0$. The crucial observation will be that the other twists E' do not satisfy $4 \mid \#E'(\mathbb{F}_q)$.

By Example 9.10.20, if $j(E) = 1728$ then $q \equiv 1 \pmod 4$, $q = a^2+b^2$ for some $a, b \in \mathbb{Z}$, and the group orders are $q+1\pm 2a$ and $q+1\pm 2b$. Note that, without loss of generality, the solution (a,b) to $q = a^2+b^2$ is such that a is odd and b is even. Then $2a \not\equiv 2b \pmod 4$ and so only one of $q+1+2a$ and $q+1+2b$ is divisible by 4. Since $q+1+2a \equiv q+1-2a \pmod 4$ (and similarly for the other case) it follows that only one pair of quadratic twists can be given in Montgomery model.

By Exercise 9.10.22, if $j(E) = 0$ then $q \equiv 1 \pmod 3$, $q = a^2+ab+b^2$ for some $a, b \in \mathbb{Z}$, and the possible group orders are

$$q+1\pm(a-b), \quad q+1\pm(2a+b), \quad q+1\pm(2b+a).$$

Without loss of generality a is odd and b may be either odd or even. If a and b are both odd then $2a-b$ and $2b-a$ are both odd and so $q+1\pm(a+b)$ is the only pair of group orders that are even. Similarly, if a is odd and b is even then $a+b$ and $2b+a$ are both odd and so $q+1\pm(2a+b)$ is the only pair of group orders that are even. This completes the proof. □

Example 9.12.13. The elliptic curve $y^2 = x^3 + a_4x$ is isomorphic over $\overline{\mathbb{k}}$ to the curve $\sqrt{a_4}Y^2 = X^3 + X$ in Montgomery form via $(x,y) \mapsto (X,Y) = (x/\sqrt{a_4}, y/a_4)$.

The elliptic curve $y^2 = x^3 + a_6$ is isomorphic over $\overline{\mathbb{k}}$ to the curve

$$1/(\sqrt{3}(-a_6)^{1/3})Y^2 = X^3 + \sqrt{3}X^2 + X$$

in Montgomery model. To see this, consider the point $P = ((-a_6)^{1/3}, 0)$ and move it to $(0,0)$ via $W = x - a_6^{1/3}$, giving $y^2 = W^3 + 3(-a_6)^{1/3}W^2 + 3(-a_6)^{2/3}W$.

9.12.2 Edwards Model

Euler and Gauss considered the genus 1 curve $x^2 + y^2 = 1 - x^2y^2$ and described a group operation on its points. Edwards generalised this to a wide class of elliptic curves (we refer to [190] for details and historical discussion). Further extensions were proposed by Bernstein, Birkner, Joye, Lange, and Peters (see [48] and its references). Edwards curves have several important features: they give a complete group law on $E(\mathbb{F}_q)$ for some fields $\mathbb{F}_q$ (in other words, there is a single rational map $+ : E \times E \to E$ that computes addition for all[4] possible inputs in $E(\mathbb{F}_q) \times E(\mathbb{F}_q)$) and the addition formulae can be implemented extremely efficiently in some cases. Hence this model for elliptic curves is very useful for many cryptographic applications.

Definition 9.12.14. Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2$. Let $a, d \in \Bbbk$ satisfy $a \neq 0, d \neq 0, a \neq d$. The **twisted Edwards model** is

$$ax^2 + y^2 = 1 + dx^2y^2.$$

Exercise 9.12.15. Show that a curve in twisted Edwards model is non-singular as an affine curve. Show that if any of the conditions $a \neq 0, d \neq 0$ and $a \neq d$ are not satisfied then the affine curve has a singular point.

Bernstein, Lange and Farashahi [55] have also formulated an Edwards model for elliptic curves in characteristic 2.

The Weierstrass model of an elliptic curve over $\Bbbk$ (where $\mathrm{char}(\Bbbk) \neq 2$) is of the form $y^2 = F(x)$ and it would be natural to write the twisted Edwards model in the form $y^2 = (1 - ax^2)/(1 - dx^2)$. A natural formulation of the group law would be such that the inverse of a point (x, y) is $(x, -y)$. This leads to having identity element $(x, y) = (1/\sqrt{a}, 0)$. Instead, for historical reasons, it is traditional to think of the curve as

$$x^2 = (1 - y^2)/(a - dy^2).$$

The identity element is then $(0, 1)$ and the inverse of (x, y) is $(-x, y)$.

The group operation on twisted Edwards models is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right). \tag{9.14}$$

This is shown to be a group law in [52, 48]. A geometric description of the Edwards group law on the singular curve is given by Arène, Lange, Naehrig and Ritzenthaler [12]. An inversion-free (i.e., projective) version and explicit formulae for efficient arithmetic are given in [48].

Exercise 9.12.16. Let E be a curve over $\Bbbk$ in twisted Edwards model. Show that $(0, -1) \in E(\Bbbk)$ has order 2 and that $(\pm 1/\sqrt{a}, 0) \in E(\overline{\Bbbk})$ have order 4.

Exercise 9.12.17. Determine the points at infinity on a curve in twisted Edwards model and show they are singular.

We now give a non-singular projective model for twisted Edwards models that allows us to view the points at infinity and determine their orders.

[4] Note that this is a stronger statement than the unified group law of Exercise 9.1.1 as the group law on (twisted) Edwards curve also includes addition of a point with its inverse or the identity element. Also, the group law on (twisted) Edwards curves achieves this with no loss of efficiency, unlike Exercise 9.1.1. On the other hand, we should mention that the group law on (twisted) Edwards curves is never complete for the group $E(\overline{\mathbb{F}}_q)$.

Lemma 9.12.18. *Let $\Bbbk$ be a field of characteristic not equal to 2. Let $a, d \in \Bbbk$ with $a, d \neq 0$. There are four points at infinity over $\overline{\Bbbk}$ on a twisted Edwards model over $\Bbbk$ and they all have order dividing 4.*

Proof: (Sketch) The rational map $\phi(x, y) = (X_0 = xy, X_1 = x, X_2 = y, X_3 = 1)$ maps a twisted Edwards curve to the projective algebraic set

$$X = V(aX_1^2 + X_2^2 - X_3^2 - dX_0^2, X_1X_2 - X_0X_3) \subset \mathbb{P}^3.$$

It can be shown that X is irreducible and of dimension 1.

The points at infinity on the affine twisted Edwards model correspond to the points

$$(1 : \pm\sqrt{d/a} : 0 : 0) \quad \text{and} \quad (1 : 0 : \pm\sqrt{d} : 0)$$

with $X_3 = 0$. To see that the points at infinity on X are non-singular, set $X_0 = 1$ and obtain the Jacobian matrix

$$\begin{pmatrix} 2aX_1 & 2X_2 & -2X_3 \\ X_2 & X_1 & -1 \end{pmatrix},$$

which is seen to have rank 2 when evaluated at the points $(\pm\sqrt{d/a}, 0, 0)$ and $(0, \pm\sqrt{d}, 0)$.

Let $(X_0 : X_1 : X_2 : X_3)$ and $(Z_0 : Z_1 : Z_2 : Z_3)$ be points on X and define the values

$$S_1 = (X_1Z_2 + Z_1X_2),\ S_2 = (X_2Z_2 - aX_1Z_1),\ S_3 = (X_3Z_3 + dX_0Z_0),\ S_4 = (X_3Z_3 - dX_0Z_0).$$

The group law formula on the affine twisted Edwards curve corresponds to the formula

$$(X_0 : X_1 : X_2 : X_3) + (Z_0 : Z_1 : Z_2 : Z_3) = (S_1S_2 : S_1S_4 : S_2S_3 : S_3S_4).$$

One can verify that $(0 : 0 : 1 : 1)$ is the identity by computing

$$(X_0 : X_1 : X_2 : X_3) + (0 : 0 : 1 : 1) = (X_1X_2 : X_1X_3 : X_2X_3 : X_3^2).$$

When $X_3 \neq 0$ one replaces the first coordinate X_1X_2 by X_0X_3 and divides by X_3 to get $(X_0 : X_1 : X_2 : X_3)$. When $X_3 = 0$ one multiplies through by X_0, replaces X_0X_3 by X_1X_2 everywhere, and divides by X_1X_2.

Similarly, one can verify that $(0 : 0 : -1 : 1)$ and $(1 : \pm\sqrt{d/a} : 0 : 0)$ have order 2, and $(1 : 0 : \pm\sqrt{d} : 0)$ have order 4. □

We now show that the Edwards group law is complete for points defined over $\Bbbk$ in certain cases.

Lemma 9.12.19. *Let $\Bbbk$ be a field,* $\mathrm{char}(\Bbbk) \neq 2$ *and let $a, d \in \Bbbk$ be such that $a \neq 0, d \neq 0, a \neq d$. Suppose a is a square in $\Bbbk^*$ and d is not a square in $\Bbbk^*$. Then the affine group law formula for twisted Edwards curves of equation (9.14) is defined for all points over $\Bbbk$.*

Proof: Let $\epsilon = dx_1x_2y_1y_2$. Suppose, for contradiction, that $\epsilon = \pm 1$. Then $x_1, x_2, y_1, y_2 \neq 0$. One can show, by substituting $ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2$, that

$$dx_1^2y_1^2(ax_2^2 + y_2^2) = ax_1^2 + y_1^2.$$

Adding $\pm 2\sqrt{a}\epsilon x_1y_1$ to both sides and inserting the definition of ϵ gives

$$(\sqrt{a}x_1 \pm \epsilon y_1)^2 = dx_1^2y_1^2(\sqrt{a}x_2 \pm y_2)^2.$$

Hence, if either $\sqrt{a}x_2 + y_2 \neq 0$ or $\sqrt{a}x_2 - y_2 \neq 0$ then one can deduce that d is a square in $\Bbbk^*$. On the other hand, if $\sqrt{a}x_2 + y_2 = \sqrt{a}x_2 - y_2 = 0$ one deduces that $x_2 = 0$. Both cases are a contradiction. □

It turns out that twisted Edwards curves and Montgomery curves cover exactly the same $\Bbbk$-isomorphism classes of elliptic curves.

Lemma 9.12.20. *Let $M : By^2 = x^3 + Ax^2 + x$ be a Montgomery model for an elliptic curve over $\Bbbk$ (so $B \neq 0$ and $A^2 \neq 4$). Define $a = (A+2)/B$ and $d = (A-2)/B$. Then $a \neq 0, d \neq 0$ and $a \neq d$. The map $(x, y) \mapsto (X = x/y, Y = (x-1)/(x+1))$ is a birational map over $\Bbbk$ from M to the twisted Edwards curve*

$$E : aX^2 + Y^2 = 1 + dX^2Y^2.$$

Conversely, if E is as above then define $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. Then $(X, Y) \mapsto (x = (1+Y)/(1-Y), y = (1+Y)/(X(1-Y)))$ is a birational map over $\Bbbk$ from E to M.

Exercise 9.12.21. Prove Lemma 9.12.20.

The birational map in Lemma 9.12.20 is a group homomorphism. Indeed, the proofs of the group law in [52, 49] use this birational map to transfer the group law from the Montgomery model to the twisted Edwards model.

Exercise 9.12.22. Show that the birational map from Montgomery model to twisted Edwards model in Lemma 9.12.20 is undefined only for points P of order dividing 2 and $P = (-1, \pm\sqrt{(A-2)/B})$ (which has order 4). Show that the map from Edwards model to Montgomery model is undefined only for points $P = (0, \pm 1)$ and points at infinity.

Exercise 9.12.23. Show that a non-trivial quadratic twist of the twisted Edwards model $ax^2 + y^2 = 1 + dx^2y^2$ over $\Bbbk$ is $aux^2 + y^2 = 1 + dux^2y^2$ where $u \in \Bbbk^*$ is a non-square.

Exercise 9.12.24. Show that if an elliptic curve E can be written in twisted Edwards model then the only non-trivial twist of E that can also be written in twisted Edwards model is the quadratic twist.

Example 9.12.25. The curve

$$x^2 + y^2 = 1 - x^2y^2$$

has an automorphism $\rho(x, y) = (ix, 1/y)$ (which fixes the identity point $(0, 1)$) for $i = \sqrt{-1}$. One has $\rho^2 = -1$. Hence this curve corresponds to a twist of the Weierstrass curve $y^2 = x^3 + x$ having j-invariant 1728.

Example 9.12.26. Elliptic curves with CM by $D = -3$ (equivalently, j-invariant 0) can only be written in Edwards model if $\sqrt{3} \in \mathbb{F}_q$. Taking $d = (\sqrt{3}+2)/(\sqrt{3}-2)$ gives the Edwards curve

$$E : x^2 + y^2 = 1 + dx^2y^2,$$

which has j-invariant 0. We construct the automorphism corresponding to ζ_3 in stages. First we give the isomorphism $\phi : E \to M$ where $M : BY^2 = X^3 + AX^2 + X$ is the curve in Montgomery model with $A = 2(1+d)/(1-d)$ and $B = 4/(1-d)$. This map is $\phi(x, y) = ((1+y)/(1-y), (1+y)/(x(1-y)))$ as in Lemma 9.12.20. The action of ζ_3 on M is given by

$$\zeta(X, Y) = (\zeta_3 X + (1-\zeta_3)/\sqrt{3}, Y).$$

Then we apply $\phi^{-1}(X, Y) = (X/Y, (X-1)/(X+1))$.

9.12.3 Jacobi Quartic Model

Exercises 9.12.27 and 9.12.29 give some details of the Jacobi quartic model.

Exercise 9.12.27. Let $\Bbbk$ be a field of characteristic not equal to 2 and let $a, d \in \Bbbk$ be such that $a^2 \neq d$. Show that the algebraic set

$$C : y^2 = dx^4 + 2ax^2 + 1 \tag{9.15}$$

is irreducible. Show that the point at infinity on C is singular and that the affine curve is non-singular over $\overline{\Bbbk}$. Verify that the map $\phi(x, y) = (X, Y) = (a + (y + 1)/x^2, X/x)$ is a birational map over $\Bbbk$ from C to

$$E : 2Y^2 = X\left(X^2 - 2aX + (a^2 - d)\right). \tag{9.16}$$

Show that if d is a square then $E(\Bbbk)$ contains $E[2]$.

Definition 9.12.28. Let $\Bbbk$ be a field of characteristic not equal to 2 and let $a, d \in \Bbbk$ be such that $a^2 \neq d$. The affine curve of equation (9.15) is called the **Jacobi quartic model**. (By Exercise 9.12.27 it is birational to some elliptic curve.)

Addition formulae for Jacobi quartic curves are given by Hisil, Wong, Carter and Dawson [286].

Exercise 9.12.29. Let $q = p^m$ where $p > 2$ is prime. Show that every elliptic curve over $\mathbb{F}_q$ with $2 \mid \#E(\mathbb{F}_q)$ has a twist that is birational over $\mathbb{F}_q$ to a curve in Jacobi quartic form.

9.13 Statistical Properties of Elliptic Curves over Finite Fields

There are a number of questions, relevant for cryptography, about the set of all elliptic curves over $\mathbb{F}_q$.

The theory of complex multiplication states that if $|t| < 2\sqrt{q}$ and $\gcd(t, q) = 1$ then the number of isomorphism classes of elliptic curves E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ is given by the Hurwitz class number $H(t^2 - 4q)$. Theorem 9.11.12 gave a similar result for the supersingular case. As noted in Section 9.10.1, this means that the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with $q + 1 - t$ points is $O(D \log(D) \log(\log(D)))$, where $D = \sqrt{4q - t^2}$. We now give Lenstra's bounds on the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves with group orders in a subset of the Hasse interval.

Since the number of elliptic curves in short Weierstrass form (assuming now that $2 \nmid q$) that are $\mathbb{F}_q$-isomorphic to a given curve E is $(q - 1)/\#\mathrm{Aut}(E)$, it is traditional to count the number of $\mathbb{F}_q$-isomorphism classes weighted by $\#\mathrm{Aut}(E)$ (see Section 1.4 of Lenstra [377] for discussion and precise definitions). In other words, each $\mathbb{F}_q$-isomorphism class of elliptic curves with $j(E) = 0$ or $j(E) = 1728$ contributes less than one to the total. This makes essentially no difference to the asymptotic statements in Theorem 9.13.1. The weighted sum of all $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ is p.

Theorem 9.13.1. *(Proposition 1.9 of Lenstra [377] with the improvement of Theorem 2 of McKee [413]) There exists a constant $C_1 \in \mathbb{R}_{>0}$ such that, for any prime $p > 3$ and any $S \subset [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}] \cap \mathbb{Z}$, the weighted sum of $\mathbb{F}_p$-isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) \in S$ is at most $C_1 \#S \sqrt{p} \log(p) \log(\log(p))$.*

There exists a constant $C_2 \in \mathbb{R}_{>0}$ such that, for any prime $p > 3$ and any $S \subset [p + 1 - \sqrt{p}, p + 1 + \sqrt{p}] \cap \mathbb{Z}$, the weighted sum of $\mathbb{F}_p$-isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) \in S$ is at least $C_2(\#S - 2)\sqrt{p}/\log(p)$.

Lenstra also gave a result about divisibility of the group order by small primes.

Theorem 9.13.2. *(Proposition 1.14 of [377]) Let $p > 3$ and $l \neq p$ be primes. Then the weighted sum of all elliptic curves E over $\mathbb{F}_p$ such that $l \mid \#E(\mathbb{F}_p)$ is $p/(l-1) + O(l\sqrt{p})$ if $p \not\equiv 1 \pmod{l}$ and $pl/(l^2-1) + O(l\sqrt{p})$ if $p \equiv 1 \pmod{l}$. (Here the constants in the O are independent of l and p.)*

This result was generalised by Howe [295] to count curves with $N \mid \#E(\mathbb{F}_q)$ where N is not prime.

For cryptography it is important to determine the probability that a randomly chosen elliptic curve over $\mathbb{F}_q$ (i.e., choosing coefficients $a_4, a_6 \in F_q$ uniformly at random) is prime. A conjectural result was given by Galbraith and McKee [225].

Conjecture 9.13.3. *Let P_1 be the probability that a number within $2\sqrt{p}$ of $p+1$ is prime. Then the probability that an elliptic curve over $\mathbb{F}_p$ (p prime) has a prime number of points is asymptotic to $c_p P_1$ as $p \to \infty$, where*

$$c_p = \frac{2}{3} \prod_{l>2} \left(1 - \frac{1}{(l-1)^2}\right) \prod_{l \mid (p-1), l>2} \left(1 + \frac{1}{(l+1)(l-2)}\right).$$

Here the products are over all primes l satisfying the stated conditions.

Galbraith and McKee also give a precise conjecture for the probability that a random elliptic curve E over $\mathbb{F}_p$ has $\#E(\mathbb{F}_p) = kr$ where r is prime and $k \in \mathbb{N}$ is small.

Related problems have also been considered. For example, Koblitz [345] studies the probability that $\#E(\mathbb{F}_p)$ is prime for a fixed elliptic curve E over $\mathbb{Q}$ as p varies. A similar situation arises in the Sato-Tate distribution; namely the distribution on $[-1, 1]$ arising from $(\#E(\mathbb{F}_p) - (p+1))/(2\sqrt{p})$ for a fixed elliptic curve E over $\mathbb{Q}$ as p varies. We refer to Murty and Shparlinski [447] for a survey of other results in this area (including discussion of the Lang-Trotter conjecture).

9.14 Elliptic Curves over Rings

The elliptic curve factoring method (and some other theoretical applications in cryptography) use elliptic curves over the ring $\mathbb{Z}/N\mathbb{Z}$. When $N = \prod_{i=1}^{k} p_i$ is square-free[5] one can use the Chinese remainder theorem to interpret a triple (x, y, z) such that $y^2z + a_1xyz + a_3yz^2 \equiv x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \pmod{N}$ as an element of the direct sum $\oplus_{i=1}^{k} E(\mathbb{F}_{p_i})$ of groups of elliptic curves over fields. It is essential to use the projective representation, since there can be points that are the point at infinity modulo p_1 but not the point at infinity modulo p_2 (in other words, $p_1 \mid z$ but $p_2 \nmid z$). Considering triples (x, y, z) such that $\gcd(x, y, z) = 1$ (otherwise, the point modulo some prime is $(0, 0, 0)$) up to multiplication by elements in $(\mathbb{Z}/N\mathbb{Z})^*$ leads to a projective elliptic curve point in $E(\mathbb{Z}/N\mathbb{Z})$. The usual formulae for the group operations can be used modulo N and, when they are defined, give a group law. We refer to Section 2.11 of Washington [626] for a detailed discussion, including a set of formulae for all cases of the group law. For a more theoretical discussion we refer to Lenstra [377, 378].

[5] The non-square-free case is more subtle. We do not discuss it.

Chapter 10

Hyperelliptic Curves

Hyperelliptic curves are a natural generalisation of elliptic curves, and it was suggested by Koblitz [346] that they might be useful for public key cryptography. Note that there is not a group law on the points of a hyperelliptic curve; instead we use the divisor class group of the curve. The main goals of this chapter are to explain the geometry of hyperelliptic curves, to describe Cantor's algorithm [118] (and variants) to compute in the divisor class group of hyperelliptic curves, and then to state some basic properties of the divisor class group.

Definition 10.0.1. Let $\mathbb{k}$ be a perfect field. Let $H(x), F(x) \in \mathbb{k}[x]$ (we stress that $H(x)$ and $F(x)$ are not assumed to be monic). An affine algebraic set of the form $C : y^2 + H(x)y = F(x)$ is called a **hyperelliptic equation**. The **hyperelliptic involution** $\iota : C \to C$ is defined by $\iota(x, y) = (x, -y - H(x))$.

Exercise 10.0.2. Let C be a hyperelliptic equation over $\mathbb{k}$. Show that if $P \in C(\mathbb{k})$ then $\iota(P) \in C(\mathbb{k})$.

When the projective closure (in an appropriate space) of the algebraic set C in Definition 10.0.1 is irreducible, dimension 1, non-singular and of genus $g \geq 2$ then we will call it a hyperelliptic curve. By definition, a curve is projective and non-singular. We will give conditions for when a hyperelliptic equation is non-singular. Exercise 10.1.20 will give a projective non-singular model, but in practice one can work with the affine hyperelliptic equation. To "see" the points at infinity we will move them to points on a related affine equation, namely the curve $C^\dagger$ of equation (10.3).

The classical definition of a hyperelliptic curve (over an algebraically closed field $\overline{\mathbb{k}}$) is that it is a non-singular projective irreducible curve C over $\overline{\mathbb{k}}$ (usually of genus $g \geq 2$) with a degree 2 rational map $\phi : C \to \mathbb{P}^1$ over $\overline{\mathbb{k}}$. This is equivalent to C having an (affine) equation of the form $y^2 + H(x)y = F(x)$ over $\overline{\mathbb{k}}$. When C is defined over a non-algebraically closed field $\mathbb{k}$ then the existence of a rational map $\phi : C \to \mathbb{P}^1$ over $\overline{\mathbb{k}}$ does not imply the existence of such a map over $\mathbb{k}$, and so C might not have an equation

over $\mathbb{k}$ of this form. This subtlety does not arise when working over finite fields (to show this, combine Theorem 10.7.4 with the Riemann-Roch theorem), hence we will define hyperelliptic curves using a generalisation of the Weierstrass equation.

The genus has already been defined (see Definition 8.4.8) as a measure of the complexity of a curve. The treatment of the genus in this chapter is very "explicit". We will give precise conditions (Lemmas 10.1.6 and 10.1.8) that explain when the degree of a hyperelliptic equation is minimal. From this minimal degree we define the genus. In contrast, the approach of most other authors is to use the Riemann-Roch theorem.

We remark that one can also consider the algebraic group quotient $\mathrm{Pic}^0_{\mathbb{F}_q}(C)/[-1]$ of equivalence classes $\{D, -D\}$ where D is a reduced divisor. For genus 2 curves this object can be described as a variety, called the **Kummer surface**. It is beyond the scope of this book to give the details of this case. We refer to Chapter 3 of Cassels and Flynn [123] for background. Gaudry [244] and Gaudry and Lubicz [247] have given fast algorithms for computing with this algebraic group quotient.

10.1 Non-Singular Models for Hyperelliptic Curves

Consider the singular points on the affine curve $C(x, y) = y^2 + H(x)y - F(x) = 0$. The partial derivatives are $\partial C(x,y)/\partial y = 2y + H(x)$ and $\partial C(x,y)/\partial x = H'(x)y - F'(x)$, so a singular point in particular satisfies $2F'(x) + H(x)H'(x) = 0$. If $H(x) = 0$ and if the characteristic of $\mathbb{k}$ is not 2 then C is non-singular over $\overline{\mathbb{k}}$ if and only if $F(x)$ has no repeated root in $\overline{\mathbb{k}}$.

Exercise 10.1.1. Show that the curve $y^2 + H(x)y = F(x)$ over $\mathbb{k}$ has no affine singular points if and only if one of the following conditions hold.

1. $\mathrm{char}(\mathbb{k}) = 2$ and $H(x)$ is a non-zero constant.
2. $\mathrm{char}(\mathbb{k}) = 2$, $H(x)$ is a non-zero polynomial and $\gcd(H(x), F'(x)^2 - F(x)H'(x)^2) = 1$.
3. $\mathrm{char}(\mathbb{k}) \neq 2$, $H(x) = 0$ and $\gcd(F(x), F'(x)) = 1$.
4. $\mathrm{char}(\mathbb{k}) \neq 2$, $H(x) \neq 0$ and $\gcd(H(x)^2 + 4F(x), 2F'(x) + H(x)H'(x)) = 1$ (this applies even when $H(x) = 0$ or $H'(x) = 0$).

We will now give a simple condition for when a hyperelliptic equation is geometrically irreducible and of dimension 1.

Lemma 10.1.2. *Let $C(x, y) = y^2 + H(x)y - F(x)$ over $\mathbb{k}$ be a hyperelliptic equation. Suppose that $\deg(F(x))$ is odd. Suppose also that there is no point $P = (x_P, y_P) \in C(\overline{\mathbb{k}})$ such that $(\partial C(x,y)/\partial x)(P) = (\partial C(x,y)/\partial y)(P) = 0$. Then the affine algebraic set $V(C(x, y))$ is geometrically irreducible. The dimension of $V(C(x, y))$ is 1.*

Proof: From Theorem 5.3.10, $C(x, y) = 0$ is $\overline{\mathbb{k}}$-reducible if and only if $C(x, y)$ factors over $\overline{\mathbb{k}}[x, y]$. By considering $C(x, y)$ as an element of $\overline{\mathbb{k}}(x)[y]$ it follows that such a factorisation must be of the form $C(x, y) = (y - a(x))(y - b(x))$ with $a(x), b(x) \in \overline{\mathbb{k}}[x]$. Since $\deg(F)$ is odd it follows that $\deg(a(x)) \neq \deg(b(x))$ and that at least one of $a(x)$ and $b(x)$ is non-constant. Hence $a(x) - b(x)$ is a non-constant polynomial, so let $x_P \in \overline{\mathbb{k}}$ be a root of $a(x) - b(x)$ and set $y_P = a(x_P) = b(x_P)$ so that $(x_P, y_P) \in C(\overline{\mathbb{k}})$. It is then easy to check that both partial derivatives vanish at P. Hence, under the conditions of the Lemma, $V(C(x, y))$ is $\overline{\mathbb{k}}$-irreducible and so is an affine variety.

Now that $V(C(x,y))$ is known to be a variety we can consider the dimension. The function field of the affine variety is $\Bbbk(x)(y)$, which is a quadratic algebraic extension of $\Bbbk(x)$ and so has transcendence degree 1. Hence the dimension of is 1. □

The proof of Lemma 10.1.2 shows that a hyperelliptic equation $y^2 + H(x)y - F(x)$ corresponds to a geometrically irreducible curve as long as it does not factorise as $(y - a(x))(y - b(x))$ over $\overline{\Bbbk}[x]$. In practice it is not hard to determine whether or not there exist polynomials $a(x), b(x) \in \overline{\Bbbk}[x]$ such that $H(x) = -a(x) - b(x)$ and $F(x) = -a(x)b(x)$. So determining if a hyperelliptic equation is geometrically irreducible is easy.

Let $H(x), F(x) \in \Bbbk[x]$ be such that $y^2 + H(x)y = F(x)$ is a non-singular affine curve. Define $D = \max\{\deg(F(x)), \deg(H(x)) + 1\}$. The projective closure of C in $\mathbb{P}^2$ is given by

$$y^2 z^{D-2} + z^{D-1} H(x/z)y = z^D F(x/z). \tag{10.1}$$

Exercise 10.1.3. Show that if $D > 2$ then there are at most two points at infinity on the curve of equation (10.1). Show further that if $D > 3$ and $\deg(F) > \deg(H) + 1$ then there is a unique point $(0 : 1 : 0)$ at infinity, which is a singular point.

In Definition 10.1.15 we will define the genus of a hyperelliptic curve in terms of the degree of the hyperelliptic equation. To do this it will be necessary to have conditions that ensure that this degree is minimal. Example 10.1.4 and Exercise 10.1.5 show how a hyperelliptic equation that is a variety can be isomorphic to an equation of significantly lower degree (remember that isomorphism is only defined for varieties).

Example 10.1.4. The curve $y^2 + xy = x^{200} + x^{101} + x^3 + 1$ over $\mathbb{F}_2$ (which is irreducible and non-singular) is isomorphic over $\mathbb{F}_2$ to the curve $Y^2 + xY = x^3 + 1$ via the map $(x, y) \mapsto (x, Y + x^{100})$.

Exercise 10.1.5. Let $\Bbbk$ be any field. Show that the affine algebraic variety $y^2 + (1 - 2x^3)y = -x^6 + x^3 + x + 1$ is isomorphic to a variety having an equation of total degree 2. Show that the resulting curve has genus 0.

Lemma 10.1.6. *Let $\Bbbk$ be a perfect field of characteristic 2 and $h(x), f(x) \in \Bbbk[x]$. Suppose the hyperelliptic equation $C : y^2 + h(x)y = f(x)$ is a variety. Then it is isomorphic over $\Bbbk$ to $Y^2 + H(x)Y = F(x)$ where one of the following conditions hold:*

1. $\deg(F(x)) > 2\deg(H(x))$ *and* $\deg(F(x))$ *is odd;*
2. $\deg(F(x)) = 2\deg(H(x)) = 2d$ *and the equation $u^2 + H_d u + F_{2d}$ has no solution in $\Bbbk$ (where $H(x) = H_d x^d + H_{d-1}x^{d-1} + \cdots + H_0$ and $F(x) = F_{2d}x^{2d} + \cdots + F_0$);*
3. $\deg(F(x)) < \deg(H(x))$.

Proof: Let $d_H = \deg(H(x))$ and $d_F = \deg(F(x))$. The change of variables $y = Y + cx^i$ transforms $y^2 + H(x)y = F(x)$ to $Y^2 + H(x)Y = F(x) + c^2x^{2i} + H(x)cx^i$. Hence, if $\deg(F(x)) > 2\deg(H(x))$ and $\deg(F(x))$ is even then one can remove the leading coefficient by choosing $i = \deg(F(x))/2$ and $c = \sqrt{F_{2i}}$ (remember that $\mathrm{char}(\Bbbk) = 2$ and $\Bbbk$ is perfect so $c \in \Bbbk$). Similarly, if $\deg(H(x)) \leq j = \deg(F(x)) < 2\deg(H(x))$ then one can remove the leading coefficient $F_j x^i$ from F by taking $i = j - \deg(H(x))$ and $c = F_j/H_{d_H}$. Repeating these processes yields the first and third claims. The second case follows easily. □

Note that in the second case in Lemma 10.1.6 one can lower the degree using a $\overline{\Bbbk}$-isomorphism. Hence, geometrically (i.e., over $\overline{\Bbbk}$) one can assume that a hyperelliptic equation is of the form of case 1 or 3.

Example 10.1.7. The affine curve $y^2 + x^3y = x^6 + x + 1$ is isomorphic over $\mathbb{F}_{2^2}$ to $Y^2 + x^3Y = x + 1$ via $Y = y + ux^3$ where $u \in \mathbb{F}_{2^2}$ satisfies $u^2 + u = 1$. (Indeed, these curves are quadratic twists; see Definition 10.2.2.)

Lemma 10.1.8. *Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2$. Every hyperelliptic curve over $\Bbbk$ is isomorphic over $\Bbbk$ to an equation of the form $y^2 + (H_dx^d + \cdots + H_0)y = F_{2d}x^{2d} + F_{2d-1}x^{2d-1} + \cdots + F_0$ where either:*

1. *$H_d = 0$ and ($F_{2d} \neq 0$ or $F_{2d-1} \neq 0$);*
2. *$H_d \neq 0$ and ($F_{2d} \neq -(H_d/2)^2$ or $F_{2d-1} \neq -H_dH_{d-1}/2$).*

Proof: If $H_d = F_{2d} = F_{2d-1} = 0$ then just replace d by $d-1$. If $H_d \neq 0$ and both $F_{2d} = -(H_d/2)^2$ and $F_{2d-1} = -H_dH_{d-1}/2$ then the morphism $(x, y) \mapsto (x, Y = y + \frac{H_d}{2}x^d)$ maps the hyperelliptic equation to

$$(Y - \tfrac{H_d}{2}x^d)^2 + (H_dx^d + \cdots + H_0)(Y - \tfrac{H_d}{2}x^d) - (F_{2d}x^{2d} + F_{2d-1}x^{2d-1} + \cdots + F_0).$$

This can be shown to have the form

$$Y^2 + h(x)Y = f(x)$$

with $\deg(h(x)) \leq d-1$ and $\deg(f(x)) \leq 2d-2$. (This is what happened in Exercise 10.1.5.) □

Exercise 10.1.9. Show that the hyperelliptic curve $y^2 + (2x^3 + 1)y = -x^6 + x^5 + x + 1$ is isomorphic to $Y^2 + Y = x^5 + x^3 + x + 1$.

10.1.1 Projective Models for Hyperelliptic Curves

For the rest of the chapter we will assume that our hyperelliptic equations are $\overline{\Bbbk}$-irreducible and non-singular as affine algebraic sets. We also assume that when $\mathrm{char}(\Bbbk) = 2$ one of the conditions of Lemma 10.1.6 holds and when $\mathrm{char}(\Bbbk) \neq 2$ one of the conditions of Lemma 10.1.8 holds. The interpretation of $\deg(H(x))$ and $\deg(F(x))$ in terms of the genus of the curve will be discussed in Section 10.1.3.

There are several ways to write down a non-singular projective model for a hyperelliptic curve. The simplest is to use weighted projective space.

Definition 10.1.10. Let $\Bbbk$ be a perfect field and $H(x), F(x) \in \Bbbk[x]$. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic equation. Write H_j for the coefficients of $H(x)$ and F_j for the coefficients of $F(x)$. Define $d_H = \deg(H(x))$ and $d_F = \deg(F(x))$. Let $d = \max\{d_H, \lceil d_F/2 \rceil\}$ and suppose $d > 0$. Set $H_d = \cdots = H_{d_H+1} = 0$ and $F_{2d} = \cdots = F_{d_F+1} = 0$ if necessary.

The **weighted projective hyperelliptic equation** is the equation

$$Y^2 + (H_dX^d + H_{d-1}X^{d-1}Z + \cdots + H_0Z^d)Y = F_{2d}X^{2d} + F_{2d-1}X^{2d-1}Z + \cdots + F_0Z^{2d} \quad (10.2)$$

in weighted projective space where X and Z have weight 1 and Y has weight d.

Points (x, y) on the affine equation correspond to points $(x : y : 1)$ on the weighted projective equation. If the original affine algebraic set is non-singular then the corresponding points on the weighted projective model are also non-singular (since singularity is a local property). The map ι on C extends to $\iota(X : Y : Z) = (X : -Y - H(X, Z) : Z)$ where $H(X, Z)$ is the degree d homogenisation of $H(x)$. Points with $Z = 0$ correspond to the points at infinity. Lemma 10.1.11 shows that there are at most two points at infinity on this equation and that they are not singular on this equation.

Lemma 10.1.11. *The points at infinity on equation (10.2) are of the form* $(1 : \alpha : 0)$ *where* $\alpha \in \overline{\Bbbk}$ *satisfies* $\alpha^2 + H_d\alpha - F_{2d} = 0$. *If the conditions of Lemma 10.1.6 or Lemma 10.1.8 hold as appropriate, then the points at infinity are non-singular.*

Proof: Let $Z = 0$. If $X = 0$ then $Y = 0$ (which is not a projective point) so we may assume that $X = 1$. The points at infinity are therefore as claimed.

To study non-singularity, make the problem affine by setting $X = 1$. The equation is

$$C^\dagger : Y^2 + (H_d + H_{d-1}Z + \cdots H_0Z^d)Y = F_{2d} + F_{2d-1}Z + \cdots F_0Z^d. \tag{10.3}$$

The partial derivatives evaluated at $(\alpha, 0)$ are $2\alpha + H_d$ and $H_{d-1}\alpha - F_{2d-1}$. When $\mathrm{char}(\Bbbk) \neq 2$ the point being singular would imply $H_d = -2\alpha$ in which case $F_{2d} = \alpha^2 + H_d\alpha = -\alpha^2 = -(H_d/2)^2$ and $F_{2d-1} = H_{d-1}\alpha = -H_dH_{d-1}/2$. One easily sees that these equations contradict the conditions of Lemma 10.1.8.

When $\mathrm{char}(\Bbbk) = 2$ the point being singular would imply $H_d = 0$ (and so $\alpha^2 = F_{2d}$) and $H_{d-1}\alpha = F_{2d-1}$. First consider the case $F_{2d} = 0$. Then $\alpha = 0$ and so $F_{2d-1} = 0$, but this contradicts the definition of d. Now consider the case $F_{2d} \neq 0$, so that $\alpha \neq 0$. Since $\deg(H(x)) \leq d - 1$ we are in case 1 of Lemma 10.1.6, but then $\deg(F(x))$ must be odd, which is a contradiction. □

Example 10.1.12. Let $\Bbbk$ be a perfect field with $\mathrm{char}(\Bbbk) \neq 2$. The curve $y^2 = F(x)$ where $\deg(F(x))$ is odd has a single point $(1 : 0 : 0)$ at infinity.

Exercise 10.1.13. Let C be a hyperelliptic equation as in Definition 10.0.1. Let $d = \max\{\deg(H(x)), \lceil \deg(F(x))/2 \rceil\}$. Show that the curve $C^\dagger : Y^2 + H(Z)Y = F(Z)$ in equation (10.3) has $\max\{\deg(H(Z)), \lceil \deg(F(Z))/2 \rceil\} = d$.

Theorem 10.1.14 justifies the use of the word "curve".

Theorem 10.1.14. *Let* $C(x, y) = y^2 + H(x)y - F(x)$ *over* $\Bbbk$ *be a hyperelliptic equation that is geometrically irreducible as an affine algebraic set. Suppose there is no point* $P = (x_P, y_P) \in C(\overline{\Bbbk})$ *such that* $(\partial C(x, y)/\partial x)(P) = (\partial C(x, y)/\partial y)(P) = 0$. *Suppose further that the conditions of Lemma 10.1.6 or Lemma 10.1.8 hold as appropriate. Then the associated weighted projective algebraic set of equation (10.2) is geometrically irreducible, has dimension 1, is non-singular, and is birational to the hyperelliptic equation.*

Recall that Lemma 10.1.2 gave some conditions for when the affine algebraic set $V(C(x, y))$ is $\overline{\Bbbk}$-irreducible.

Proof: It follows immediately that the projective algebraic set of equation (10.2) is $\overline{\Bbbk}$-irreducible and has dimension 1. Non-singularity has been explained already. The birational map from the weighted projective equation to C is simply $\phi(X : Y : Z) = (X/Z, Y/Z^d)$. □

From a practical point of view one does not need to work with weighted projective space. Let $C : y^2 + H(x)y = F(x)$ be the original curve and let $C^\dagger$ be the curve of equation (10.3). Consider the birational map $\rho : C \to C^\dagger$ given by $(Z, Y) = \rho(x, y) = (1/x, y/x^d)$. Then C and $C^\dagger$ give two "affine parts" of the projective curve and every point on the curve lies on at least one of these affine algebraic sets. This birational map corresponds to the isomorphism $(X : Y : Z) \mapsto (Z : Y : X)$ from the weighted projective model of C to the weighted projective model of $C^\dagger$.

We can finally give a formal definition for a hyperelliptic curve. Technically, we should distinguish the terms "hyperelliptic equation" and "hyperelliptic curve", since the former is an affine variety whose "obvious" projective closure is singular. In practice, we abuse notation and call the affine hyperelliptic equation a hyperelliptic curve.

Definition 10.1.15. Let $\Bbbk$ be a perfect field. Let $H(x), F(x) \in \Bbbk[x]$ be such that:

- $\deg(H(x)) \geq 3$ or $\deg(F(x)) \geq 5$;
- the affine hyperelliptic equation $y^2+H(x)y = F(x)$ is $\overline{\Bbbk}$-irreducible and non-singular;
- the conditions of Lemma 10.1.6 and Lemma 10.1.8 hold.

The non-singular projective curve of equation (10.2) is called a **hyperelliptic curve**. The **genus** of the hyperelliptic curve is $g = \max\{\deg(H(x))-1, \lfloor \deg(F(x))-1)/2 \rfloor\}$ (see Section 10.1.3 for justification of this).

It looks like Definition 10.1.15 excludes some potentially interesting equations (such as $y^2 + H(x)y = F(x)$ where $\deg(F(x)) = 4$ and $\deg(H(x)) = 2$). In fact, it can be shown that all the algebraic sets excluded by the definition are either $\overline{\Bbbk}$-reducible, singular over $\overline{\Bbbk}$, or birational over $\overline{\Bbbk}$ to a curve of genus 0 or 1 over $\overline{\Bbbk}$.

The equation $\alpha^2 + H_d\alpha - F_{2d} = 0$ in Lemma 10.1.11 can have a $\Bbbk$-rational repeated root, two roots in $\Bbbk$, or two conjugate roots in $\overline{\Bbbk}$. It follows that there are three possible behaviours at infinity: a single $\Bbbk$-rational point, two distinct $\Bbbk$-rational points, a pair of distinct points defined over a quadratic extension of $\Bbbk$ (which are Galois conjugates). These three cases correspond to the fact that the place at infinity in $\Bbbk[x]$ is ramified, split or inert respectively in the field extension $\Bbbk(C)/\Bbbk(x)$. A natural terminology for the three types of behaviour at infinity is therefore to call them ramified, split and inert.

Definition 10.1.16. Let C be a hyperelliptic curve as in Definition 10.1.15. We denote the **points at infinity** on the associated hyperelliptic curve by $\infty^+ = (1 : \alpha^+ : 0)$ and $\infty^- = (1 : \alpha^- : 0)$ (when there is only one point, set $\infty = \infty^+ = \infty^- = (1 : \alpha : 0)$). If there is a single point at infinity then equation (10.2) is called a **ramified model of a hyperelliptic curve**. If there are two distinct points at infinity then when $\alpha^+, \alpha^- \in \Bbbk$ equation (10.2) is called a **split model of a hyperelliptic curve** and when $\alpha^+, \alpha^- \notin \Bbbk$ it is an **inert model of a hyperelliptic curve**.

One finds in the literature the names **imaginary hyperelliptic curve** (respectively, **real hyperelliptic curve**) for ramified model and split model respectively. Exercise 10.1.18 classifies ramified hyperelliptic models. Exercise 10.1.19 shows that if $C(\Bbbk) \neq \varnothing$ then one may transform C into a ramified or split model. Hence, when working over finite fields, it is not usually necessary to deal with curves having an inert model.

Exercise 10.1.17. With notation as in Definition 10.1.16 show that $\iota(\infty^+) = \infty^-$.

Exercise 10.1.18. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve over $\Bbbk$ satisfying all the conditions above. Let $d = \max\{\deg(H(x)), \lceil \deg(F(x))/2 \rceil\}$. Show that this is a ramified model if and only if ($\deg(H(x)) < d$ and $\deg(F(x)) = 2d-1$) or ($\mathrm{char}(\Bbbk) \neq 2$, $\deg(F(x)) = 2d$, $\deg(H(x)) = d$ and $F_{2d} = -(H_d/2)^2$).

Exercise 10.1.19. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve over $\Bbbk$ and let $P \in C(\Bbbk)$. Define the rational map

$$\rho_P(x, y) = (1/(x - x_P), y/(x - x_P)^d).$$

Then $\rho_P : C \to C'$ where C' is also a hyperelliptic curve. Show that ρ_P is just the translation map $P \mapsto (0, y_P)$ followed by the map ρ and so is an isomorphism from C to C'.

Show that if $P = \iota(P)$ then C is birational over $\Bbbk$ (using ρ_P) to a hyperelliptic curve with ramified model. Show that if $P \neq \iota(P)$ then C is birational over $\Bbbk$ to a hyperelliptic curve with split model.

We now indicate a different projective model for hyperelliptic curves.

Exercise 10.1.20. Let the notation and conditions be as above. Assume $C : y^2 + H(x)y = F(x)$ is irreducible and non-singular as an affine curve. Let $Y, X_d, X_{d-1} \ldots, X_1, X_0$ be coordinates for $\mathbb{P}^{d+1}$ (one interprets $X_i = x^i$). The **projective hyperelliptic equation** is the projective algebraic set in $\mathbb{P}^{d+1}$ given by

$$\begin{aligned} Y^2 + (H_dX_d + H_{d-1}X_{d-1} + \cdots + H_0X_0)Y &= F_{2d}X_d^2 + F_{2d-1}X_dX_{d-1} + \cdots + F_1X_1X_0 + F_0X_0^2, \\ X_i^2 &= X_{i-1}X_{i+1}\ , \quad \text{for } 1 \leq i \leq d-1, \\ X_dX_i &= X_{\lceil (d+i)/2 \rceil}X_{\lfloor (d+i)/2 \rfloor}\ , \quad \text{for } 0 \leq i \leq d-2. \end{aligned} \tag{10.4}$$

1. Give a birational map (assuming for the moment that the above model is a variety) between the affine algebraic set C and the model of equation (10.4).
2. Show that the hyperelliptic involution ι extends to equation (10.4) as
$$\iota(Y : X_d : \cdots : X_0) = (-Y - H_dX_d - H_{d-1}X_{d-1} - \cdots - H_0X_0 : X_d : \cdots : X_0)$$
3. Show that the points at infinity on equation (10.4) satisfy $X_0 = X_1 = X_2 = \cdots = X_{d-1} = 0$ and $Y^2 + H_dX_dY - F_{2d}X_d^2 = 0$. Show that if $F_{2d} = H_d = 0$ then there is a single point at infinity.
4. Show that if the conditions of Lemma 10.1.6 or Lemma 10.1.8 hold then equation (10.4) is non-singular at infinity.
5. Show that equation (10.4) is a variety.

10.1.2 Uniformizers on Hyperelliptic Curves

The aim of this section is to determine uniformizers for all points on hyperelliptic curves. We begin in Lemma 10.1.21 by determining uniformizers for the affine points of a hyperelliptic curve.

Lemma 10.1.21. *Let $P = (x_P, y_P) \in C(\Bbbk)$ be a point on a hyperelliptic curve. If $P = \iota(P)$ then $(y - y_P)$ is a uniformizer at P (and $v_P(x - x_P) = 2$). If $P \neq \iota(P)$ then $(x - x_P)$ is a uniformizer at P.*

Proof: We have

$$\begin{aligned} (y - y_P)(y + y_P + H(x_P)) &= y^2 + H(x_P)y - (y_P^2 + H(x_P)y_P) \\ &= F(x) + y(H(x_P) - H(x)) - F(x_P). \end{aligned}$$

Now, use the general fact for any polynomial that $F(x) = F(x_P) + (x - x_P)F'(x_P) \pmod{(x - x_P)^2}$. Hence, the above expression is congruent modulo $(x - x_P)^2$ to

$$(x - x_P)(F'(x_P) - yH'(x_P)) \pmod{(x - x_P)^2}.$$

When $P = \iota(P)$ then $(y - y_P)(y + (y_P + H(x_P))) = (y - y_P)^2$. Note also that $F'(x_P) - y_PH'(x_P)$ is not zero since $2y_P + H(x_P) = 0$ and yet C is not singular. Writing $G(x, y) = (y - y_P)^2/(x - x_P) \in \Bbbk[x, y]$ we have $G(x_P, y_P) \neq 0$ and

$$x - x_P = (y - y_P)^2 \frac{1}{G(x, y)}.$$

Hence, a uniformizer at P is $(y - y_P)$ and $v_P(x - x_P) = 2$.

For the case $P \neq \iota(P)$ note that $v_P(y - y_P) > 0$ and $v_P(y + y_P + H(x_P)) = 0$. It follows that $v_P(y - y_P) \geq v_P(x - x_P)$. □

We now consider uniformizers at infinity on a hyperelliptic curve C over $\Bbbk$. The easiest way to proceed is to use the curve $C^\dagger$ of equation (10.3).

Lemma 10.1.22. *Let C be a hyperelliptic curve and let $\rho : C \to C^\dagger$ be as in equation (10.3). Let $P = \rho(\infty^+) = (0, \alpha^+) \in C^\dagger(\Bbbk)$. If $\iota(\infty^+) = \infty^+$ (i.e., if there is one point at infinity) then $Y - \alpha^+$ is a uniformizer at P on $C^\dagger$ and so $(y/x^d) - \alpha^+$ is a uniformizer at ∞^+ on C. If $\iota(\infty^+) \neq \infty^+$ then Z is a uniformizer at P on $C^\dagger$ (i.e., $1/x$ is a uniformizer at ∞^+ on C).*

Proof: Note that if $\iota(\infty^+) = \infty^+$ then $\iota(P) = P$ and if $\iota(\infty^+) \neq \infty^+$ then $\iota(P) \neq P$. It immediately follows from Lemma 10.1.21 that $Y - \alpha^+$ or Z is a uniformizer at P on $C^\dagger$. Lemma 8.1.13, Exercise 8.2.11 and Lemma 8.2.9 show that for any $f \in \Bbbk(C^\dagger)$ and $P \in C(\Bbbk)$, $v_P(f \circ \rho) = v_{\rho(P)}(f)$. Hence, uniformizers at infinity on C are $(Y - \alpha^+) \circ \rho = (y/x^d) - \alpha^+$ or $Z \circ \rho = 1/x$. □

Exercise 10.1.23. Let C be a hyperelliptic curve in ramified model. Show that $v_\infty(x) = -2$. Show that if the curve has equation $y^2 = F(x)$ where $\deg(F(x)) = 2g + 1$ then x^g/y is an alternative uniformizer at infinity.

Now suppose C is given as a split or inert model. Show that $v_{\infty^+}(x) = v_{\infty^-}(x) = -1$.

Exercise 10.1.24. Let C be a hyperelliptic curve (ramified, split or inert). If $u(x) = (x - x_0)$ is a function on C and $P_0 = (x_0, y_0) \in C(\overline{\Bbbk})$ then $\mathrm{div}(u(x)) = (P_0) + (\iota(P_0)) - (\infty^+) - (\infty^-)$.

Exercise 10.1.25. Let C be a hyperelliptic curve of genus g. Show that if C is in ramified model then $v_\infty(y) = -(2g+1)$ and if C is in split model then $v_{\infty^+}(y) = v_{\infty^-}(y) = -(g+1)$.

Exercise 10.1.26. Let C be a hyperelliptic curve. Let $A(x), B(x) \in \Bbbk[x]$ and let $P = (x_P, y_P) \in C(\overline{\Bbbk})$ be a point on the affine curve. Show that $v_P(A(x) - yB(x))$ is equal to e where $(x - x_P)^e \| (A(x)^2 + H(x)A(x)B(x) - F(x)B(x)^2)$.

Exercise 10.1.27. Describe uniformizers at infinity in terms of the model of equation (10.4).

We now describe a polynomial that will be crucial for arithmetic on hyperelliptic curves with a split model. Essentially, $G^+(x)$ is a function that cancels the pole of y at ∞^+. This leads to another choice of uniformizer at ∞^+ for these models.

Exercise 10.1.28. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve in split model over $\Bbbk$ of genus g. Let $\alpha^+, \alpha^- \in \Bbbk$ be the roots of $Y^2 + H_d Y - F_{2d}$. Show that there exists a polynomial $G^+(x) = \alpha^+ x^d + \cdots \in \Bbbk[x]$ of degree $d = g + 1$ such that $\deg(G^+(x)^2 + H(x)G^+(x) - F(x)) \leq d - 1 = g$. Similarly, show that there is a polynomial $G^-(x) = \alpha^- x^d + \cdots$ such that $\deg(G^-(x)^2 + H(x)G^-(x) - F(x)) \leq d - 1 = g$. Indeed, show that $G^-(x) = -G^+(x) - H(x)$.

Exercise 10.1.29. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve in split model over $\Bbbk$ of genus g and let $G^+(x)$ be as in Exercise 10.1.28. Show that $v_{\infty^+}(y - G^+(x)) \geq 1$.

10.1.3 The Genus of a Hyperelliptic Curve

In Lemma 10.1.6 and Lemma 10.1.8 we showed that some hyperelliptic equations $y^2 + h(x)y = f(x)$ are birational to hyperelliptic equations $y^2+H(x)y = F(x)$ with $\deg(F(x)) < \deg(f(x))$ or $\deg(H(x)) < \deg(h(x))$. Hence, it is natural to suppose that the geometry of the curve C imposes a lower bound on the degrees of the polynomials $H(x)$ and $F(x)$ in its curve equation. The right measure of the complexity of the geometry is the genus.

Indeed, the Riemann-Roch theorem implies that if C is a hyperelliptic curve over $\Bbbk$ of genus g and there is a function $x \in \Bbbk(C)$ of degree 2 then C is birational over $\Bbbk$ to an equation of the form $y^2 + H(x)y = F(x)$ with $\deg(H(x)) \leq g + 1$ and $\deg(F(x)) \leq 2g + 2$. Furthermore, the Hurwitz genus formula shows that if $y^2 + H(x)y = F(x)$ is non-singular and with degrees reduced as in Lemma 10.1.6 and Lemma 10.1.8 then the genus is $\max\{\deg(H(x)) - 1, \lceil \deg(F(x))/2 - 1 \rceil\}$. (Theorem 8.7.3, as it is stated, cannot be applied for hyperelliptic curves in characteristic 2, but a more general version of the Hurwitz genus formula proves the above statement about the genus.) Hence, writing $d = g + 1$, the conditions of Lemma 10.1.6 and Lemma 10.1.8 together with

$$\deg(H(x)) = d \quad \text{or} \quad 2d - 1 \leq \deg(F(x)) \leq 2d \tag{10.5}$$

are equivalent to the curve $y^2 + H(x)y = F(x)$ having genus g.

It is not necessary for us to prove the Riemann-Roch theorem or the Hurwitz genus formula. Our discussion of Cantor reduction (see Lemma 10.3.20 and Lemma 10.4.6) will directly prove a special case of the Riemann-Roch theorem for hyperelliptic curves, namely that every divisor class contains a representative corresponding to an effective divisor of degree at most $g = d - 1$.

The reader should interpret the phrase "hyperelliptic curve of genus g" as meaning the conditions of Lemma 10.1.6 and Lemma 10.1.8 together with equation (10.5) on the degrees of $H(x)$ and $F(x)$ hold.

10.2 Isomorphisms, Automorphisms and Twists

We consider maps between hyperelliptic curves in this section. We are generally interested in isomorphisms over $\overline{\Bbbk}$ rather than just $\Bbbk$.

In the elliptic curve case (see Section 9.3) there was no loss of generality by assuming that isomorphisms fix infinity (since any isomorphism can be composed with a translation map). Since the points on a hyperelliptic curve do not, in general, form a group, one can no longer make this assumption. Nevertheless, many researchers have restricted attention to the special case of maps between curves that map points at infinity (with respect to an affine model of the domain curve) to points at infinity on the image curve. Theorem 10.2.1 classifies this special case.

In this chapter, and in the literature as a whole, isomorphisms are usually not assumed to fix infinity. For example, the isomorphism ρ_P defined earlier in Exercise 10.1.19 does not fix infinity. Isomorphisms that map points at infinity to points at infinity map ramified models to ramified models and unramified models to unramified models.

Theorem 10.2.1. *Let $C_1 : y_1^2 + H_1(x_1)y_1 = F_1(x_1)$ and $C_2 : y_2^2 + H_2(x_2)y_2 = F_2(x_2)$ be hyperelliptic curves over $\Bbbk$ of genus g. Then every isomorphism $\phi : C_1 \to C_2$ over $\Bbbk$ that maps points at infinity of C_1 to points at infinity of C_2 is of the form*

$$\phi(x_1, y_1) = (ux_1 + r, wy_1 + t(x_1))$$

where $u, w, r \in \Bbbk$ and $t \in \Bbbk[x_1]$. If C_1 and C_2 have ramified models then $\deg(t) \leq g$. If C_1 and C_2 have split or inert models then $\deg(t) \leq g + 1$ and the leading coefficient of

$t(x_1)$ is not equal to the leading coefficient of $-wG^+(x_1)$ or $-wG^-(x_1)$ (where G^+ and G^- are as in Exercise 10.1.28).

Proof: (Sketch) The proof is essentially the same as the proof of Proposition 3.1(b) of Silverman [564]; one can also find the ramified case in Proposition 1.2 of Lockhart [392]. One notes that the valuations at infinity of x_1 and x_2 have to agree, and similarly for y_1 and y_2. It follows that x_2 lies in same Riemann-Roch spaces as x_1 and similarly for y_2 and y_1. The result follows (the final conditions are simply that the valuations at infinity of y_1 and y_2 must agree, so we are prohibited from setting $y_2 = w(y_1 + t(x))$ such that it lowers the valuation of y_2). □

We now introduce quadratic twists in the special case of finite fields. As mentioned in Example 9.5.2, when working in characteristic zero there are infinitely many quadratic twists.

Definition 10.2.2. Let $C : y^2 = F(x)$ be a hyperelliptic curve over a finite field $\mathbb{k}$ where $\mathrm{char}(\mathbb{k}) \neq 2$. Let $u \in \mathbb{k}^*$ be a non-square (i.e., there is no $v \in \mathbb{k}^*$ such that $u = v^2$) and define $C^{(u)} : y^2 = uF(x)$.

Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve over a finite field $\mathbb{k}$ where $\mathrm{char}(\mathbb{k}) = 2$. Let $u \in \mathbb{k}$ be such that $\mathrm{Tr}_{\mathbb{k}/\mathbb{F}_2}(u) = 1$. Define $C^{(u)} : y^2 + H(x)y = F(x) + uH(x)^2$.

In both cases the $\mathbb{k}$-isomorphism class of the curve $C^{(u)}$ is called the non-trivial **quadratic twist** of C.

Exercise 10.2.3. Show that the quadratic twist is well-defined when $\mathbb{k}$ is a finite field. In other words, show that in the case $\mathrm{char}(\mathbb{k}) \neq 2$ if u and u' are two different non-squares in $\mathbb{k}^*$ then the corresponding curves $C^{(u)}$ and $C^{(u')}$ as in Definition 10.2.2 are isomorphic over $\mathbb{k}$. Similarly, when $\mathrm{char}\mathbb{k} = 2$ and for two different choices of trace one elements $u, u' \in \mathbb{k}$, show that the corresponding curves $C^{(u)}$ and $C^{(u')}$ are isomorphic over $\mathbb{k}$.

Exercise 10.2.4. Let C be a hyperelliptic curve over a finite field $\mathbb{k}$ and let $C^{(u)}$ be a non-trivial quadratic twist. Show that $\#C(\mathbb{F}_q) + \#C^{(u)}(\mathbb{F}_q) = 2(q+1)$.

Exercise 10.2.5. Let $C : y^2 = F(x)$ be a hyperelliptic curve of genus g over $\mathbb{k}$ (where $\mathrm{char}(\mathbb{k}) \neq 2$). Show that C is isomorphic over $\overline{\mathbb{k}}$ to a curve of the form

$$Y^2 = X(X-1)(X-a_1)(X-a_2)\cdots(X-a_{2g-1})$$

for some $a_1, a_2, \ldots, a_{2g-1} \in \overline{\mathbb{k}}$.

Exercise 10.2.5 indicates that one generally needs $2g-1$ values to specify a hyperelliptic curve of genus g (in fancy terminology: the moduli space of genus g hyperelliptic curves has dimension $2g-1$). It is natural to seek an analogue of the j-invariant for hyperelliptic curves (i.e., some parameters $j_1, \ldots, j_{2g-1}$ associated with each curve C such that C_1 is isomorphic over $\overline{\mathbb{k}}$ to C_2 if and only if the corresponding values $j_1, \ldots, j_{2g-1}$ are equal). Such values have been given by Igusa in the case of genus 2 curves and Shioda [550] for genus 3 curves. It is beyond the scope of this book to present and explain them. We refer to Igusa [304] and Section 5.1.6 of [16] for details of the Igusa invariants.

A natural problem (analogous to Exercise 9.3.7 for the case of elliptic curves) is to write down a genus 2 curve corresponding to a given triple of values for the Igusa invariants. Mestre [420] has given an algorithm to do this for curves over finite fields[1] (for details also see Section 7 of Weng [628]).

We now consider automorphisms. Define $\mathrm{Aut}(C)$ to be the set of all isomorphisms $\phi : C \to C$ over $\overline{\mathbb{k}}$. As usual, $\mathrm{Aut}(C)$ is a group under composition.

[1] It can also be applied over infinite fields.

Lemma 10.2.6. *Let C be a hyperelliptic curve over $\Bbbk$. The hyperelliptic involution commutes with every element of* $\mathrm{Aut}(C)$*. Furthermore, let $\phi : C \to \mathbb{P}^1$ be the canonical morphism $\phi(x,y) = x$. For every automorphism $\psi : C \to C$ there is a linear fractional transformation $\gamma : \mathbb{P}^1 \to \mathbb{P}^1$ (i.e., $\gamma(x) = (ax+b)/(cx+d)$ for some $a,b,c,d \in \Bbbk$ such that $ad - bc \neq 0$) such that the following diagram commutes*

$$\begin{array}{ccc} C & \xrightarrow{\psi} & C \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ \mathbb{P}^1 & \xrightarrow{\gamma} & \mathbb{P}^1 \end{array}$$

Proof: The result follows from Theorem III.7.3 of Farkas and Kra [200] (which uses the notion of Weierstrass points) and Corollaries 2 and 3 on page 102 of [200]. □

Exercise 10.2.7. Prove Lemma 10.2.6 in the special case of automorphisms that map points at infinity to points at infinity. Show that, in this case, γ has no denominator.

Example 10.2.8. Let $p > 2$ be a prime and $C : y^2 = x^p - x$ over $\mathbb{F}_p$. For $a \in \mathbb{F}_p^*, b \in \mathbb{F}_p$ one has isomorphisms

$$\phi_a(x,y) = (ax, \pm\sqrt{a}y) \qquad \text{and} \qquad \psi_{b,\pm}(x,y) = (x+b, \pm y)$$

from C to itself (in both cases they fix the point at infinity). Hence, the subgroup of $\mathrm{Aut}(C)$ consisting of maps that fix infinity is a group of at least $2p(p-1)$ elements.

There is also the birational map $\rho(x,y) = (-1/x, y/x^{(p+1)/2})$ that corresponds to an isomorphism $\rho : C \to C$ on the projective curve. This morphism does not fix infinity. Since all the compositions $\psi_{b',\pm} \circ \rho \circ \psi_{b,\pm} \circ \phi_a$ are distinct one has $2p^2(p-1)$ isomorphisms of this form. Hence, $\mathrm{Aut}(C)$ has size at least $2p(p-1) + 2p^2(p-1) = 2p(p+1)(p-1)$.

Exercise 10.2.9. Let $p > 2$ be a prime and $C : y^2 = x^p - x + 1$ over $\mathbb{F}_p$. Show that the subgroup of $\mathrm{Aut}(C)$ consisting of automorphisms that fix infinity has order $2p$.

Exercise 10.2.10. Let $p > 2$ be a prime and $C : y^2 = x^n + 1$ over $\mathbb{F}_p$ with $n \neq p$ (when $n = p$ the equation is singular). Show that the subgroup of $\mathrm{Aut}(C)$ consisting of automorphisms that fix infinity has order $2n$.

We now give the important Hurwitz-Roquette theorem, which bounds the size of the automorphism group.

Theorem 10.2.11. *(Hurwitz-Roquette) Let C be a curve of genus g over a field $\Bbbk$ such that* $\mathrm{char}(\Bbbk) > g+1$ *and such that C is not isomorphic to the curve of Example 10.2.8. Then* $\#\mathrm{Aut}(C) \leq 84(g-1)$.

Proof: The case $\mathrm{char}(\Bbbk) = 0$ is Exercise IV.2.5 of Hartshorne [278] and the general case is due to Roquette [501]. □

Stichtenoth [587] has given the bound $\#\mathrm{Aut}(C) \leq 16g^4$, which applies even when $\mathrm{char}(\Bbbk) \leq g+1$ for all curves C except the Hermitian curve $y^q + y = x^{q+1}$.

We refer to Chapter 2 of Gaudry's thesis [243] for a classification of $\mathrm{Aut}(C)$ when the genus is two. There are many challenges to determining/classifying $\mathrm{Aut}(C)$ for hyperelliptic curves; we do not attempt a complete analysis of the literature.

Exercise 10.2.12. Let $p \equiv 1 \pmod 8$ and let $C : y^2 = x^5 + Ax$ over $\mathbb{F}_p$. Write $\zeta_8 \in \overline{\mathbb{F}}_p$ for a primitive 8-th root of unity. Show that $\zeta_8 \in \mathbb{F}_{p^4}$. Show that $\psi(x,y) = (\zeta_8^2 x, \zeta_8 y)$ is an automorphism of C. Show that $\psi^4 = \iota$.

10.3 Effective Affine Divisors on Hyperelliptic Curves

This section is about how to represent effective divisors on affine hyperelliptic curves, and algorithms to compute with them. A convenient way to represent divisors is using Mumford representation, and this is only possible if the divisor is semi-reduced.

Definition 10.3.1. Let C be a hyperelliptic curve over $\Bbbk$ and denote by $C \cap \mathbb{A}^2$ the affine curve. An **effective affine divisor** on C is

$$D = \sum_{P \in (C \cap \mathbb{A}^2)(\overline{\Bbbk})} n_P(P)$$

where $n_P \geq 0$ (and, as always, $n_P \neq 0$ for only finitely many P). A divisor on C is **semi-reduced** if it is an effective affine divisor and for all $P \in (C \cap \mathbb{A}^2)(\overline{\Bbbk})$ we have

1. If $P = \iota(P)$ then $n_P \in \{0, 1\}$.
2. If $P \neq \iota(P)$ then $n_P > 0$ implies $n_{\iota(P)} = 0$.

We slightly adjust the notion of equivalence for divisors on $C \cap \mathbb{A}^2$.

Definition 10.3.2. Let C be a hyperelliptic curve over a field $\Bbbk$ and let $f \in \Bbbk(C)$. We define

$$\operatorname{div}(f) \cap \mathbb{A}^2 \ = \sum_{P \in (C \cap \mathbb{A}^2)(\overline{\Bbbk})} v_P(f)(P).$$

Two divisors D, D' on $C \cap \mathbb{A}^2$ are **equivalent**, written $D \equiv D'$, if there is some function $f \in \overline{\Bbbk}(C)$ such that $D = D' + \operatorname{div}(f) \cap \mathbb{A}^2$.

Lemma 10.3.3. *Let C be a hyperelliptic curve. Every divisor on $C \cap \mathbb{A}^2$ is equivalent to a semi-reduced divisor.*

Proof: Let $D = \sum_{P \in C \cap \mathbb{A}^2} n_P(P)$. By Exercise 10.1.24 the function $x - x_P$ has divisor $(P) + (\iota(P))$ on $C \cap \mathbb{A}^2$. If $n_P < 0$ for some $P \in (C \cap \mathbb{A}^2)(\overline{\Bbbk})$ then, by adding an appropriate multiple of $\operatorname{div}(x - x_P)$, one can arrange that $n_P = 0$ (this will increase $n_{\iota(P)}$). Similarly, if $n_P > 0$ and $n_{\iota(P)} > 0$ (or if $P = \iota(P)$ and $n_P \geq 2$) then subtracting a multiple of $\operatorname{div}(x - x_P)$ lowers the values of n_P and $n_{\iota(P)}$. Repeating this process yields a semi-reduced divisor. □

Example 10.3.4. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on a hyperelliptic curve C such that $x_1 \neq x_2$. Let $D = -(P_1) + 2(P_2) + (\iota(P_2))$. Then D is not semi-reduced. One has

$$D + \operatorname{div}(x - x_1) = D + (P_1) + (\iota(P_1)) = (\iota(P_1)) + 2(P_2) + (\iota(P_2)),$$

which is still not semi-reduced. Subtracting $\operatorname{div}(x - x_2)$ from the above gives

$$D + \operatorname{div}((x - x_1)/(x - x_2)) = (\iota(P_1)) + (P_2),$$

which is semi-reduced.

10.3.1 Mumford Representation of Semi-Reduced Divisors

Mumford [445] introduced[2] a representation for semi-reduced divisors. The condition that the divisor is semi-reduced is crucial: if points $P = (x_P, y_P)$ and (x_P, y'_P) with $y_P \neq y'_P$ both appear in the support of the divisor then no polynomial $v(x)$ can satisfy both $v(x_P) = y_P$ and $v(x_P) = y'_P$.

Lemma 10.3.5. *Let $D = \sum_{i=1}^{l} e_i(x_i, y_i)$ be a non-zero semi-reduced divisor on a hyperelliptic curve $C : y^2 + H(x)y = F(x)$ (hence D is affine and effective). Define*

$$u(x) = \prod_{i=1}^{l} (x - x_i)^{e_i} \in \overline{\Bbbk}[x].$$

Then there is a unique polynomial $v(x) \in \overline{\Bbbk}[x]$ such that $\deg(v(x)) < \deg(u(x))$, $v(x_i) = y_i$ for all $1 \leq i \leq l$, and

$$v(x)^2 + H(x)v(x) - F(x) \equiv 0 \pmod{u(x)}. \tag{10.6}$$

In particular, $v(x) = 0$ if and only if $u(x) \mid F(x)$.

Proof: Since D is semi-reduced there is no conflict in satisfying the condition $v(x_i) = y_i$. If all $e_i = 1$ then the result is trivial. For each i such that $e_i > 1$ write $v(x) = y_i + (x - x_i)W(x)$ for some polynomial $W(x)$. We compute $v(x) \pmod{(x - x_i)^{e_i}}$ so it satisfies $v(x)^2 + H(x)v(x) - F(x) \equiv 0 \pmod{(x - x_i)^{e_i}}$ by Hensel lifting (see Section 2.13) as follows: If $v(x)^2 + H(x)v(x) - F(x) = (x - x_i)^j G_j(x)$ then set $v^\dagger(x) = v(x) + w(x - x_i)^j$ where w is an indeterminate and note that

$$v^\dagger(x)^2 + H(x)v^\dagger(x) - F(x) \equiv (x - x_i)^j (G_j(x) + 2v(x)w + H(x)w) \pmod{(x - x_i)^{j+1}}.$$

It suffices to find w such that this is zero, in other words, solve $G_j(x_i) + w(2y_i + H(x_i)) = 0$. Since D is semi-reduced, we know $2y_i + H(x_i) \neq 0$ (since $P = \iota(P)$ implies $n_P = 1$). The result follows by the Chinese remainder theorem. □

Definition 10.3.6. Let D be a non-zero semi-reduced divisor. The polynomials $(u(x), v(x))$ of Lemma 10.3.5 are the **Mumford representation** of D. If $D = 0$ then take $u(x) = 1$ and $v(x) = 0$. A pair of polynomials $u(x), v(x) \in \overline{\Bbbk}[x]$ is called a **Mumford representation** if $u(x)$ is monic, $\deg(v(x)) < \deg(u(x))$ and if equation (10.6) holds.

We have shown that every semi-reduced divisor D has a Mumford representation and that the polynomials satisfying the conditions in Definition 10.3.6 are unique. We now show that one can easily recover an affine divisor D from the pair $(u(x), v(x))$: write $u(x) = \prod_{i=1}^{l} (x - x_i)^{e_i}$ and let $D = \sum_{i=1}^{l} e_i(x_i, v(x_i))$.

Exercise 10.3.7. Show that the processes of associating a Mumford representation to a divisor and associating a divisor to a Mumford representation are inverse to each other. More precisely, let D be a semi-reduced divisor on a hyperelliptic curve. Show that if one represents D in Mumford representation and then obtains a corresponding divisor D' as explained above, then $D' = D$.

[2] Mumford remarks on page 3-17 of [445] that a special case of these polynomials arises in the work of Jacobi. However, Jacobi only gives a representation for semi-reduced divisors with g points in their support, rather than arbitrary semi-reduced divisors.

Exercise 10.3.8. Let $u(x), v(x) \in \mathbb{k}[x]$ be such that equation (10.6) holds. Let D be the corresponding semi-reduced divisor. Show that

$$D = \sum_{P \in (C \cap \mathbb{A}^2)(\overline{\mathbb{k}})} \min\{v_P(u(x)), v_P(y - v(x))\}(P).$$

This is called the **greatest common divisor** of $\mathrm{div}(u(x))$ and $\mathrm{div}(y - v(x))$ and is denoted $\mathrm{div}(u(x), y - v(x))$.

Exercise 10.3.9. Let $(u_1(x), v_1(x))$ and $(u_2(x), v_2(x))$ be the Mumford representations of two semi-reduced divisors D_1 and D_2. Show that if $\gcd(u_1(x), u_2(x)) = 1$ then $\mathrm{Supp}(D_1) \cap \mathrm{Supp}(D_2) = \varnothing$.

Lemma 10.3.10. *Let C be a hyperelliptic curve over $\mathbb{k}$ and let D be a semi-reduced divisor on C with Mumford representation $(u(x), v(x))$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{k})$.*

1. *$\sigma(D)$ is semi-reduced.*
2. *The Mumford representation of $\sigma(D)$ is $(\sigma(u(x)), \sigma(v(x)))$.*
3. *D is defined over $\mathbb{k}$ if and only if $u(x), v(x) \in \mathbb{k}[x]$.*

Exercise 10.3.11. Prove Lemma 10.3.10.

Exercise 10.3.8 shows that the Mumford representation of a semi-reduced divisor D is natural from the point of view of principal divisors. This explains why condition (10.6) is the natural definition for the Mumford representation. There are two other ways to understand condition (10.6). First, the divisor D corresponds to an ideal in the ideal class group of the affine coordinate ring $\mathbb{k}[x, y]$ and condition (10.6) shows this ideal is equal to the $\mathbb{k}[x, y]$-ideal $(u(x), y - v(x))$. Second, from a purely algorithmic point of view, condition (10.6) is needed to make the Cantor reduction algorithm work (see Section 10.3.3).

A divisor class contains infinitely many divisors whose affine part is semi-reduced. Later we will define a reduced divisor to be one whose degree is sufficiently small. One can then consider whether there is a unique such representative of the divisor class. This issue will be considered in Lemma 10.3.24 below.

Exercise 10.3.12 is relevant for the index calculus algorithms on hyperelliptic curves and it is convenient to place it here.

Exercise 10.3.12. A semi-reduced divisor D defined over $\mathbb{k}$ with Mumford representation $(u(x), v(x))$ is said to be a **prime divisor** if the polynomial $u(x)$ is irreducible over $\mathbb{k}$. Show that if D is not a prime divisor, then D can be efficiently expressed as a sum of prime divisors by factoring $u(x)$. More precisely, show that if $u(x) = \prod u_i(x)^{c_i}$ is the complete factorization of $u(x)$ over $\mathbb{k}$, then $D = \sum c_i \mathrm{div}(u_i(x), y - v_i(x))$ where $v_i(x) = v(x) \bmod u_i(x)$.

10.3.2 Addition and Semi-Reduction of Divisors in Mumford Representation

We now present Cantor's algorithm [118][3] for addition of semi-reduced divisors on a hyperelliptic curve C. As above, we take a purely geometric point of view. An alternative,

[3]The generalisation of Cantor's algorithm to all hyperelliptic curves was given by Koblitz [346].

and perhaps more natural, interpretation of Cantor's algorithm is multiplication of ideals in $\Bbbk[x,y] \subset \Bbbk(C)$.

Given two semi-reduced divisors D_1 and D_2 with Mumford representation $(u_1(x), v_1(x))$ and $(u_2(x), v_2(x))$ we want to compute the Mumford representation $(u_3(x), v_3(x))$ of the sum $D_1 + D_2$. Note that we are not yet considering reduction of divisors in the divisor class group. There are two issues that make addition not completely trivial. First, if P is in the support of D_1 and $\iota(P)$ is in the support of D_2 then we remove a suitable multiple of $(P) + (\iota(P))$ from $D_1 + D_2$. Second, we must ensure that the Mumford representation takes multiplicities into account (i.e., so that equation (10.6) holds for $(u_3(x), v_3(x))$).

Example 10.3.13. Let $P = (x_P, y_P)$ on $y^2 + H(x)y = F(x)$ be such that $P \neq \iota(P)$. Let $D_1 = D_2 = (P)$ so that $u_1(x) = u_2(x) = (x - x_P)$ and $v_1(x) = v_2(x) = y_P$. Then $D_1 + D_2 = 2(P)$. The Mumford representation for this divisor has $u_3(x) = (x - x_P)^2$ and $v(x) = y_P + w(x - x_P)$ for some $w \in \overline{\Bbbk}$. To satisfy equation (10.6) one finds that

$$y_P^2 + 2y_P w(x - x_P) + H(x)y_P + wH(x)(x - x_P) - F(x) \equiv 0 \pmod{(x - x_P)^2}.$$

Writing $F(x) \equiv F(x_P) + F'(x_P)(x - x_P) \pmod{(x - x_P)^2}$ and $H(x) \equiv H(x_P) + H'(x_P)(x - x_P) \pmod{(x - x_P)^2}$ gives

$$w = \frac{F'(x_P) - y_P H'(x_P)}{2y_P + H(x_P)},$$

which is defined since $P \neq \iota(P)$.

To help motivate the formula for $v_3(x)$ in Theorem 10.3.14 we now make some observations. First, note that the equation

$$1 = s_1(x)(x - x_P) + s_3(x)(2y_P + H(x))$$

has the solution

$$s_3(x) = \frac{1}{2y_P + H(x_P)} \quad \text{and} \quad s_1(x) = -s_3(x)(H'(x_P) + (x - x_P)G(x))$$

where $G(x) = (H(x) - H(x_P) - H'(x_P)(x - x_P))/(x - x_P)^2$. In other words, we have $H(x) = H(x_P) + (x - x_P)H'(x_P) + (x - x_P)^2 G(x)$. Furthermore, note that

$$v(x) \equiv s_1(x)(x - x_P)y_P + s_3(x)(y_P^2 + F(x)) \pmod{(x - x_P)^2}.$$

The core of Cantor's addition and semi-reduction algorithm is to decide which functions $(x - x_P)$ are needed (and to which powers) to obtain a semi-reduced divisor equivalent to $D_1 + D_2$. The **crucial observation** is that if P is in the support of D_1 and $\iota(P)$ is in the support of D_2 then $(x - x_P) \mid u_1(x), (x - x_P) \mid u_2(x)$ and $v_1(x_P) = -v_2(x_P) - H(x_P)$ and so $(x - x_P) \mid (v_1(x) + v_2(x) + H(x))$. The exact formulae are given in Theorem 10.3.14. The process is called **Cantor's addition algorithm** or **Cantor's composition algorithm**.

Theorem 10.3.14. *Let $(u_1(x), v_1(x))$ and $(u_2(x), v_2(x))$ be Mumford representations of two semi-reduced divisors D_1 and D_2. Let $s(x) = \gcd(u_1(x), u_2(x), v_1(x) + v_2(x) + H(x))$ and let $s_1(x), s_2(x), s_3(x) \in \Bbbk[x]$ be such that*

$$s(x) = s_1(x)u_1(x) + s_2(x)u_2(x) + s_3(x)(v_1(x) + v_2(x) + H(x)).$$

Define $u_3(x) = u_1(x)u_2(x)/s(x)^2$ and

$$v_3(x) = (s_1(x)u_1(x)v_2(x) + s_2(x)u_2(x)v_1(x) + s_3(x)(v_1(x)v_2(x) + F(x)))/s(x). \quad (10.7)$$

Then $u_3(x), v_3(x) \in \Bbbk[x]$ and the Mumford representation of the semi-reduced divisor D equivalent to $D_1 + D_2$ is $(u_3(x), v_3(x))$.

Proof: Let $D = D_1 + D_2 - \mathrm{div}(s(x)) \cap \mathbb{A}^2$ so that D is equivalent to $D_1 + D_2$. By the "crucial observation" above, $s(x)$ has a root x_P for some point $P = (x_P, y_P)$ on the curve if and only if P and $\iota(P)$ lie in the supports of D_1 and D_2. Taking multiplicities into account, it follows that D is semi-reduced.

It is immediate that $s(x)^2 \mid u_1(x)u_2(x)$ and so $u_3(x) \in \Bbbk[x]$. It is also immediate that $u_3(x)$ is the correct first component of the Mumford representation of D.

To show $v_3(x) \in \Bbbk[x]$ rewrite $v_3(x)$ as

$$\begin{aligned} v_3 &= \frac{v_2(s - s_2u_2 - s_3(v_1 + v_2 + H)) + s_2u_2v_1 + s_3(v_1v_2 + F)}{s} && (10.8) \\ &= v_2 + s_2(v_1 - v_2)(u_2/s) + s_3(F - v_2H - v_2^2)/s. && (10.9) \end{aligned}$$

Since $s(x) \mid u_2(x)$ and $u_2(x) \mid (F - v_2H - v_2^2)$ the result follows.

We now need the equation

$$(v_1 + v_2 + H)(v_3 - y) \equiv (y - v_1)(y - v_2) \pmod{u_3}. \tag{10.10}$$

This is proved by inserting the definition of v_3 from equation (10.7) to get

$$\begin{aligned} (v_1 + v_2 + H)(v_3 - y) \equiv\ & -(v_1 + v_2 + H)y + (s_1u_1(v_2^2 + Hv_2 - F) + s_2u_2(v_1^2 + Hv_1 - F) \\ & +(v_1v_2 + F)(s_1u_1 + s_2u_2 + s_3(v_1 + v_2 + H))/s \pmod{u_3(x)}. \end{aligned}$$

Then using $(y - v_1)(y - v_2) = F - (v_1 + v_2 + H)y + v_1v_2$ and $u_i \mid (v_i^2 + Hv_i - F)$ for $i = 1, 2$ proves equation (10.10).

Finally, it remains to prove that equation (10.6) holds. We do this by showing that

$$v_P(v(x)^2 + H(x)v(x) - F(x)) \geq v_P(u(x))$$

for all $P = (x_P, y_P) \in \mathrm{Supp}(D)$. Suppose first that $P \neq \iota(P)$ and that $(x - x_P)^e \| u_3(x)$. Then it is sufficient to show that $v_P(y - v_3(x)) \geq e$. This will follow from equation (10.10). First note that $v_P(y - v_3) = v_P((v_1 + v_2 + H)(v_3 - y))$ and that this is at least $\min\{v_P(u_3), v_P((y - v_1)(y - v_2))\}$. Then $v_P(y - v_1) + v_P(y - v_2) \geq v_P(u_1(x)) + v_P(u_2(x)) \geq e$.

Now for the case $P = \iota(P) \in \mathrm{Supp}(D)$. Recall that such points only occur in semi-reduced divisors with multiplicity 1. Since $u_3(x)$ is of minimal degree we know $(x - x_P) \| u_3(x)$. It suffices to show that $v_3(x_P) = y_P$, but this follows from equation (10.9). Without loss of generality, $P \in \mathrm{Supp}(D_2)$ and $P \notin \mathrm{Supp}(D_1)$ (if $P \in \mathrm{Supp}(D_i)$ for both $i = 1, 2$ then $P \notin \mathrm{Supp}(D)$) so $(x - x_P) \nmid s(x)$, $v_2(x_P) = y_P$ and $(u_2/s)(x_P) = 0$. Hence $v_3(x_P) = v_2(x_P) + 0 = y_P$. □

Exercise 10.3.15. Let $C : y^2 + (x^2 + 2x + 10)y = x^5 + x + 1$ over $\mathbb{F}_{11}$. Let $D_1 = (0, 4) + (6, 4)$ and $D_2 = (0, 4) + (1, 1)$. Determine the Mumford representation of $D_1, D_2, 2D_1, D_1 + D_2$.

We remark that, in practical implementation, one almost always has $\gcd(u_1(x), u_2(x)) = 1$ and so $s(x) = 1$ and the addition algorithm can be simplified. Indeed, it is possible to give explicit formulae for the general cases in the addition algorithm for curves of small genus, we refer to Sections 14.4, 14.5 and 14.6 of [16].

Exercise 10.3.16. Show that the Cantor addition algorithm for semi-reduced divisors of degree $\leq m$ has complexity $O(m^2 M(\log(q))$ bit operations.

10.3.3 Reduction of Divisors in Mumford Representation

Suppose we have an affine effective divisor D with Mumford representation $(u(x), v(x))$. We wish to obtain an equivalent divisor (affine and effective) whose Mumford representation has $\deg(u(x))$ of low degree. We will show in Theorem 10.3.21 and Lemma 10.4.6 that one can ensure $\deg(u(x)) \leq g$, where g is the genus; we will call such divisors reduced. The idea is to consider

$$u^{\dagger}(x) = \text{monic}\left((v(x)^2 + H(x)v(x) - F(x))/u(x)\right) \quad , \quad v^{\dagger}(x) = -v(x) - H(x) \pmod{u^{\dagger}(x)} \tag{10.11}$$

where $\text{monic}\left(u_0 + u_1 x + \cdots + u_k x^k\right)$ for $u_k \neq 0$ is defined to be $(u_0/u_k) + (u_1/u_k)x + \cdots + x^k$. Obtaining $(u^{\dagger}(x), v^{\dagger}(x))$ from $(u(x), v(x))$ is a **Cantor reduction step**. This operation appears in the classical reduction theory of binary quadratic forms.

Lemma 10.3.17. *Let D be an affine effective divisor on a hyperelliptic curve C with Mumford representation $(u(x), v(x))$. Define $(u^{\dagger}(x), v^{\dagger}(x))$ as in equation (10.11). Then $(u^{\dagger}(x), v^{\dagger}(x))$ is the Mumford representation of a semi-reduced divisor $D^{\dagger}$ and $D^{\dagger} \equiv D$ on $C \cap \mathbb{A}^2$.*

Proof: One checks that $(u^{\dagger}(x), v^{\dagger}(x))$ satisfies condition (10.6) and so there is an associated semi-reduced divisor $D^{\dagger}$.

Write $D = (P_1) + \cdots + (P_n)$ (where the same point can appear more than once). Then $\text{div}(y - v(x)) \cap \mathbb{A}^2 = (P_1) + \cdots + (P_n) + (P_{n+1}) + \cdots + (P_{n+m})$ for some points $P_{n+1}, \ldots, P_{n+m}$ (not necessarily distinct from the earlier n points, or from each other) and $\text{div}(v(x)^2 + H(x)v(x) - F(x)) \cap \mathbb{A}^2 = \text{div}((y - v(x))(-y - H(x) - v(x))) \cap \mathbb{A}^2 = (P_1) + (\iota(P_1)) + \cdots + (P_{n+m}) + (\iota(P_{n+m}))$. Now, $\text{div}(u^{\dagger}(x)) = (P_{n+1}) + (\iota(P_{n+1})) + \cdots + (P_{n+m}) + (\iota(P_{n+m}))$. It follows that $D^{\dagger} = (\iota(P_{n+1})) + \cdots + (\iota(P_{n+m}))$ and that $D = D^{\dagger} + \text{div}(y - v(x)) \cap \mathbb{A}^2 - \text{div}(u^{\dagger}(x)) \cap \mathbb{A}^2$. □

Example 10.3.18. Consider

$$C : y^2 = F(x) = x^5 + 2x^4 - 8x^3 + 10x^2 + 40x + 1$$

over $\mathbb{Q}$. Let $P_1 = (-4, 1), P_2 = (-2, 5), P_3 = (0, 1)$ and $D = (P_1) + (P_2) + (P_3)$. The Mumford representation of D is $(u(x), v(x)) = (x(x + 2)(x + 4), -x^2 - 4x + 1)$, which is easily checked by noting that $v(x_{P_i}) = y_{P_i}$ for $1 \leq i \leq 3$.

To reduce D one sets $u^{\dagger}(x) = \text{monic}\left((v(x)^2 - F(x))/u(x)\right) = \text{monic}(-x^2 + 5x - 6) = (x - 3)(x - 2)$ and $v^{\dagger}(x) = -v(x) \pmod{u^{\dagger}(x)} = 9x - 7$.

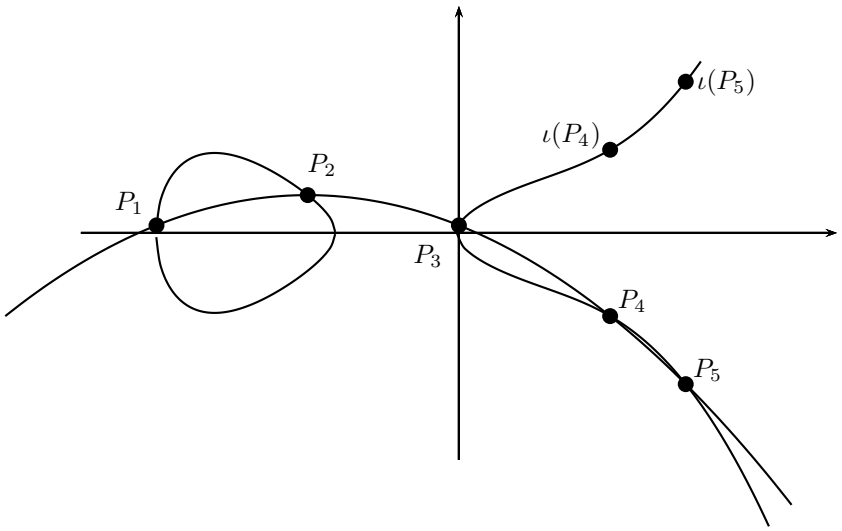
One can check that $\text{div}(y - v(x)) = (P_1) + (P_2) + (P_3) + (P_4) + (P_5)$ where $P_4 = (2, -11)$ and $P_5 = (3, -20)$, that $\text{div}(u^{\dagger}(x)) = (P_4) + (\iota(P_4)) + (P_5) + (\iota(P_5))$ and that $D \equiv \text{div}(u^{\dagger}(x), y - v^{\dagger}(x)) \cap \mathbb{A}^2 = (\iota(P_4)) + (\iota(P_5))$. See Figure 10.1 for an illustration.

Exercise 10.3.19. Show that the straight lines $l(x, y)$ and $v(x)$ in the elliptic curve addition law (Definition 7.9.1) correspond to the polynomials $y - v(x)$ and $u^{\dagger}(x)$ (beware of the double meaning of $v(x)$ here) in a Cantor reduction step.

Lemma 10.3.20. *Let $C : y^2 + H(x)y = F(x)$ and let $(u(x), v(x))$ be the Mumford representation of a semi-reduced divisor D. Write $d_H = \deg(H(x)), d_F = \deg(F(x)), d_u = \deg(u(x))$ and $d_v = \deg(v(x))$. Let $d = \max\{d_H, \lceil d_F/2 \rceil\}$. Let $(u^{\dagger}(x), v^{\dagger}(x))$ be the polynomials arising from a Cantor reduction step.*

1. *If $d_v \geq d$ then $\deg(u^{\dagger}(x)) \leq d_u - 2$.*
2. *If $d_F \leq 2d - 1$ and $d_u \geq d > d_v$ then $\deg(u^{\dagger}(x)) \leq d - 1$ (this holds even if $d_H = d$).*

Figure 10.1: Cantor reduction on a hyperelliptic curve.



3. If $d_F = 2d$ and $d_u > d > d_v$ then $\deg(u^\dagger(x)) \leq d-1$.

Proof: Note that $d_u > d_v$. If $d_v \geq d$ then

$$\deg(v(x)^2 + H(x)v(x) - F(x)) \leq \max\{2d_v, d_H + d_v, d_F\} \leq \max\{2(d_u-1), d+(d_u-1), 2d\}.$$

Hence, $\deg(u^\dagger(x)) = \deg(v^2 + Hv - F) - d_u \leq \max\{d_u - 2, d-1, 2d-d_u\} = d_u - 2$.

If $d_F \leq 2d-1$ and $d_u \geq d > d_v$ then, by a similar argument, $\deg(u^\dagger(x)) \leq 2d - 1 - d_u \leq d-1$. Finally, if $d_F = 2d$ and $d_u > d > d_v$ then $\deg(v^2 + Hv + F) = 2d$ and $\deg(u^\dagger) = 2d - d_u < d$. □

Theorem 10.3.21. *Suppose $C : y^2 + H(x)y = F(x)$ is a hyperelliptic curve of genus g with $\deg(F(x)) \leq 2g+1$. Then every semi-reduced divisor is equivalent to a semi-reduced divisor of degree at most g.*

Proof: Perform Cantor reduction steps repeatedly. By Lemma 10.3.20 the desired condition will eventually hold. □

Theorem 10.3.21 is an "explicit Riemann-Roch theorem" for hyperelliptic curves with a single point at infinity (also for hyperelliptic curves $y^2 + H(x)y = F(x)$ with two points at infinity but $\deg(F(x)) \leq 2g+1$) as it shows that every divisor class contains a representative as an affine effective divisor of degree at most g. The general result is completed in Lemma 10.4.6 below.

Definition 10.3.22. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve of genus g. A semi-reduced divisor on C is **reduced** if its degree is at most g.

Exercise 10.3.23. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve with $d = \max\{\deg(H), \lceil \deg(F)/2 \rceil\}$. Let $(u(x), v(x))$ be the Mumford representation of a divisor with $\deg(v(x)) < \deg(u(x)) < d$. Show that if $\deg(F(x)) \geq 2d-1$ and one performs a Cantor reduction step on $(u(x), v(x))$ then the resulting polynomials $(u^\dagger(x), v^\dagger(x))$ are such that $\deg(u^\dagger(x)) \geq d$.

When $\deg(F) = 2d$ then Lemma 10.3.20 is not sufficient to prove an analogue of Theorem 10.3.21. However, one can at least reduce to a divisor of degree $d = g+1$. It

is notable that performing a Cantor reduction step on a divisor of degree d in this case usually yields another divisor of degree d. This phenomena will be discussed in detail in Section 10.4.2.

We now consider the uniqueness of the reduced divisor of Theorem 10.3.21. Lemma 10.3.24 below shows that non-uniqueness can only arise with split or inert models. It follows that there is a unique reduced divisor in every divisor class for hyperelliptic curves with ramified model. For hyperelliptic curves with split or inert model there is not necessarily a unique reduced divisor.

Lemma 10.3.24. *Let $y^2 + H(x)y = F(x)$ be a hyperelliptic curve over $\Bbbk$ of genus g. Let $d_H = \deg(H(x))$ and $d_F = \deg(F(x))$. Let D_1 and D_2 be semi-reduced divisors of degree at most g. Assume that $D_1 \neq D_2$ but $D_1 \equiv D_2$. Then $d_F = 2g + 2$ or $d_H = g + 1$.*

Proof: First note that $d_H \leq g + 1$ and $d_F \leq 2g + 2$. Let $D_3' = D_1 + \iota_*(D_2)$ so that $D_3' \equiv D_1 - D_2 \equiv 0$ as an affine divisor. Let D_3 be the semi-reduced divisor equivalent to D_3' (i.e., by removing all occurences $(P) + (\iota(P))$). Note that the degree of D_3 is at most $2g$ and that $D_3 \neq 0$. Since $D_3 \equiv 0$ and D_3 is an effective affine divisor we have $D_3 = \mathrm{div}(G(x, y))$ on $C \cap \mathbb{A}^2$ for some non-zero polynomial $G(x, y)$. Without loss of generality $G(x, y) = a(x) - b(x)y$. Furthermore, $b(x) \neq 0$ (since $\mathrm{div}(a(x))$ is not semi-reduced for any non-constant polynomial $a(x)$).

Exercise 10.1.26 shows that the degree of $\mathrm{div}(a(x) - b(x)y)$ on $C \cap \mathbb{A}^2$ is the degree of $a(x)^2 + H(x)a(x)b(x) - F(x)b(x)^2$. We need this degree to be at most $2g$. This is easily achieved if $d_F \leq 2g$ (in which case $d_H = g + 1$ for the curve to have genus g). However, if $2g + 1 \leq d_F \leq 2g + 2$ then we need either $\deg(a(x)^2) = \deg(F(x)b(x)^2)$ or $\deg(H(x)a(x)b(x)) = \deg(F(x)b(x)^2)$. The former case is only possible if d_F is even (i.e., $d_F = 2g + 2$). If $d_F = 2g + 1$ and $d_H \leq g$ then the latter case implies $\deg(a(x)) \geq g + 1 + \deg(b(x))$ and so $\deg(a(x)^2) > \deg(F(x)b(x)^2)$ and $\deg(G(x, y)) > 2g$. □

For hyperelliptic curves of fixed (small) genus it is possible to give explicit formulae for the general cases of the composition and reduction algorithms. For genus 2 curves this was done by Harley [277] (the basic idea is to formally solve for $u^\dagger(x)$ such that $u^\dagger(x)u(x) = \mathrm{monic}(v(x)^2 + H(x)v(x) - F(x))$ as in equation (10.11)). For extensive discussion and details (and also for non-affine coordinate systems for efficient hyperelliptic arithmetic) we refer to Sections 14.4, 14.5 and 14.6 of [16].

10.4 Addition in the Divisor Class Group

We now show how Cantor's addition and reduction algorithms for divisors on the affine curve can be used to perform arithmetic in the divisor class group of the projective curve. A first remark is that Lemma 10.3.3 implies that every degree zero divisor class on a hyperelliptic curve has a representative of the form $D + n^+(\infty^+) + n^-(\infty^-)$ where D is a semi-reduced (hence, affine and effective) divisor and $n^+, n^- \in \mathbb{Z}$ (necessarily, $\deg(D) + n^+ + n^- = 0$).

10.4.1 Addition of Divisor Classes on Ramified Models

On a hyperelliptic curve with ramified model there is only a single point at infinity. We will show in this section that, for such curves, one can compute in the divisor class group using only affine divisors.

We use the Cantor algorithms for addition, semi-reduction, and reduction. In general, if one has a semi-reduced divisor D then, by case 1 of Lemma 10.3.20, a reduction step reduces the degree of D by 2. Hence, at most $\deg(D)/2$ reduction steps are possible.

Theorem 10.4.1. *Let C be a hyperelliptic curve with ramified model. Then every degree 0 divisor class on C has a unique representative of the form $D - n(\infty)$ where D is semi-reduced and where $0 \leq n \leq g$.*

Proof: Theorem 10.3.21 showed that every affine divisor is equivalent to a semi-reduced divisor D such that $0 \leq \deg(D) \leq g$. This corresponds to the degree zero divisor $D - n(\infty)$ where $n = \deg(D)$. Uniqueness was proved in Lemma 10.3.24. □

A degree zero divisor of the form $D - n(\infty)$ where D is a semi-reduced divisor of degree n and $0 \leq n \leq g$ is called **reduced**. We represent D using Mumford representation as $(u(x), v(x))$ and we know that the polynomials $u(x)$ and $v(x)$ are unique. The divisor class is defined over $\Bbbk$ if and only if the corresponding polynomials $u(x), v(x) \in \Bbbk[x]$. Addition of divisors is performed using Cantor's composition and reduction algorithms as above.

Exercise 10.4.2. Let $C : y^2 + H(x)y = F(x)$ be a ramified model of a hyperelliptic curve over $\mathbb{F}_q$. Show that the inverse (also called the negative) of a divisor class on C represented as $(u(x), v(x))$ is $(u(x), -v(x) - (H(x) \pmod{u(x)}))$.

Exercise 10.4.3. Let C be a hyperelliptic curve over $\Bbbk$ of genus g with ramified model. Let D_1 and D_2 be reduced divisors on C. Show that one can compute a reduced divisor representing $D_1 + D_2$ in $O(g^3)$ operations in $\Bbbk$. Show that one can compute $[n]D_1$ in $O(\log(n)g^3)$ operations in $\Bbbk$ (here $[n]D_1$ means the n-fold addition $D_1 + D_1 + \cdots + D_1$).

When the genus is 2 (i.e., $d = 3$) and one adds two reduced divisors (i.e., effective divisors of degree ≤ 2) then the sum is an effective divisor of degree at most 4 and so only one reduction operation is needed to compute the reduced divisor. Similarly, for curves of any genus, at most one reduction operation is needed to compute a reduced divisor equivalent to $D + (P)$ where D is a reduced divisor (such ideas were used by Katagi, Akishita, Kitamura and Takagi [333, 332] to speed up cryptosystems using hyperelliptic curves).

For larger genus there are several variants of the divisor reduction algorithm. In Section 4 of [118], Cantor gives a method that uses higher degree polynomials than $y - v(x)$ and requires fewer reduction steps. In Section VII.2.1 of [65], Gaudry presents a reduction algorithm, essentially due to Lagrange, that is useful when $g \geq 3$. The NUCOMP algorithm (originally proposed by Shanks in the number field setting) is another useful alternative. We refer to Jacobson and van der Poorten [323] and Section VII.2.2 of [65] for details. It seems that NUCOMP should be used once the genus of the curve exceeds 10 (and possibly even for $g \geq 7$).

Exercise 10.4.4. Let C be a hyperelliptic curve of genus 2 over a field $\Bbbk$ with a ramified model. Show that every $\Bbbk$-rational divisor class has a unique representative of one of the following four forms:

1. $(P) - (\infty)$ where $P \in C(\Bbbk)$, including $P = \infty$. Here $u(x) = (x - x_P)$ or $u(x) = 1$.
2. $2(P) - 2(\infty)$ where $P \in C(\Bbbk)$ excluding points P such that $P = \iota(P)$. Here $u(x) = (x - x_P)^2$.
3. $(P) + (Q) - 2(\infty)$ where $P, Q \in C(\Bbbk)$ are such that $P, Q \neq \infty$, $P \neq Q$, $P \neq \iota(Q)$. Here $u(x) = (x - x_P)(x - x_Q)$.
4. $(P) + (\sigma(P)) - 2(\infty)$ where $P \in C(\mathbb{K}) - C(\Bbbk)$ for any quadratic field extension $\mathbb{K}/\Bbbk$, $\mathrm{Gal}(\mathbb{K}/\Bbbk) = \langle\sigma\rangle$ and $\sigma(P) \notin \{P, \iota(P)\}$. Here $u(x)$ is an irreducible quadratic in $\Bbbk[x]$.

Exercise 10.4.5 can come in handy when computing pairings on hyperelliptic curves.

Exercise 10.4.5. Let $D_1 = \mathrm{div}(u_1(x), y - v_1(x)) \cap \mathbb{A}^2$ and $D_2 = \mathrm{div}(u_2(x), y - v_2(x)) \cap \mathbb{A}^2$ be semi-reduced divisors on a hyperelliptic curve with ramified model over $\Bbbk$. Write $d_1 = \deg(u_1(x))$ and $d_2 = \deg(u_2(x))$. Let $D_3 = \mathrm{div}(u_3(x), y - v_3(x)) \cap \mathbb{A}^2$ be a semi-reduced divisor of degree d_3 such that $D_3 - d_3(\infty) \equiv D_1 - d_1(\infty) + D_2 - d_2(\infty)$. Show that if $d_2 = d_3$ then $D_1 - d_1(\infty) \equiv D_3 - D_2$.

10.4.2 Addition of Divisor Classes on Split Models

This section is rather detailed and can safely be ignored by most readers. It presents results of Paulus and Rück [479] and Galbraith, Harrison and Mireles [219].

Let C be a hyperelliptic curve of genus g over $\Bbbk$ with a split model. We have already observed that every degree zero divisor class has a representative of the form $D + n^+(\infty^+) + n^-(\infty^-)$ where D is semi-reduced and $n^+, n^- \in \mathbb{Z}$. Lemma 10.3.20 has shown that we may assume $0 \leq \deg(D) \leq g + 1$. One could consider the divisor to be reduced if this is the case, but this would not be optimal.

The Riemann-Roch theorem implies we should be able to take $\deg(D) \leq g$ but Cantor reduction becomes "stuck" if the input divisor has degree $g+1$. The following simple trick allows us to reduce to semi-reduced divisors of degree g (and this essentially completes the proof of the "Riemann-Roch theorem" for these curves). Recall the polynomial $G^+(x)$ of degree $d = g + 1$ from Exercise 10.1.28.

Lemma 10.4.6. *Let $y^2 + H(x)y = F(x)$ be a hyperelliptic curve of genus g over $\Bbbk$ with split model. Let $u(x), v(x)$ be a Mumford representation such that $\deg(u(x)) = g + 1$. Define*

$$v^\ddagger(x) = G^+(x) + (v(x) - G^+(x) \pmod{u(x)}) \in \Bbbk[x],$$

where we mean that $v(x) - G^+(x)$ is reduced to a polynomial of degree at most $\deg(u(x)) - 1 = g$. Define

$$u^\dagger(x) = \mathrm{monic}\left(\frac{v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x)}{u(x)}\right) \quad \text{and} \quad v^\dagger(x) = -v^\ddagger(x) - H(x) \pmod{u^\dagger(x)}. \tag{10.12}$$

Then $\deg(u^\dagger(x)) \leq g$ and

$$\mathrm{div}(u(x), y - v(x)) \cap \mathbb{A}^2 = \mathrm{div}(u^\dagger(x), y - v^\dagger(x)) \cap \mathbb{A}^2 - \mathrm{div}(u^\dagger(x)) \cap \mathbb{A}^2 + \mathrm{div}(y - v^\ddagger(x)) \cap \mathbb{A}^2. \tag{10.13}$$

Proof: Note that $v^\ddagger(x) \equiv v(x) \pmod{u(x)}$ and so $v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x) \equiv 0 \pmod{u(x)}$, hence $u^\dagger(x)$ is a polynomial. The crucial observation is that $\deg(v^\ddagger(x)) = \deg(G^+(x)) = d = g + 1$ and so the leading coefficient of $v^\ddagger(x)$ agrees with that of $G^+(x)$. Hence $\deg(v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x)) \leq 2d - 1 = 2g + 1$ and so $\deg(u^\dagger(x)) \leq 2d - 1 - d = d - 1 = g$ as claimed. To show equation (10.13) it is sufficient to write $u(x)u^\dagger(x) = \prod_{i=1}^{l}(x - x_i)^{e_i}$ and to note that

$$\begin{aligned} \mathrm{div}(y - v^\ddagger(x)) \cap \mathbb{A}^2 &= \sum_{i=1}^{l} e_i(x_i, v^\ddagger(y_i)) \\ &= \mathrm{div}(u(x), y - v(x)) \cap \mathbb{A}^2 + \mathrm{div}(u^\dagger(x), y + H(x) + v^\dagger(x)) \cap \mathbb{A}^2 \end{aligned}$$

and that $\mathrm{div}(u^\dagger(x)) = \mathrm{div}(u^\dagger(x), y - v^\dagger(x)) + \mathrm{div}(u^\dagger(x), y + v^\dagger(x) + H(x))$. □

Example 10.4.7. Let $C : y^2 = F(x) = x^6 + 6 = (x-1)(x+1)(x-2)(x+2)(x-3)(x+3)$ over $\mathbb{F}_7$. Then $G^+(x) = x^3$. Consider the divisor $D = (1,0) + (-1,0) + (2,0)$ with Mumford representation $(u(x), v(x)) = ((x-1)(x+1)(x-2), 0)$. Performing standard Cantor reduction gives $u^\dagger(x) = F(x)/u(x) = (x+2)(x-3)(x+3)$, which corresponds to the trivial divisor equivalence $D \equiv (-2,0) + (3,0) + (-3,0)$. Instead, we take $v^\ddagger = G^+(x) + (-G^+(x) \pmod{u(x)}) = x^3 + (-x^3 + u(x)) = u(x)$. Then $u^\dagger(x) = \text{monic}\left((v^\ddagger(x)^2 - F(x))/u(x)\right) = x^2 + 5x + 2$ and $v^\dagger(x) = 3x + 5$. The divisor $\text{div}(u^\dagger(x), y - v^\dagger(x)) \cap \mathbb{A}^2$ is a sum $(P) + (\sigma(P))$ where $P \in C(\mathbb{F}_{7^2}) - C(\mathbb{F}_7)$ and σ is the non-trivial element of $\text{Gal}(\mathbb{F}_{7^2}/\mathbb{F}_7)$.

The operation $(u(x), v(x)) \mapsto (u^\dagger(x), v^\dagger(x))$ of equation (10.12) is called **composition and reduction at infinity**; the motivation for this is given in equation (10.18) below. Some authors call it a **baby step**. This operation can be performed even when $\deg(u(x)) < d$, and we analyse it in the general case in Lemma 10.4.14.

Exercise 10.4.8. Let the notation be as in Lemma 10.4.6. Let $d_u = \deg(u(x))$ so that $v^\ddagger(x)$ agrees with $G^+(x)$ for the leading $d - d_u + 1$ coefficients and so $m = \deg(v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x)) \leq d + d_u - 1$. Let $d_{u^\dagger} = \deg(u^\dagger(x))$ so that $m = d_u + d_{u^\dagger}$. Show that $v_{\infty^-}(y - v^\ddagger(x)) = -d$, $\text{div}(y - v^\ddagger(x)) =$

$$\text{div}(u(x), y - v(x)) \cap \mathbb{A}^2 + \text{div}(u^\dagger(x), y + H(x) + v^\dagger(x)) \cap \mathbb{A}^2 - (d_u + d_{u^\dagger} - d)(\infty^+) - d(\infty^-), \tag{10.14}$$

and $v_{\infty^+}(y - v^\ddagger(x)) = -(d_u + d_{u^\dagger} - d)$.

We now discuss how to represent divisor classes. An obvious choice is to represent classes as $D - d(\infty^+)$ where D is an affine effective divisor of degree d (see Paulus and Rück [479] for a full discussion of this case). A more natural representation, as pointed out by Galbraith, Harrison and Mireles [219], is to use balanced representations at infinity. In other words, when g is even, to represent divisor classes as $D - (g/2)((\infty^+) + (\infty^-))$ where D is an effective divisor of degree g.

Definition 10.4.9. Let C be a hyperelliptic curve of genus g over $\Bbbk$ in split model. If g is even then define $D_\infty = \frac{g}{2}((\infty^+) + (\infty^-))$. If g is odd then define $D_\infty = \frac{(g+1)}{2}(\infty^+) + \frac{(g-1)}{2}(\infty^-)$.

Let $u(x), v(x) \in \Bbbk[x]$ be the Mumford representation of a semi-reduced divisor $D = \text{div}(u(x), y - v(x)) \cap \mathbb{A}^2$ and $n \in \mathbb{Z}$. Then $\text{div}(u(x), v(x), n)$ denotes the degree zero divisor

$$D + n(\infty^+) + (g - \deg(u(x)) - n)(\infty^-) - D_\infty.$$

If $0 \leq \deg(u(x)) \leq g$ and $0 \leq n \leq g - \deg(u(x))$ then such a divisor is called **reduced**.

Uniqueness of this representation is shown in Theorem 10.4.19. When g is odd then one could also represent divisor classes using $D_\infty = (g+1)/2((\infty^+) + (\infty^-))$. This is applicable in the inert case too. A problem is that this would lead to polynomials of higher degree than necessary in the Mumford representation, and divisor class representatives would no longer necessarily be unique.

It is important to realise that $u(x)$ and $v(x)$ are only used to specify the affine divisor. The values of $v_{\infty^+}(y - v(x))$ and $v_{\infty^-}(y - v(x))$ have no direct influence over the degree zero divisor under consideration. Note also that we allow $n \in \mathbb{Z}$ in Definition 10.4.9 in general, but reduced divisors must have $n \in \mathbb{Z}_{\geq 0}$.

For hyperelliptic curves with split model then $\infty^+, \infty^- \in \Bbbk$ and so a divisor $(u(x), v(x), n)$ is defined over $\Bbbk$ if and only if $u(x), v(x) \in \Bbbk[x]$. Note that when the genus is even then

D_∞ is $\Bbbk$-rational even when the model is inert, though in this case a divisor $(u(x), v(x), n)$ with $n \neq 0$ is not defined over $\Bbbk$ if $u(x), v(x) \in \Bbbk[x]$.

We may now consider Cantor's addition algorithm in this setting.

Lemma 10.4.10. *Let C be a hyperelliptic curve over $\Bbbk$ of genus g with split model. Let $\mathrm{div}(u_1(x), v_1(x), n_1)$ and $\mathrm{div}(u_2(x), v_2(x), n_2)$ be degree zero divisors as above. Write $D_i = \mathrm{div}(u_i(x), y - v_i(x)) \cap \mathbb{A}^2$ for $i = 1, 2$ and let $D_3 = \mathrm{div}(u_3(x), y - v_3(x)) \cap \mathbb{A}^2$ be the semi-reduced divisor equivalent to $D_1 + D_2$, and $s(x)$ such that $D_1 + D_2 = D_3 + \mathrm{div}(s(x)) \cap \mathbb{A}^2$. Let $m = g/2$ when g is even and $m = (g+1)/2$ otherwise. Then*

$$\mathrm{div}(u_1, v_1, n_1) + \mathrm{div}(u_2, v_2, n_2) \equiv \mathrm{div}(u_3, v_3, n_1 + n_2 + \deg(s) - m). \tag{10.15}$$

Proof: We will show that

$$\mathrm{div}(u_1, v_1, n_1) + \mathrm{div}(u_2, v_2, n_2) = \mathrm{div}(u_3, v_3, n_1 + n_2 + \deg(s) - m) \ + \ \mathrm{div}(s(x)).$$

The left-hand side is

$$D_1 + D_2 + (n_1 + n_2 - m)(\infty^+) + (3m - \deg(u_1) - \deg(u_2) - n_1 - n_2)(\infty^-) \ - \ D_\infty. \tag{10.16}$$

Replacing $D_1 + D_2$ by $D_3 + \mathrm{div}(s(x)) \cap \mathbb{A}^2$ has no effect on the coefficients of ∞^+ or ∞^-, but since we actually need $\mathrm{div}(s(x))$ on the whole of C we have $D_1 + D_2 = D_3 + \mathrm{div}(s(x)) + \deg(s(x))((\infty^+) + (\infty^-))$. Writing $\mathrm{div}(u_3, v_3, n_3) = \mathrm{div}(u_3, y - v_3) \cap \mathbb{A}^2 + n_3(\infty^+) + (g - \deg(u_3) - n_3)(\infty^-) - D_\infty$ gives $n_3 = n_1 + n_2 + \deg(s(x)) - m$ as required.

Note that $\deg(u_3) + \deg(s) = \deg(u_1) + \deg(u_2)$ so the coefficient of ∞^- in equation (10.16) is also correct (as it must be). □

We now discuss reduction of divisors on a hyperelliptic curve with a split model. We first consider the basic Cantor reduction step. There are two relevant cases for split models (namely the first and third cases in Lemma 10.3.20) that we handle as Lemma 10.4.11 and Exercise 10.4.12.

Lemma 10.4.11. *Let $C : y^2 + H(x)y = F(x)$ where $\deg(F(x)) = 2d = 2g + 2$ be a hyperelliptic curve over $\Bbbk$ of genus g with split model. Let $\mathrm{div}(u(x), v(x), n)$ be a degree zero divisor as in Definition 10.4.9. Let $(u^\dagger(x), v^\dagger(x))$ be the polynomials arising from a Cantor reduction step (i.e., $u^\dagger(x)$ and $v^\dagger(x)$ are given by equation (10.11)). If $\deg(v(x)) \geq d = g + 1$ then set $n^\dagger = n + \deg(v(x)) - \deg(u^\dagger(x)) = n + (\deg(u(x)) - \deg(u^\dagger(x)))/2$ and if $\deg(v(x)) < g + 1 < \deg(u(x))$ then set $n^\dagger = n + g + 1 - \deg(u^\dagger(x))$. Then*

$$\mathrm{div}(u, v, n) = \mathrm{div}(u^\dagger, v^\dagger, n^\dagger) + \mathrm{div}(y - v(x)) - \mathrm{div}(u^\dagger(x)) \tag{10.17}$$

and $\mathrm{div}(u, v, n) \equiv \mathrm{div}(u^\dagger, v^\dagger, n^\dagger)$.

Proof: If $\deg(v(x)) \geq d$ then $\deg(u(x)) + \deg(u^\dagger(x)) = 2\deg(v(x))$ and $v_{\infty^+}(y - v(x)) = v_{\infty^-}(y - v(x)) = -\deg(v(x))$. For equation (10.17) to be satisfied we require

$$n = n^\dagger + v_{\infty^+}(y - v(x)) - v_{\infty^+}(u^\dagger(x))$$

and the formula for $n^\dagger$ follows (the coefficients of ∞^- must also be correct, as the divisors all have degree 0).

In the second case of reduction we have $\deg(v(x)) < d < \deg(u(x))$ and hence $\deg(u(x)) + \deg(u^\dagger(x)) = 2d$ and $v_{\infty^+}(y - v(x)) = v_{\infty^-}(y - v(x)) = -d$. The formula for $n^\dagger$ follows as in the first case. □

Exercise 10.4.12. Let $C : y^2 + H(x)y = F(x)$ where $\deg(F(x)) < 2d = 2g + 2$ be a hyperelliptic curve over $\Bbbk$ of genus g with split model. Let $\mathrm{div}(u(x), v(x), n)$ be a degree zero divisor as in Definition 10.4.9 such that $d \leq \deg(u(x))$. Let $(u^\dagger(x), v^\dagger(x))$ be the polynomials arising from a Cantor reduction step. Show that $\mathrm{div}(u, v, n) \equiv \mathrm{div}(u^\dagger, v^\dagger, n^\dagger)$ where, if $\deg(v(x)) < d$ then $n^\dagger = n + g + 1 - \deg(u^\dagger(x))$ and if $\deg(v(x)) \geq d$ then $n^\dagger = n + \deg(v(x)) - \deg(u^\dagger(x))$.

Example 10.4.13. Let $C : y^2 = x^6 + 3$ over $\mathbb{F}_7$. Let $D_1 = \mathrm{div}((x-1)(x-2), 2, 0) = (1, 2) + (2, 2) - D_\infty$ and $D_2 = \mathrm{div}((x-3)(x-4), 2, 0) = (3, 2) + (4, 2) - D_\infty$. Cantor addition gives $D_1 + D_2 = D_3 = \mathrm{div}((x-1)(x-2)(x-3)(x-4), 2, -1)$, which is not a reduced divisor. Applying Cantor reduction to D_3 results in $u^\dagger(x) = (x-5)(x-6)$ and $v^\dagger(x) = -2$ and $n^\dagger = n_3 + (g+1) - \deg(u^\dagger(x)) = -1 + 3 - 2 = 0$. Hence, we have $D_3 \equiv \mathrm{div}((x-5)(x-6), -2, 0)$, which is a reduced divisor.

We now explain the behaviour of a composition at infinity and reduction step.

Lemma 10.4.14. *Let $C : y^2 + H(x)y = F(x)$ where $\deg(F(x)) = 2d = 2g + 2$ be a hyperelliptic curve over $\Bbbk$ of genus g with split model. Let $\mathrm{div}(u(x), v(x), n)$ be a degree zero divisor as in Definition 10.4.9 such that $1 \leq \deg(u(x)) \leq g+1$. Let $v^\ddagger(x)$, $u^\dagger(x)$ and $v^\dagger(x)$ be as in Lemma 10.4.6. Let $n^\dagger = n + \deg(u(x)) - (g+1)$ and $D^\dagger = \mathrm{div}(u^\dagger(x), v^\dagger(x), n^\dagger)$. Then*

$$D = D^\dagger + \mathrm{div}(y - v^\ddagger(x)) - \mathrm{div}(u^\dagger(x)).$$

If one uses $G^-(x)$ in Lemma 10.4.6 then $n^\dagger = n + g + 1 - \deg(u^\dagger(x))$.

It follows that if $\deg(u(x)) = g + 1$ then $\mathrm{div}(u, y - v) \cap \mathbb{A}^2 \equiv \mathrm{div}(u^\dagger, y - v^\dagger) \cap \mathbb{A}^2$ and there is no adjustment at infinity (the point of the operation in this case is to lower the degree from $\deg(u(x)) = g + 1$ to $\deg(u^\dagger(x)) \leq g$). But if, for example, $\deg(u(x)) = \deg(u^\dagger(x)) = g$ then we have

$$\mathrm{div}(u, y - v) \cap \mathbb{A}^2 - D_\infty \equiv \mathrm{div}(u^\dagger, y - v^\dagger) \cap \mathbb{A}^2 + (\infty^+) - (\infty^-) - D_\infty \qquad (10.18)$$

and so the operation corresponds to addition of D with the degree zero divisor $(\infty^-) - (\infty^+)$. This justifies the name "composition at infinity". To add $(\infty^+) - (\infty^-)$ one should use $G^-(x)$ instead of $G^+(x)$ in Lemma 10.4.6.

Exercise 10.4.15. Prove Lemma 10.4.14.

We can finally put everything together and obtain the main result about reduced divisors on hyperelliptic curves with split model.

Theorem 10.4.16. *Let C be a hyperelliptic curve over $\Bbbk$ of genus g with split model. Then every divisor class contains a reduced divisor as in Definition 10.4.9.*

Proof: We have shown the existence of a divisor in the divisor class with semi-reduced affine part, and hence of the form $(u(x), v(x), n)$ with $n \in \mathbb{Z}$. Cantor reduction and composition and reduction at infinity show that we can assume $\deg(u(x)) \leq g$. Finally, to show that one may assume $0 \leq n \leq g - \deg(u(x))$ note that Lemma 10.4.14 maps n to $n^\dagger = n + (g+1) - \deg(u(x))$. Hence, if $n > g - \deg(u(x))$ then $n > n^\dagger \geq 0$ and continuing the process gives a reduced divisor. On the other hand, if $n < 0$ then using $G^-(x)$ instead one has $n^\dagger = n + g + 1 - \deg(u^\dagger(x)) \leq g - \deg(u^\dagger(x))$. □

Exercise 10.4.17. Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve of genus g over $\mathbb{F}_q$ in split model. If g is even, show that the inverse of $\mathrm{div}(u(x), v(x), n)$ is $\mathrm{div}(u(x), -v(x) - (H(x) \pmod{u(x)}), g - \deg(u(x)) - n)$. If g is odd then show that computing the inverse of a divisor may require performing composition and reduction at infinity.

Example 10.4.18. Let $C : y^2 = x^6 + x + 1$ over $\mathbb{F}_{37}$. Then $d = 3$ and $G^+(x) = x^3$. Let $D = (1, 22)+(2, 17)+(\infty^+)-(\infty^-)-D_\infty$, which is represented as $\mathrm{div}(u(x), v(x), 1)$ where $u(x) = (x-1)(x-2) = x^2+34x+2$ and $v(x) = 32x+27$. This divisor is not reduced. Then $v^\ddagger(x) = x^3 + 25x + 33$ and $\deg(v^\ddagger(x)^2 - F(x)) = 4$. Indeed, $v^\ddagger(x)^2 - F(x) = 13u(x)u^\dagger(x)$ where $u^\dagger(x) = x^2 + 28x + 2$. It follows that $v^\dagger(x) = 7x + 22$ and that

$$\mathrm{div}(u(x), v(x), 1) \equiv \mathrm{div}(u^\dagger(x), v^\dagger(x), 0),$$

which is reduced.

Explicit formulae for all these operations for genus 2 curves of the form $y^2 = x^6 + F_4x^4 + F_3x^3 + F_2x^2 + F_1x + F_0$ have been given by Erickson, Jacobson, Shang, Shen and Stein [199].

Uniqueness of the Representation

We have shown that every divisor class for hyperelliptic curves with a split model contains a reduced divisor. We now discuss the uniqueness of this reduced divisor, following Paulus and Rück [479].

Theorem 10.4.19. *Let C be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model. Then every divisor class has a unique representative of the form*

$$D + n(\infty^+) + (g - \deg(D) - n)(\infty^-) - D_\infty$$

where D is a semi-reduced divisor (hence, affine and effective) and $0 \leq n \leq g - \deg(D)$.

Proof: Existence has already been proved using the reduction algorithms above, so it suffices to prove uniqueness. Hence, suppose

$$D_1+n_1(\infty^+)+(g-\deg(D_1)-n_1)(\infty^-)-D_\infty \equiv D_2+n_2(\infty^+)+(g-\deg(D_2)-n_2)(\infty^-)-D_\infty$$

with all terms satisfying the conditions of the theorem. Then, taking the difference and adding $\mathrm{div}(u_2(x)) = D_2 + \iota(D_2) - \deg(D_2)((\infty^+) + (\infty^-))$, there is a function $f(x, y)$ such that

$$\mathrm{div}(f(x, y)) = D_1 + \iota(D_2) - (n_2 + \deg(D_2) - n_1)(\infty^+) - (n_1 + \deg(D_1) - n_2)(\infty^-).$$

Since $f(x, y)$ has poles only at infinity it follows that $f(x, y) = a(x) + yb(x)$ where $a(x), b(x) \in \mathbb{k}[x]$. Now, $0 \leq n_i \leq n_i + \deg(D_i) \leq g$ and so $-g \leq v_{\infty^+}(f(x, y)) = -(n_2 + \deg(D_2) - n_1) \leq g$ and $-g \leq v_{\infty^-}(f(x, y)) = -(n_1 + \deg(D_1) - n_2) \leq g$. But $v_{\infty^+}(y) = v_{\infty^-}(y) = -(g + 1)$ and so $b(x) = 0$ and $f(x, y) = a(x)$. But $\mathrm{div}(a(x)) = D+\iota(D)-\deg(a(x))((\infty^+)+(\infty^-))$ and so $D_1 = D_2$, $n_1+\deg(D_1)-n_2 = n_2+\deg(D_2)-n_1$ and $n_1 = n_2$. □

Exercise 10.4.20. Let C be a hyperelliptic curve over $\mathbb{k}$ of genus $g = d - 1$ with split model. Show that $(\infty^+) - (\infty^-)$ is not a principal divisor and that this divisor is represented as $(1, 0, \lceil g/2 \rceil + 1)$.

If $\mathbb{k} = \mathbb{F}_q$ is a finite field then $(\infty^+) - (\infty^-)$ has finite order. We write $R \in \mathbb{N}$ for the order of $(\infty^+) - (\infty^-)$ and call it the **regulator**. Since $R((\infty^+) - (\infty^-))$ is a principal divisor there is some function $f(x, y) \in \mathbb{k}(C)$ such that $\mathrm{div}(f) = R((\infty^+) - (\infty^-))$. It follows that $f(x, y) \in \mathbb{k}[x, y]$ (otherwise it would have some affine pole) and is a unit in the ring $\mathbb{k}[x, y]$. The polynomial $f(x, y)$ is called the fundamental unit of the ring $\mathbb{k}[x, y]$ (this is analogous to the fundamental unit of a real quadratic number field).

Exercise 10.4.21. Show that $R \geq g+1$.

Exercise 10.4.22. Let C be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model and let $P \in C(\mathbb{k})$ be such that $P \neq \iota(P)$. Show that the order of the divisor $(P) - (\iota(P))$ is always at least $g+1$.

10.5 Jacobians, Abelian Varieties and Isogenies

As mentioned in Section 7.8, we can consider $\mathrm{Pic}^0_{\mathbb{k}}(C)$ as an algebraic group, by considering the **Jacobian variety** J_C of the curve. The fact that the divisor class group is an algebraic group is not immediate from our description of the group operation as an algorithm (rather than a formula).

Indeed, J_C is an Abelian variety (namely, a projective algebraic group). The dimension of the variety J_C is equal to the genus of C. Unfortunately, we do not have space to introduce the theory of Abelian varieties and Jacobians in this book. We remark that the Mumford representation directly gives an affine part of the Jacobian variety of a hyperelliptic curve (see Propositions 1.2 and 1.3 of Mumford [445] for the details).

An explicit description of the Jacobian variety of a curve of genus 2 has been given by Flynn; we refer to Chapter 2 of Cassels and Flynn [123] for details, references and further discussion.

There are several important concepts in the theory of Abelian varieties that are not able to be expressed in terms of divisor class groups.[4] Hence, our treatment of hyperelliptic curves will not be as extensive as the case of elliptic curves. In particular, we do not give a rigorous discussion of isogenies (i.e., morphisms of varieties that are group homomorphisms with finite kernel) for Abelian varieties of dimension $g > 1$. However, we do mention one important result. The Poincaré reducibility theorem (see Theorem 1 of Section 19 (page 173) of Mumford [444]) states that if A is an Abelian variety over $\mathbb{k}$ and B is an Abelian subvariety of A (i.e., B is a subset of A that is an Abelian variety over $\mathbb{k}$), then there is an Abelian subvariety $B' \subseteq A$ over $\mathbb{k}$ such that $B \cap B'$ is finite and $B + B' = A$. It follows that A is isogenous over $\mathbb{k}$ to $B \times B'$. If an Abelian variety A over $\mathbb{k}$ has no Abelian subvarieties over $\mathbb{k}$ then we call it **simple**. An Abelian variety is **absolutely simple** if is has no Abelian subvarieties over $\overline{\mathbb{k}}$.

Despite not discussing isogenies in full generality, it is possible to discuss isogenies that arise from maps between curves purely in terms of divisor class groups. We now give some examples, but first introduce a natural notation.

Definition 10.5.1. Let C be a curve over a field $\mathbb{k}$ and let $n \in \mathbb{N}$. For $D \in \mathrm{Pic}^0_{\mathbb{k}}(C)$ define

$$[n]D = D + \cdots + D \quad (n \text{ times}).$$

Indeed, we usually assume that $[n]D$ is a reduced divisor representing the divisor class nD. Define

$$\mathrm{Pic}^0_{\mathbb{k}}(C)[n] = \{D \in \mathrm{Pic}^0_{\mathbb{k}}(C) : [n]D = 0\}.$$

Recall from Corollary 8.3.10 that if $\phi : C_1 \to C_2$ is a non-constant rational map (and hence a non-constant morphism) over $\mathbb{k}$ between two curves then there are corresponding group homomorphisms $\phi^* : \mathrm{Pic}^0_{\mathbb{k}}(C_2) \to \mathrm{Pic}^0_{\mathbb{k}}(C_1)$ and $\phi_* : \mathrm{Pic}^0_{\mathbb{k}}(C_1) \to \mathrm{Pic}^0_{\mathbb{k}}(C_2)$. Furthermore, by part 5 of Theorem 8.3.8 we have $\phi_*\phi^*(D) = [\deg(\phi)]D$ on $\mathrm{Pic}^0_{\mathbb{k}}(C_2)$.

[4] There are two reasons for this: first the divisor class group is merely an abstract group and so does not have the geometric structure necessary for some of these concepts; second, not every Abelian variety is a Jacobian variety.

In the special case of a non-constant rational map $\phi : C \to E$ over $\Bbbk$ where E is an elliptic curve we can compose with the Abel-Jacobi map $E \to \mathrm{Pic}^0_{\Bbbk}(E)$ of Theorem 7.9.8 given by $P \mapsto (P) - (\mathcal{O}_E)$ to obtain group homomorphisms that we call $\phi^* : E \to \mathrm{Pic}^0_{\Bbbk}(C)$ and $\phi_* : \mathrm{Pic}^0_{\Bbbk}(C) \to E$.

Exercise 10.5.2. Let $\phi : C \to E$ be a non-constant rational map over $\Bbbk$ where E is an elliptic curve over $\Bbbk$. Let $\phi^* : E \to \mathrm{Pic}^0_{\Bbbk}(C)$ and $\phi_* : \mathrm{Pic}^0_{\Bbbk}(C) \to E$ be the group homomorphisms as above. Show that ϕ_* is surjective as a map from $\mathrm{Pic}^0_{\Bbbk}(C)$ to $E(\overline{\Bbbk})$ and that the kernel of ϕ^* is contained in $E[\deg(\phi)]$.

If C is a curve of genus 2 and there are two non-constant rational maps $\phi_i : C \to E_i$ over $\overline{\Bbbk}$ for elliptic curves E_1, E_2 then one naturally has a group homomorphism $\phi_{1,*} \times \phi_{2,*} : \mathrm{Pic}^0_{\Bbbk}(C) \to E_1(\overline{\Bbbk}) \times E_2(\overline{\Bbbk})$. If $\ker(\phi_{1,*}) \cap \ker(\phi_{2,*})$ is finite then it follows from the theory of Abelian varieties that the Jacobian variety J_C is isogenous to the product $E_1 \times E_2$ of the elliptic curves and one says that J_C is a **split Jacobian**.

Example 10.5.3. Let $C : y^2 = x^6 + 2x^2 + 1$ be a genus 2 curve over $\mathbb{F}_{11}$. Consider the rational maps

$$\phi_1 : C \to E_1 : Y^2 = X^3 + 2X + 1$$

given by $\phi_1(x, y) = (x^2, y)$ and

$$\phi_2 : C \to E_2 : Y^2 = X^3 + 2X^2 + 1$$

given by $\phi_2(x, y) = (1/x^2, y/x^3)$. The two elliptic curves E_1 and E_2 are neither isomorphic or isogenous. One has $\#E_1(\mathbb{F}_{11}) = 16$, $\#E_2(\mathbb{F}_{11}) = 14$ and $\#\mathrm{Pic}^0_{\mathbb{F}_{11}}(C) = 14 \cdot 16$.

It can be shown (this is not trivial) that $\ker(\phi_{1,*}) \cap \ker(\phi_{2,*})$ is finite. Further, since $\deg(\phi_1) = \deg(\phi_2) = 2$ it can be shown that the kernel of $\phi_{1,*} \times \phi_{2,*}$ is contained in $\mathrm{Pic}^0_{\Bbbk}(C)[2]$.

The Jacobian of a curve satisfies the following universal property. Let $\phi : C \to A$ be a morphism, where A is an Abelian variety. Let $P_0 \in C(\overline{\Bbbk})$ be such that $\phi(P_0) = 0$ and consider the Abel-Jacobi map $\psi : C \to J_C$ (corresponding to $P \mapsto (P) - (P_0)$). Then there is a homomorphism of Abelian varieties $\phi' : J_C \to A$ such that $\phi = \phi' \circ \psi$. Exercise 10.5.4 gives a special case of this universal property.

Exercise 10.5.4. Let $C : y^2 = x^6 + a_2x^4 + a_4x^2 + a_6$ over $\Bbbk$, where $\mathrm{char}(\Bbbk) \neq 2$, and let $\phi(x, y) = (x^2, y)$ be non-constant rational map $\phi : C \to E$ over $\Bbbk$ where E is an elliptic curve. Let $P_0 \in C(\overline{\Bbbk})$ be such that $\phi(P_0) = \mathcal{O}_E$. Show that the composition

$$C(\overline{\Bbbk}) \to \mathrm{Pic}^0_{\Bbbk}(C) \to E(\overline{\Bbbk}),$$

where the first map is the Abel-Jacobi map $P \mapsto (P) - (P_0)$ and the second map is ϕ_*, is just the original map ϕ.

Exercise 10.5.5. Let $a_3, a_5 \in \Bbbk$, where $\mathrm{char}(\Bbbk) \neq 2$. This exercise gives maps over $\overline{\Bbbk}$ from the genus 2 curve $C : y^2 = x^5 + a_3x^3 + a_5x$ to elliptic curves.

Choose $\alpha, \beta \in \overline{\Bbbk}$ such that $a_5 = \alpha^2\beta^2$ and $a_3 = -(\alpha^2 + \beta^2)$. In other words,

$$x^4 + a_3x^2 + a_5 = (x^2 - \alpha^2)(x^2 - \beta^2) = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta).$$

Set $s = \sqrt{\alpha\beta}$, $A = (1 + (\alpha + \beta)/(2s))/2$ and $B = (1 - (\alpha + \beta)/(2s))/2$. Show that $A(x + s)^2 + B(x - s)^2 = x^2 + (\alpha + \beta)x + s^2$, $B(x + s)^2 + A(x - s)^2 = x^2 - (\alpha + \beta)x + s^2$ and $(x + s)^2 - (x - s)^2 = 4sx$. Hence, show that

$$x(x^4 + a_3x^2 + a_5) = \frac{((x + s)^2 - (x - s)^2)}{4s}(A(x + s)^2 + B(x - s)^2)(B(x + s)^2 + A(x - s)^2).$$

Now, set $Y = y/(x-s)^3$ and $X = ((x+s)/(x-s))^2$. Show that

$$Y^2 = (X-1)/(4s)(AX+B)(BX+A) = \frac{AB}{4s}(X-1)(X^2 + (B/A + A/B)X + 1).$$

Calling the above curve E_1, the rational map $\phi_1(x,y) = (X,Y)$ maps C to E_1. Similarly, taking $Y = y/(x+s)^3$ and $X = ((x-s)/(x+s))^2$ gives an elliptic curve $E_2 : Y^2 = -(X-1)/(4s)(BX+A)(AX+B)$ and a rational map $\phi_2 : C \to E_2$. Note that E_2 is a quadratic twist of E_1.

There is a vast literature on split Jacobians and we are unable to give a full survey. We refer to Sections 4, 5 and 6 of Kuhn [356] or Chapter 14 of Cassels and Flynn [123] for further examples.

10.6 Elements of Order n

We now bound the size of the set of elements of order dividing n in the divisor class group of a curve. As with many other results in this chapter, the best approach is via the theory of Abelian varieties. We state Theorem 10.6.1 for general curves, but without proof. The result is immediate for Abelian varieties over $\mathbb{C}$, as they are isomorphic to $\mathbb{C}^g/L$ where L is a rank $2g$ lattice. The elements of order n in $\mathbb{C}^g/L$ are given by the n^{2g} points in $\frac{1}{n}L/L$.

Theorem 10.6.1. *Let C be a curve of genus g over $\Bbbk$ and let $n \in \mathbb{N}$. If $\mathrm{char}(\Bbbk) = 0$ or $\gcd(n, \mathrm{char}(\Bbbk)) = 1$ then $\#\mathrm{Pic}^0_{\Bbbk}(C)[n] = n^{2g}$. If $\mathrm{char}(\Bbbk) = p > 0$ then $\#\mathrm{Pic}^0_{\Bbbk}(C)[p] = p^e$ where $0 \leq e \leq g$.*

Proof: See Theorem 4 of Section 7 of Mumford [444]. □

We now present a special case of Theorem 10.6.1 (at least, giving a lower bound), namely elements of order 2 in the divisor class group of a hyperelliptic curve with a ramified model.

Lemma 10.6.2. *Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) \neq 2$. Let $F(x) \in \Bbbk[x]$ be a monic polynomial of degree $2g+1$ and let $C : y^2 = F(x)$. Let d be the number of roots of $F(x)$ over $\Bbbk$. Let $B_{\Bbbk} = \{(x_1, 0), \ldots, (x_d, 0)\}$ where $x_1, \ldots, x_d \in \Bbbk$ are the roots of $F(x)$ in $\Bbbk$.*

If $d \neq 2g+1$ then $B_{\Bbbk}$ generates a subgroup of $\mathrm{Pic}^0_{\Bbbk}(C)$ of exponent 2 and order 2^d. If $d = 2g+1$ then $B_{\Bbbk}$ generates a subgroup of $\mathrm{Pic}^0_{\Bbbk}(C)$ of exponent 2 and order 2^{2g}.

Exercise 10.6.3. Prove Lemma 10.6.2 via the following method.

1. First, consider $B_{\overline{\Bbbk}} = \{P_1, \ldots, P_{2g+1}\}$ and for any subset $T \subset \{1, \ldots, 2g+1\}$ define
$$D_T = \sum_{j \in T} (P_j) - \#T(\infty).$$
Show that D_T has order 2 in $\mathrm{Pic}^0_{\overline{\Bbbk}}(C)$.

2. For $T \subset \{1, \ldots, 2g+1\}$ we define the **complement** $T' = \{1, \ldots, 2g+1\} - T$ (so that $T \cap T' = \varnothing$ and $T \cup T' = \{1, \ldots, 2g+1\}$). Show that $D_{T_1} + D_{T_2} \equiv D_{T_3}$ where $T_3 = T_1 \cup T_2 - (T_1 \cap T_2)$. Show (using Lemma 10.3.24 and other results) that $D_{T_1} \equiv D_{T_2}$ if and only if $T_1 = T_2$ or $T_1 = T_2'$.

3. Hence, deduce that the subgroup generated by $B_{\Bbbk}$ consists only of divisor classes represented by reduced divisors with support in $B_{\overline{\Bbbk}}$. Complete the proof by counting such divisor classes (note that if $d < 2g+1$ then $T \subset B_{\Bbbk}$ implies $T' \not\subset B_{\Bbbk}$).

Lemma 10.6.2 describes 2^{2g} divisor classes over $\overline{\Bbbk}$ of order dividing 2. Since Theorem 10.6.1 states that there are exactly 2^{2g} such divisor classes over $\overline{\Bbbk}$ it follows that every 2-torsion divisor class has a representative of this form. A corollary is that any function $f \in \overline{\Bbbk}(C)$ with divisor $\mathrm{div}(f) = 2(P_1) + 2(P_2) - 4(\infty)$ is equal to $c(x - x_1)(x - x_2)$ for some $c, x_1, x_2 \in \overline{\Bbbk}$.

A determination of the 2-torsion in Jacobians of hyperelliptic curves over finite fields is given by Cornelissen; see [147] and its erratum.

Division Ideals

In some applications (particularly when generalising Schoof's algorithm for point counting) it is desired to determine the elements of a given order in the divisor class group. It is therefore necessary to have an analogue of the elliptic curve division polynomials. Early attempts on this problem, in the context of point counting algorithms, appear in the work of Pila and Kampkötter.

We sketch some results of Cantor [119]. Let $C : y^2 = F(x)$ over $\Bbbk$ be such that $F(x)$ is monic of degree $2g + 1$ and $\mathrm{char}(\Bbbk) \neq 2$ (though Section 9 of [119] does discuss how to proceed when $\mathrm{char}(\Bbbk) = 2$). Cantor defines polynomials ψ_n for $n \geq g + 1$ such that for $P = (x_P, y_P) \in C(\overline{\Bbbk})$ we have $\psi_n(x_P, y_P) = 0$ if and only if $n((x_P, y_P) - (\infty))$ lies in the set Θ of all divisor classes with a Mumford representative of the form $\mathrm{div}(u(x), y - v(x))$ having $\deg(u(x)) \leq g - 1$. While points $P \in C(\overline{\Bbbk})$ such that $[n]((P) - (\infty))$ is principal will be roots of these polynomials, we stress that these polynomials do have other roots as well. Also, since most divisor classes do not have representatives of the form $(P) - (\infty)$ for a point P on the curve when $g > 1$, in general there are divisor classes of order n that are not of this form. Equation (8.1) of [119] gives explicit recurrence formulae for ψ_n in the case when $g = 2$. Section 10 of [119] gives the first few values of $\psi_n(x, y)$ for the genus 2 curve $y^2 = x^5 + 1$.

Let C be a genus 2 curve. Note that if $D = (x_1, y_1) + (x_2, y_2) - 2(\infty)$ has order n then either $[n]((x_i, y_i) - (\infty)) \equiv 0$ or $[n]((x_1, y_1) - (\infty)) \equiv -[n]((x_2, y_2) - (\infty))$. Hence one can find general divisors of order n using formulae for computing $[n]((x, y) - (\infty))$ and equating polynomials. In other words, to determine divisors of order n it is sufficient to obtain rational functions that give the Mumford representation of $[n]((x, y) - (\infty))$.

Let $n \in \mathbb{N}$ and let C be a genus 2 curve over $\Bbbk$ in ramified model. There are polynomials $d_{n,0}(x), d_{n,1}(x), d_{n,2}(x), e_{n,0}(x), e_{n,1}(x), e_{n,2}(x) \in \Bbbk[x]$ of degrees respectively $2n^2 - 3$, $2n^2 - 2$, $2n^2 - 1$, $3n^2 - 2$, $3n^2 - 3$, $3n^2 - 2$ such that, for a "generic point" $P = (x_P, y_P) \in C(\overline{\Bbbk})$, the Mumford representation of $[n]((x_P, y_P) - (\infty))$ is

$$\left(x^2 + \frac{d_{n,1}(x_P)}{d_{n,0}(x_P)} x + \frac{d_{n,2}(x_P)}{d_{n,0}(x_P)}, y_P \left(\frac{e_{1,n}(x_P)}{e_{0,n}(x_P)} x + \frac{e_{2,n}(x_P)}{e_{0,n}(x_P)} \right) \right).$$

Indeed, this can be checked directly for any curve C and any prime n by computing Cantor's algorithm in a computer algebra package. These formulae are not necessarily valid for all points $P \in C(\Bbbk)$ (such as those for which $n((x_P, y_P) - (\infty)) \equiv 0$). For details we refer to Gaudry's theses (Section 4.4 of [241] and Section 7.2 of [243]). Information about the use of these, and other, ideals in point counting algorithms is given in Section 3 of Gaudry and Schost [248].

10.7 Hyperelliptic Curves Over Finite Fields

There are a finite number of points on a curve C of genus g over a finite field $\mathbb{F}_q$. There are also finitely many possible values for the Mumford representation of a reduced divisor

on a hyperelliptic curve over a finite field. Hence, the divisor class group $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ of a curve over a finite field is a finite group. Since the affine part of a reduced divisor is a sum of at most g points (possibly defined over a field extension of degree bounded by g) it is not surprising that there is a connection between $\{\#C(\mathbb{F}_{q^i}) : 1 \leq i \leq g\}$ and $\#\mathrm{Pic}^0_{\mathbb{F}_q}(C)$. Indeed, there is also a connection between $\{\#\mathrm{Pic}^0_{\mathbb{F}_{q^i}}(C) : 1 \leq i \leq g\}$ and $\#C(\mathbb{F}_q)$. The aim of this section is to describe these connections. We also give some important bounds on these numbers (analogous to the Hasse bound for elliptic curves). Most results are presented for general curves (i.e., not only hyperelliptic curves).

One of the most important results in the theory of curves over finite fields is the following theorem of Hasse and Weil. The condition that the roots of $L(t)$ have absolute value $\sqrt{q}$ can be interpreted as an analogue of the Riemann hypothesis. This result gives precise bounds on the number of points on curves and divisor class groups over finite fields.

Theorem 10.7.1. *(Hasse-Weil) Let C be a curve of genus g over $\mathbb{F}_q$. There exists a polynomial $L(t) \in \mathbb{Z}[t]$ of degree $2g$ with the following properties.*

1. $L(1) = \#\mathrm{Pic}^0_{\mathbb{F}_q}(C)$.
2. *One can write $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ with $\alpha_i \in \mathbb{C}$ such that $\alpha_{g+i} = \overline{\alpha_i}$ (this is complex conjugation) and $|\alpha_i| = \sqrt{q}$ for $1 \leq i \leq g$.*
3. *$L(t) = q^g t^{2g} L(1/(qt))$ and so*
$$L(t) = 1 + a_1 t + \cdots + a_{g-1}t^{g-1} + a_g t^g + q a_{g-1} t^{g+1} + \cdots + q^{g-1} a_1 t^{2g-1} + q^g t^{2g}.$$
4. *For $n \in \mathbb{N}$ define $L_n(t) = \prod_{i=1}^{2g}(1 - \alpha_i^n t)$. Then $\#\mathrm{Pic}^0_{\mathbb{F}_{q^n}}(C) = L_n(1)$.*

Proof: The polynomial $L(t)$ is the numerator of the zeta function of C. For details see Section V.1 of Stichtenoth [589], especially Theorem V.1.15. The proof that $|\alpha_i| = \sqrt{q}$ for all $1 \leq i \leq 2g$ is Theorem V.2.1 of Stichtenoth [589].

A proof of some parts of this result in a special case is given in Exercise 10.7.14. □

Exercise 10.7.2. Show that part 3 of Theorem 10.7.1 follows immediately from part 2.

Definition 10.7.3. The polynomial $L(t)$ of Theorem 10.7.1 is called the **L-polynomial** of the curve C over $\mathbb{F}_q$.

Theorem 10.7.4. *(Schmidt) Let C be a curve of genus g over $\mathbb{F}_q$. There there exists a divisor D on C of degree 1 that is defined over $\mathbb{F}_q$.*

We stress that this result does not prove that C has a point defined over $\mathbb{F}_q$ (though when q is large compared with the genus existence of a point in $C(\mathbb{F}_q)$ will follow by the Weil bounds). The result implies that even a curve with no points defined over $\mathbb{F}_q$ does have a divisor of degree 1 (hence, not an effective divisor) that is defined over $\mathbb{F}_q$.

Proof: See Corollary V.1.11 of Stichtenoth [589]. □

We now describe the precise connection between the roots α_i of the polynomial $L(t)$ (corresponding to $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$) and $\#C(\mathbb{F}_{q^n})$ for $n \in \mathbb{N}$.

Theorem 10.7.5. *Let C be a curve of genus g over $\mathbb{F}_q$ and let $\alpha_i \in \mathbb{C}$ for $1 \leq i \leq 2g$ be as in Theorem 10.7.1. Let $n \in \mathbb{N}$. Then*

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n. \tag{10.19}$$

Proof: See Corollary V.1.16 of Stichtenoth [589]. □

Equation (10.19) can be read in two ways. On the one hand it shows that given $L(t)$ one can determine $\#C(\mathbb{F}_{q^n})$. On the other hand, it shows that if one knows $\#C(\mathbb{F}_{q^n})$ for $1 \leq n \leq g$ then one has g non-linear equations in the g variables $\alpha_1, \ldots, \alpha_g$ (there are only g variables since $\alpha_{i+g} = q/\alpha_i$ for $1 \leq i \leq g$). The following result shows that one can therefore deduce the coefficients $a_1, \ldots, a_g$ giving the polynomial $L(t)$.

Lemma 10.7.6. *(Newton's identities) Let $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ and define $t_n = \sum_{i=1}^{2g} \alpha_i^n$. Let $a_1, \ldots, a_{2g}$ be such that $\prod_{i=1}^{2g}(x - \alpha_i) = x^{2g} + a_1 x^{2g-1} + \cdots + a_{2g}$. Then, for $1 \leq n \leq 2g$,*

$$na_n = -t_n - \sum_{i=1}^{n-1} a_{n-i} t_i.$$

In particular, $a_1 = -t_1$ and $a_2 = (t_1^2 - t_2)/2$.

Exercise 10.7.7.★ Prove Lemma 10.7.6.

Exercise 10.7.8. Suppose C is a genus 3 curve over $\mathbb{F}_7$ such that $\#C(\mathbb{F}_7) = 8, \#C(\mathbb{F}_{7^2}) = 92, \#C(\mathbb{F}_{7^3}) = 344$. Determine $L(t)$ and hence $\#\mathrm{Pic}^0_{\mathbb{F}_7}(C)$. (One can take $y^2 = x^7 + x + 1$ for C.)

Exercise 10.7.9. (**Weil bounds**) Let C be a curve of genus g over $\mathbb{F}_q$. Use Theorem 10.7.1 and Theorem 10.7.5 to show that

$$|\#C(\mathbb{F}_{q^n}) - (q^n + 1)| \leq 2g\sqrt{q^n}$$

and

$$(\sqrt{q^n} - 1)^{2g} \leq \#\mathrm{Pic}^0_{\mathbb{F}_{q^n}}(C) \leq (\sqrt{q^n} + 1)^{2g}.$$

More precise bounds on $\#C(\mathbb{F}_q)$ are known; we refer to Section V.3 of Stichtenoth [589] for discussion and references.

We now sketch the relationship between the above results and the q-power Frobenius map $\pi : C \to C$ given by $\pi(x, y) = (x^q, y^q)$. This is best discussed in terms of Abelian varieties and so is strictly beyond the scope of the present book; however Exercise 10.7.11 shows how to consider the Frobenius map in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$. We refer to Section 21 of Mumford [444], especially the subsection entitled "Application II: The Riemann Hypothesis". Briefly, the Frobenius map on C induces a morphism $\pi : J_C \to J_C$ where J_C is the Jacobian variety of C (note that J_C is defined over $\mathbb{F}_q$). Note that π is not an isomorphism. This morphism is a group homomorphism with $\ker(\pi) = \{0\}$ and so is an isogeny. More generally, if A is an Abelian variety over $\mathbb{F}_q$ then there is a q-power Frobenius morphism $\pi : A \to A$. Just as in the case of elliptic curves one has $A(\mathbb{F}_{q^n}) = \ker(\pi^n - 1)$ and so $\#A(\mathbb{F}_{q^n}) = \ker(\pi^n - 1) = \deg(\pi^n - 1)$ (note that π is inseparable and $\pi^n - 1$ is a separable morphism). By considering the action of π on the Tate module (the Tate module of an Abelian variety is defined in the analogous way to elliptic curves, see Section 19 of [444]) it can be shown that π satisfies a characteristic equation given by a monic polynomial $P_A(T) \in \mathbb{Z}[T]$ of degree $2g$. It follows that $\deg(\pi - 1) = P_A(1)$. Writing $P_A(T) = \prod_{i=1}^{2g}(T - \alpha_i)$ over $\mathbb{C}$ it can be shown that $\#A(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1 - \alpha_i^n)$. It follows that the roots α_i are the same values as those used earlier, and that $P(T) = T^{2g}L(1/T)$.

Definition 10.7.10. Let C be a curve over $\mathbb{F}_q$. The **characteristic polynomial of Frobenius** is the polynomial $P(T) = T^{2g}L(1/T)$.

The Frobenius map $\pi : C \to C$ also induces the map $\pi_* : \mathrm{Pic}^0_{\mathbb{F}_q}(C) \to \mathrm{Pic}^0_{\mathbb{F}_q}(C)$, and we abuse notation by calling it π as well. If D is any divisor representing a divisor class in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ then $P(\pi)D \equiv 0$. In other words, if $P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_1 q^{g-1} T + q^g$ then

$$\pi^{2g}(D) + [a_1]\pi^{2g-1}(D) + \cdots + [a_1 q^{g-1}]\pi(D) + [q^g]D \equiv 0 \tag{10.20}$$

where the notation $[n]D$ is from Definition 10.5.1.

Exercise 10.7.11. Let C be a curve over $\mathbb{F}_q$ and D a reduced divisor on C over $\overline{\mathbb{F}}_q$ with Mumford representation $(u(x), v(x))$. Let π be the q-power Frobenius map on C. For a polynomial $u(x) = \sum_{i=0}^{d} u_i x^i$ define $u^{(q)}(x) = \sum_{i=0}^{d} u_i^q x^i$. Show that the Mumford representation of $\pi_*(D)$ is $(u^{(q)}(x), v^{(q)}(x))$.

Example 10.7.12. (Koblitz [346]) Let $a \in \{0, 1\}$ and consider the genus 2 curve $C_a : y^2 + xy = x^5 + ax^2 + 1$ over $\mathbb{F}_2$. One can verify that $\#C_0(\mathbb{F}_2) = 4$, $\#C_1(\mathbb{F}_2) = 2$ and $\#C_0(\mathbb{F}_{2^2}) = \#C_1(\mathbb{F}_{2^2}) = 4$. Hence the characteristic polynomial of Frobenius is $P(T) = T^4 + (-1)^a T^3 + 2(-1)^a T + 4$. One can determine $\#\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_a)$ for any $n \in \mathbb{N}$. If n is composite and $m \mid n$ one has $\#\mathrm{Pic}^0_{\mathbb{F}_{2^m}}(C_a) \mid \#\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_a)$. For cryptographic applications one would like $\#\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_a)/\#\mathrm{Pic}^0_{\mathbb{F}_2}(C_a)$ to be prime, so restrict attention to primes values for n. For example, taking $n = 113$ and $a = 1$ gives group order $2 \cdot r$ where $r = 539 \cdots 381$ is a 225-bit prime.

If $D \in \mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_1)$ then $\pi^4(D) - \pi^3(D) - [2]\pi(D) + [4]D \equiv 0$ where π is the map induced on $\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_1)$ from the 2-power Frobenius map $\pi(x, y) = (x^2, y^2)$ on C.

A major result, whose proof is beyond the scope of this book, is Tate's isogeny theorem.

Theorem 10.7.13. *(Tate) Let A and B be Abelian varieties over a field $\mathbb{F}_q$. Then A is $\mathbb{F}_q$-isogenous to B if and only if $P_A(T) = P_B(T)$. Similarly, A is $\mathbb{F}_q$-isogenous to an Abelian subvariety of B if and only if $P_A(T) \mid P_B(T)$.*

Proof: See [601]. □

Exercise 10.7.14 gives a direct proof of Theorems 10.7.1 and 10.7.5 for genus 2 curves with ramified model.

Exercise 10.7.14. ★ Let q be an odd prime power. Let $F(x) \in \mathbb{F}_q[x]$ be square-free and of degree 5. Then $C : y^2 = F(x)$ is a hyperelliptic curve over $\mathbb{F}_q$ of genus 2 with a ramified model. For $n = 1, 2$ let $N_n = \#C(\mathbb{F}_{q^n})$ and define $t_n = q^n + 1 - N_n$ so that $N_n = q^n + 1 - t_n$. Define $a_1 = -t_1$ and $a_2 = (t_1^2 - t_2)/2$. Show, using direct calculation and Exercise 10.4.4, that $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ has order $q^2 + a_1(q + 1) + a_2 + 1$.

An important tool in the study of elliptic curves over finite fields is the Waterhouse theorem (Theorem 9.10.12). There is an analogous result for Abelian varieties due to Honda and Tate but it is beyond the scope of this book to present this theory (we refer to [602] for details). However, we do give one application.

Theorem 10.7.15. *(Dipippo and Howe [182]) Let $q \geq 4$ be a prime power and $n \in \mathbb{Z}_{>1}$. Let $B = (\sqrt{q} - 2)/(2(\sqrt{q} - 1))$ and $C = (\lfloor B\sqrt{q} \rfloor + 1/2)/\sqrt{q}$. If $N \in \mathbb{N}$ is such that $|N - (q^n + 1)| \leq Cq^{n-1/2}$ then there exists an Abelian variety A over $\mathbb{F}_q$ of dimension n such that $\#A(\mathbb{F}_q) = N$.*

10.8 Endomorphisms

Let A_1, A_2 be Abelian varieties over $\Bbbk$. One defines $\mathrm{Hom}_{\Bbbk}(A_1, A_2)$ to be the set of all morphisms of varieties from A_1 to A_2 over $\Bbbk$ that are group homomorphisms (see Section

19 of [444]). We define $\mathrm{Hom}(A_1, A_2)$ to be $\mathrm{Hom}_{\overline{\Bbbk}}(A_1, A_2)$. The endomorphism ring of an Abelian variety A over $\Bbbk$ is defined to be $\mathrm{End}_{\Bbbk}(A) = \mathrm{Hom}_{\Bbbk}(A, A)$. We write $\mathrm{End}(A) = \mathrm{Hom}_{\overline{\Bbbk}}(A, A)$.

It is beyond the scope of this book to give a complete treatment of the endomorphism ring. However, we make a few general remarks. First, note that $\mathrm{Hom}_{\Bbbk}(A_1, A_2)$ is a $\mathbb{Z}$-module. Second, recall that for elliptic curves every non-zero homomorphism is an isogeny (i.e., has finite kernel). This is no longer true for Abelian varieties (for example, let E be an elliptic curve and consider the homomorphism $\phi : E \times E \to E \times E$ given by $\phi(P, Q) = (P, \mathcal{O}_E)$). However, if A is a simple Abelian variety then $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra and so every non-zero endomorphism is an isogeny in this case. Furthermore, if an Abelian variety A is isogenous to $\prod_i A_i^{n_i}$ with A_i simple (and A_i not isogenous to A_j for $i \neq j$) then $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \prod_i M_{n_i}(\mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q})$ where $M_n(R)$ is the ring of $n \times n$ matrices over the ring R (see Corollary 2 of Section 19 of Mumford [444]).

10.9 Supersingular Curves

Recall from Theorem 10.6.1 that if C is a curve of genus g over a field $\Bbbk$ of characteristic p then $\#\mathrm{Pic}^0_{\Bbbk}(C)[p] \leq p^g$.

Definition 10.9.1. Let $\Bbbk$ be a field such that $\mathrm{char}(\Bbbk) = p > 0$ and let C be a curve of genus g over $\Bbbk$. The **p-rank** of C is the integer $0 \leq r \leq g$ such that $\#\mathrm{Pic}^0_{\overline{\Bbbk}}(C)[p] = p^r$.

An Abelian variety of dimension g over $\mathbb{F}_q$ is defined to be **supersingular** if it is isogenous over $\overline{\mathbb{F}}_q$ to E^g where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_q$. A curve C over $\mathbb{F}_q$ is **supersingular** if J_C is a supersingular Abelian variety. It follows that the p-rank of a supersingular Abelian variety over $\mathbb{F}_{p^n}$ is zero. The converse is not true (i.e., p-rank zero does not imply supersingular) when the dimension is 3 or more; see Example 10.9.8). If the p-rank of a dimension g Abelian variety A over $\mathbb{F}_{p^n}$ is g then A is said to be **ordinary**.

Lemma 10.9.2. *Suppose A is a supersingular Abelian variety over $\mathbb{F}_q$ and write $P_A(T)$ for the characteristic polynomial of Frobenius on A. The roots α of $P_A(T)$ are such that $\alpha/\sqrt{q}$ is a root of unity.*

Proof: Since the isogeny to E^g is defined over some finite extension $\mathbb{F}_{q^n}$ it follows from part 4 of Theorem 9.11.2 that $\alpha^n/\sqrt{q^n}$ is a root of unity. Hence, $\alpha/\sqrt{q}$ is a root of unity. □

The converse of Lemma 10.9.2 follows from the Tate isogeny theorem.

Example 10.9.3. Let $C : y^2 + y = x^5$ over $\mathbb{F}_2$. One can check that $\#C(\mathbb{F}_2) = 3$ and $\#C(\mathbb{F}_{2^2}) = 5$ and so the characteristic polynomial of the 2-power Frobenius is $P(T) = T^4 + 4 = (T^2 + 2T + 2)(T^2 - 2T + 2)$. It follows from Theorem 10.7.13 (Tate's isogeny theorem) that J_C is isogenous to $E_1 \times E_2$ where E_1 and E_2 are supersingular curves over $\mathbb{F}_2$. The characteristic polynomial of the 2^2-power Frobenius can be shown to be $T^4 + 8T^2 + 16 = (T^2 + 4)^2$ and it follows that J_C is isogenous over $\mathbb{F}_{2^2}$ to the square of a supersingular elliptic curve. Hence C is a supersingular curve.

Note that the endomorphism ring of J_C is non-commutative, since the map $\phi(x, y) = (\zeta_5 x, y)$, where $\zeta_5 \in \mathbb{F}_{2^4}$ is a root of $z^4 + z^3 + z^2 + z + 1 = 0$, does not commute with the 2-power Frobenius map.

Exercise 10.9.4. ★ Show that if C is a supersingular curve over $\mathbb{F}_q$ of genus 2 then $\#\mathrm{Pic}^0_{\mathbb{F}_q}(C) \mid (q^k - 1)$ for some $1 \leq k \leq 12$.

The following result shows that computing the p-rank and determining supersingularity are easy when $P(T)$ is known.

Theorem 10.9.5. *Let A be an Abelian variety of dimension g over $\mathbb{F}_{p^n}$ with characteristic polynomial of Frobenius $P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + p^{ng}$.*

1. *The p-rank of A is the smallest integer $0 \leq r \leq g$ such that $p \mid a_i$ for all $1 \leq i \leq g-r$.*
   (In other words, the p-rank is zero if $p \mid a_i$ for all $1 \leq i \leq g$ and the p-rank is g if $p \nmid a_1$.)
2. *A is supersingular if and only if*

$$p^{\lceil in/2 \rceil} \mid a_i \qquad \text{for all} \quad 1 \leq i \leq g.$$

Proof: Part 1 is Satz 1 of Stichtenoth [588]. Part 2 is Proposition 1 of Stichtenoth and Xing [590]. □

We refer to Yui [639] for a survey of the Cartier-Manin matrix and related criteria for the p-rank.

Exercise 10.9.6. Let A be an Abelian variety of dimension 2 over $\mathbb{F}_p$ that has p-rank zero. Show that A is supersingular.

In fact, the result of Exercise 10.9.6 holds when $\mathbb{F}_p$ is replaced by any finite field; see page 9 of Li and Oort [386].

Exercise 10.9.7. Let $C : y^2 + y = F(x)$ over $\mathbb{F}_{2^n}$ where $\deg(F(x)) = 5$ be a genus 2 hyperelliptic curve. Show that C has 2-rank zero (and hence is supersingular).

Example 10.9.8 shows that, once the genus is at least 3, p-rank zero does not imply supersingularity.

Example 10.9.8. Define $C : y^2 + y = x^7$ over $\mathbb{F}_2$. Then $P(T) = T^6 - 2T^3 + 2^3$ and so by Theorem 10.9.5 the 2-rank of C is zero but C is not supersingular.

Example 10.9.9. (Hasse/Hasse-Davenport/Duursma [185]) Let $p > 2$ be prime and $C : y^2 = x^p - x + 1$ over $\mathbb{F}_p$. One can verify that C is non-singular and the genus of C is $(p-1)/2$. It is shown in [185] that, over $\mathbb{F}_{p^2}$, $L(T) = \Phi_p((\frac{-1}{p})pT)$ where $\Phi_p(T)$ is the p-th cyclotomic polynomial. It follows that the roots of $P(T)$ are roots of unity and so C is supersingular.

Part III

Exponentiation, Factoring and Discrete Logarithms

Chapter 11

Basic Algorithms for Algebraic Groups

In Section 4.1 a number of basic computational tasks for an algebraic group G were listed. Some of these topics have been discussed already, especially providing efficient group operations and compact representations for group elements. But some other topics (such as efficient exponentiation, generating random elements in G and hashing from or into G) require further attention. The goal of this chapter is to briefly give some details about these tasks for the algebraic groups of most interest in the book.

The main goal of the chapter is to discuss exponentiation and multi-exponentiation. These operations are crucial for efficient discrete logarithm cryptography and there are a number of techniques available for specific groups that give performance improvements.

It is beyond the scope of this book to present a recipe for the best possible exponentiation algorithm in a specific application. Instead, our focus is on explaining the mathematical ideas that are used. For an "implementors guide" in the case of elliptic curves we refer to Bernstein and Lange [53].

Let G be a group (written in multiplicative notation). Given $g \in G$ and $a \in \mathbb{N}$ we wish to compute g^a. We assume in this chapter that a is a randomly chosen integer of size approximately the same as the order of g, and so a varies between executions of the exponentiation algorithm. If g does not change between executions of the algorithm then we call it a **fixed base** and otherwise it is a **variable base**.

As mentioned in Section 2.8, there is a significant difference between the cases where g is fixed (and one is computing g^a repeatedly for different values of a) and the case where both g and a vary. Section 2.8 already briefly mentioned addition chains and sliding window methods. The literature on addition chains is enormous and we do not delve further into this topic. Window methods date back to Brauer in 1939 and sliding windows to Thurber; we refer to Bernstein's excellent survey [45] for historical details. Other references for fast exponentiation are Chapters 9 and 15 of [16], Chapter 3 of [274]

and Sections 14.6 and 14.7 of [418].

11.1 Efficient Exponentiation Using Signed Exponents

In certain algebraic groups, computing the inverse of a group element is much more efficient than a general group operation. For example, Exercise 6.3.1 and Lemma 6.3.12 show that inversion in $G_{q,2}$ and $\mathbb{T}_2(\mathbb{F}_q)$ is easy. Similarly, inversion in elliptic and hyperelliptic curve groups is easy (see Section 9.1 and Exercises 10.4.2 and 10.4.17). Hence, one can exploit inversion when computing exponentiation and it is desirable to consider signed expansions for exponents.

Signed expansions and addition-subtraction chains have a long history.[1] Morain and Olivos [438] realised that, since inversion is easy for elliptic curve groups, signed expansions are natural in this context.

11.1.1 Non-Adjacent Form

We now discuss the non-adjacent form (NAF) of an integer a. This is the best signed expansion in the sense that it has the minimal number of non-zero coefficients and can be computed efficiently. The non-adjacent form was discussed by Reitwiesner [499] (where it is called "property M"). Reitwiesner proved that the NAF is unique, has minimal weight among binary expansions with coefficients in $\{-1, 0, 1\}$, and he gave an algorithm to compute the NAF of an integer. These results have been re-discovered and simplified numerous times (we refer to Section IV.2.4 of [64] and Section 5 of [544] for references).

Definition 11.1.1. Let $a \in \mathbb{N}$. A representation $a = \sum_{i=0}^{l} a_i 2^i$ is a **non-adjacent form** or **NAF** if $a_i \in \{-1, 0, 1\}$ for all $0 \leq i \leq l$ and $a_i a_{i+1} = 0$ for all $0 \leq i < l$. If $a_l \neq 0$ then the **length** of the NAF is $l + 1$.

One can transform an integer a into NAF representation using Algorithm 6. This is a "right-to-left" algorithm in the sense that it processes the least significant bits first. We define the operator $a \pmod{2m}$ to be reduction of a modulo $2m$ to the range $\{-m+1, \ldots, -1, 0, 1, \ldots, m\}$. In particular, if a is odd then $a \pmod 4 \in \{-1, 1\}$. An alternative right-to-left algorithm is given in the proof of Theorem 11.1.12.

Exercise 11.1.2. Prove that Algorithm 6 outputs a NAF.

Example 11.1.3. We compute the NAF representation of $a = 91$. Since $91 \equiv 3 \pmod 4$ the first digit is -1, which we denote as $\overline{1}$. Note that $2^2 \| 92$ so the next digit is 0. Now, $92/4 = 23 \equiv 3 \pmod 4$ and the next digit is $\overline{1}$. Since $2^3 \| 24$ the next 2 digits are 0. Continuing one finds the expansion to be $10\overline{1}00\overline{1}0\overline{1}$.

Lemma 11.1.4 shows that a simple way to compute a NAF of an integer a is to compute the binary representation of $3a$, subtract the binary representation of a (writing the result in signed binary expansion, in other words, performing the subtraction without carries), and discard the least significant bit. We write this as $((3a) - a)/2$.

Lemma 11.1.4. *Let $a \in \mathbb{N}$. Then the signed binary expansion $((3a) - (a))/2$ is in non-adjacent form.*

[1] Reitwiesner's long paper [499] suggests signed expansions as a way to achieve faster arithmetic (e.g., multiplication and division) but does not discuss exponentiation. Brickell, in 1982, seems to have been the first to suggest using negative powers of g to speed up the computation of g^a; this was in the context of computing $m^e \pmod N$ in RSA and required the precomputation of $m^{-1} \pmod N$.

Algorithm 6 Convert an integer to non-adjacent form

INPUT: $a \in \mathbb{N}$
OUTPUT: $(a_l \dots a_0)$
1: $i = 0$
2: **while** $a \neq 0$ **do**
3: **if** a even **then**
4: $a_i = 0$
5: **else**
6: $a_i = a \pmod 4$
7: **end if**
8: $a = (a - a_i)/2$
9: $i = i + 1$
10: **end while**
11: **return** $a_l \dots a_0$

Proof: Write a in binary as $(a_l \dots a_0)_2$ and write $3a$ in binary as $(b_{l+2} \dots b_0)_2$. Set $a_{-1} = a_{l+1} = a_{l+2} = 0$ and $c_{-1} = 0$. Then $b_i = a_i + a_{i-1} + c_{i-1} - 2c_i$ where $c_i = \lfloor (a_i + a_{i-1} + c_{i-1})/2 \rfloor \in \{0, 1\}$ is the carry from the i-th addition.

Now consider the signed expansion $s_i = b_i - a_i \in \{-1, 0, 1\}$. In other words, $s_i = a_{i-1} + c_{i-1} - 2c_i$. Clearly $b_0 = a_0$ and so $s_0 = 0$. We show that $s_i s_{i+1} = 0$ for $1 \leq i \leq l+1$. Suppose i is such that $s_i \neq 0$. Since $a_{i-1} + c_{i-1} \in \{0, 1, 2\}$ and $a_{i-1} + c_{i-1} \equiv s_i \pmod 2$ it follows that $a_{i-1} + c_{i-1} = 1$. This then implies that $c_i = \lfloor (1 + a_i)/2 \rfloor = a_i$. Hence, $c_{i+1} = a_i$ and $s_{i+1} = a_i + c_i - 2c_{i+1} = 0$. □

Example 11.1.5. Taking $a = 91$ again, we have $3 \cdot 91 = 273 = (100010001)_2$. Computing $(3a) - a$ is

$$100010001 \; - \; 1011011 \; = \; 10\overline{1}00\overline{1}0\overline{1}0.$$

Exercise 11.1.6. Compute NAFs for $a = 100, 201, 302$ and 403.

We now state and prove some properties of NAFs.

Exercise 11.1.7. Show that if $a_l \dots a_0$ is a NAF of a then $(-a_l) \dots (-a_0)$ is a NAF of $-a$.

Lemma 11.1.8. *The NAF representation of $a \in \mathbb{Z}$ is unique.*

Proof: Without loss of generality we may assume $a > 1$. Note that $a = 1$ has a unique representation as a NAF, so assume $a > 1$. Let $a \in \mathbb{N}$ be the smallest positive integer such that a has two (or more) distinct representations as a NAF, call them $\sum_{i=0}^{l} a_i 2^i$ and $\sum_{i=0}^{l'} a'_i 2^i$. If a is even then $a_0 = a'_0 = 0$ and so we have two distinct NAF representations of $a/2$, which contradicts the minimality of a. If a is odd then $a \equiv \pm 1 \pmod 4$ and so $a_0 = a'_0$ and $a_1 = a'_1 = 0$. Hence, we obtain two distinct NAF representations of $(a - a_0)/4 < a$, which again contradicts the minimality of a. □

Exercise 11.1.9.★ Let $a \in \mathbb{N}$. Show that a has a length $l + 1$ NAF representation if and only if $2^l - d_l \leq a \leq 2^l + d_l$ where

$$d_l = \begin{cases} (2^l - 2)/3 & \text{if } l \text{ is odd} \\ (2^l - 1)/3 & \text{if } l \text{ is even.} \end{cases}$$

Also show that if $a > 0$ then $a_l = 1$ and prove that the length of a NAF is at most one more than the length of the binary expansion of a.

Definition 11.1.10. Let $\mathcal{D} \subset \mathbb{Z}$ be such that $0 \in \mathcal{D}$. The **weight** of a representation $a = \sum_{i=0}^{l} a_i 2^i$ where $a_i \in \mathcal{D}$ is the number of values $0 \leq i \leq l$ such that $a_i \neq 0$. The weight of a is denoted weight(a). The **density** of the representation is weight$(a)/(l+1)$.

Exercise 11.1.11. Show that if $a \in \mathbb{N}$ is uniformly chosen in $2^l \leq a < 2^{l+1}$ and represented using the standard binary expansion then the expected value of the weight is $(l+1)/2$ and therefore the expected value of the density is $1/2$.

Theorem 11.1.12. *The NAF of an integer $a \in \mathbb{N}$ has minimal weight among all signed expansions $a = \sum_{i=0}^{l} a_i 2^i$ where $a_i \in \{-1, 0, 1\}$.*

Proof: Let $a = \sum_{i=0}^{l} a_i 2^i$ where $a_i \in \{-1, 0, 1\}$ be any signed expansion of a. Perform the following string re-writing process from right to left (i.e., starting with a_0). If $a_i = 0$ or $a_{i+1} = 0$ then do nothing. Otherwise (i.e., $a_i \neq 0$ and $a_{i+1} \neq 0$) there exists an integer $k \geq 1$ such that the sequence $a_{i+k}a_{i+k-1} \dots a_i a_{i-1}$ is of the form

$$01 \dots 10, \qquad \overline{1}1 \dots 10, \qquad 1\overline{1} \dots \overline{1}0, \qquad 0\overline{1} \dots \overline{1}0.$$

In each case replace the pattern with the following

$$10 \dots 0\overline{1}0, \qquad 0 \dots 0\overline{1}0, \qquad 0 \dots 010, \qquad \overline{1}0 \dots 010.$$

In each case, the resulting substring has weight less than or equal to the weight of the previous substring and is in non-adjacent form (at least up to $a_{i+k-1}a_{i+k} = 0$). Continuing the process therefore yields a NAF expansion of a of weight less than or equal to the weight of the original signed expansion. □

Example 11.1.13. We re-compute the NAF representation of $a = 91$, using the method in the proof of Theorem 11.1.12. First note that the binary expansion of 91 is 1011011. One replaces the initial 011 by $10\overline{1}$ to get $1011010\overline{1}$ One then replaces 0111 by $100\overline{1}$. Continuing one determines the NAF of 91 to be $10\overline{1}00\overline{1}0\overline{1}$.

We have established that the NAF of an integer a is unique, has minimal weight, and has length at most one bit more than the binary expansion of a. Finally, we sketch a probabilistic argument that shows that the density of a NAF is expected to be $1/3$.

Lemma 11.1.14. *Let $l \in \mathbb{N}$. Define d_l to be the expected value of the density of the NAF representation of uniformly chosen integers $2^{l+1}/3 < a < 2^{l+2}/3$. Then d_l tends to $1/3$ as l goes to infinity.*

Proof: (Sketch) Write $a = \sum_{i=0}^{l} a_i 2^l$ for the NAF representation of $a \in \mathbb{N}$. Note that Algorithm 6 has the property that, if $a_i \neq 0$, then $a_{i+1} = 0$ but the value of a_{i+2} is independent of the previous operations of the algorithm. Hence, if the bits of a are considered to be chosen uniformly at random then the probability that $a_{i+2} \neq 0$ is $1/2$. Similarly, the probability that $a_{i+2} = 0$ but $a_{i+3} \neq 0$ is $1/4$, and so on. Hence, the expected number of zeroes after the non-zero a_i is (at least approximately, since the expansion is not infinite)

$$E = 1 \cdot \tfrac{1}{2} + 2 \cdot \tfrac{1}{4} + 3 \cdot \tfrac{1}{8} + \cdots = \sum_{i=1}^{\infty} \tfrac{i}{2^i}.$$

Now,

$$E = 2E - E = \sum_{i=1}^{\infty} \tfrac{i}{2^{i-1}} - \sum_{i=1}^{\infty} \tfrac{i}{2^i} = 1 + \sum_{j=1}^{\infty} \tfrac{1}{2^j} = 2.$$

Hence, on average, there are two zeros between adjacent non-zero coefficients and the density tends to $1/3$. □

Exercise 11.1.15. Prove that the number of distinct NAFs of length k is $(2^{k+2} - (-1)^k)/3$.

Exercise 11.1.16.★ Write down an algorithm to list all NAFs of length k.

For some applications it is desired to compute a low-density signed expansion from left to right; Joye and Yen [321] give an algorithm to do this.

11.1.2 Width-w Non-Adjacent Form

Definition 11.1.17. Let $w \in \mathbb{N}_{\geq 2}$ and $m = 2^{w-1} - 1$. Define $\mathcal{D} = \{0\} \cup \{a \in \mathbb{Z} : a \text{ odd}, |a| \leq m\} = \{0, \pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)\}$. A representation $\sum_{i=0}^{l} a_i 2^i$ is a **width-w non-adjacent form** (also written w-NAF or NAF_w) if $a_i \in \mathcal{D}$ and if $a_i \neq 0$ implies $a_{i+1} = \cdots = a_{i+w-1} = 0$. When writing such expansions we write $\overline{n}$ for the digit $-n$. If $a_l \neq 0$ then the **length** of the w-NAF is $l + 1$.

This notion was first proposed in Miyaji, Ono and Cohen [430] and rediscovered in Section IV.2.5 of Blake, Seroussi and Smart [64] and Section 3.2 of Solinas [576] (the latter paper gives us the terminology).

Example 11.1.18. The NAF of an integer $a \in \mathbb{N}$ is a width-2 NAF.

All the results and proofs given above regarding NAFs generalise immediately to the case of w-NAFs.

Exercise 11.1.19. Change line 7 of Algorithm 6 to read $a_i = a \pmod{2^w}$. Show that this algorithm computes a w-NAF of the integer a.

Example 11.1.20. We compute the 3-NAF of 151. Since $151 \equiv 7 \pmod 8$ we have $a_0 = -1$. One then finds $a_1 = a_2 = 0$. Now $(151 + 1)/8 = 19 \equiv 3 \pmod 8$ so $a_3 = 3$. Finally $a_4 = a_5 = a_6 = 0$ and $a_7 = 1$. The 3-NAF of 151 is therefore $1000300\overline{1}$, having weight 3. In comparison, the NAF of 151 is $1010\overline{1}00\overline{1}$, which has weight 4.

Exercise 11.1.21. Prove that the w-NAF is unique.

Exercise 11.1.22. Write pseudocode for an efficient left-to-right exponentiation algorithm using the w-NAF representation of the exponent a. Show that the precomputation requires one squaring and $2^{w-2} - 1$ multiplications.

Exercise 11.1.23. Prove that the length of a w-NAF of an integer $a \in \mathbb{N}$ is at most one more than the bit-length of a.

Exercise 11.1.24. Modify the proof of Lemma 11.1.14 to show that the expected density of the width-w NAF of a randomly chosen l-bit integer tends to $1/(w + 1)$ as l goes to infinity.

The length of a w-NAF expansion of a can be less than $\log_2(a)$, since the most significant coefficient can be as big as $2^{w-1} - 1$. Intuitively, one might expect the length on average to be approximately $\log_2(a) - (w - 1)/2$. Further discussion of this issue together with a precise analysis of the density of w-NAFs is given by Cohen [137].

It is shown in Theorem 2.3 of Avanzi [17] and Theorem 3.3 of Muir and Stinson [442] that the w-NAF has minimal weight among all signed expansions with that digit set. Analogues of the w-NAF that can be computed from left-to-right have been studied in a number of papers, starting in Section 3 of [17] and [441].

11.1.3 Further Methods

There are two other ways to exploit these ideas, namely fractional window NAFs (proposed by Möller [432, 433]) and (fractional) sliding windows over NAFs.[2] The sliding window algorithms are natural analogues of the ones mention in Example 2.8.5 and Exercise 2.8.6.

The point of these methods is to allow fine-tuning of the precomputation cost so that one can minimise the expected overall computation for exponents of a given bit-length. The basic idea is to precompute fewer group elements than the standard version of the width-w exponentiation algorithm and then to find an expansion of the exponent a of low weight that has coefficients only corresponding to the precomputed powers of g.

Example 11.1.25. Let $w = 4$. The standard sliding window exponentiation algorithm would require precomputing $g^3, g^5, g^7, g^9, g^{11}, g^{13}$ and g^{15}. Using w-NAFs requires precomputing g^3, g^5 and g^7 (as well as g^{-1}, g^{-3}, g^{-5} and g^{-7}, which is assumed to be easy). One could also consider a fractional w-NAF method whereby only g^3 and g^5 are computed.

Consider the exponent $a = 311$. This has the 4-NAF expansion

$$100030007$$

of weight 3. So one can compute g^{311} (ignoring the precomputation) using 8 squarings and 2 multiplications. This expansion cannot be used with the fractional 4-NAF, since we have not precomputed g^7. Instead, one finds the expansion

$$500\overline{1}00\overline{1},$$

which is not a 4-NAF (since each non-zero coefficient is not followed by 3 zero coefficients). However, it still has weight 3 and one computes g^{311} with 6 squarings and 2 multiplications (as well as faster precomputation).

Exercise 11.1.26. Compute a 4-NAF and a fractional 4-NAF as in Example 11.1.25 (i.e., again using only coefficients $\{0, \pm 1, \pm 3\}$) for $a = 887$.

An important issue for these methods is to determine the expected density of the resulting expansions. In Section 5.1 of Möller [432] the formula

$$\frac{1}{w + (1+m)/2^{w-1}}$$

(where the computed powers of g are $g^{\pm 1}, g^{\pm 3}, \ldots, g^{\pm m}$ and $w = \lfloor \log_2(m) \rfloor + 1$) for the density of a fractional window NAF is derived. This formula is verified using Markov chain methods in Theorem 1 of Schmidt-Samoa, Semay and Takagi [520]. Section 2.1 of [433] proves minimality of the weight among all expansions with that digit set.

All the above algorithms compute the signed expansion in a right-to-left manner. For some applications it may be desirable to compute expansions from left-to-right. There are a number of papers on this issue.

11.2 Multi-exponentiation

An n-dimensional **multi-exponentiation** (also called **simultaneous multiple exponentiation**) is the problem of computing a product $g_1^{a_1} \cdots g_n^{a_n}$. The question of how

[2] Sliding windows over NAFs were considered in Section IV.2.3 of [64]. Fractional sliding windows over NAFs seem to have been first used in [224].

efficiently this can be done was asked by Richard Bellman as problem 5125 of volume 70, number 6 of the American Mathematical Monthly in 1963. A solution was given by E. G. Straus[3] in [594]; the idea was re-discovered by Shamir and is often attributed to him. We only give a brief discussion of this topic and refer to Section 9.1.5 of [16] and Section 3.3.3 of [274] for further details.

Algorithm 7 computes an n-dimensional multi-exponentiation. We write $a_{i,j}$ for the j-th bit of a_i (where, as usual in this book, the least significant bit is $a_{i,0}$); if $j > \log_2(a_i)$ then $a_{i,j} = 0$. The main idea is to use a single accumulating variable (in this case called h) and to perform only one squaring. If a value g_i does not change between executions of the algorithm then we call it a **fixed base** and otherwise it is a **variable base** (the precomputation can be improved when some of the g_i are fixed). We assume that the integers a_i all vary.

Algorithm 7 Basic Multi-exponentiation

INPUT: $g_1, \ldots, g_n \in G, a_1, \ldots, a_n \in \mathbb{N}$
OUTPUT: $\prod_{i=1}^{n} g_i^{a_i}$

1: Precompute all $u_{b_1,\ldots,b_n} = \prod_{i=1}^{n} g_i^{b_i}$ for $b_i \in \{0,1\}$
2: Set $l = \max_{1 \leq i \leq n} \{\lfloor \log_2(a_i) \rfloor\}$
3: $h = u_{a_{1,l},\ldots,a_{n,l}}$
4: $j = l - 1$
5: **while** $j \geq 0$ **do**
6: $\quad h = h^2$
7: $\quad h = h u_{a_{1,j},\ldots,a_{n,j}}$
8: $\quad j = j - 1$
9: **end while**
10: **return** h

Example 11.2.1. One can compute $g_1^7 g_2^5$ by setting $h = u_{1,1} = g_1 g_2$, then computing $h = h^2 = g_1^2 g_2^2$, $h = h u_{1,0} = g_1^3 g_2^2$, $h = h^2 = g_1^6 g_2^4$, $h = h u_{1,1} = g_1^7 g_2^5$.

Exercise 11.2.2. Show that one can perform the precomputation in Algorithm 7 in $2^n - n - 1$ multiplications. Show that the main loop of Algorithm 7 performs l squarings and l multiplications.

Exercise 11.2.3. (Yen, Laih, and Lenstra [638]) Show that by performing further precomputation one can obtain a sliding window multi-exponentiation algorithm that still requires l squarings in the main loop, but fewer multiplications. Determine the precomputation cost.

An alternative approach[4] to multi-exponentiation is called **interleaving**. The basic idea is to replace line 7 in Algorithm 7 by

$$\textbf{for } i = 1 \textbf{ to } n \textbf{ do } h = h g_i^{a_{i,j}} \textbf{ end for}$$

and to omit the precomputation. This version is usually less efficient than Algorithm 7 unless n is rather large. However the benefit of interleaving comes when using sliding windows: since the precomputation cost and storage requirements for the method in Exercise 11.2.3 are so high, it is often much more practical to use a sliding window version in the setting of interleaving. We refer to [431] and Section 3.3.3 of [274] for further discussion of this method.

[3] Straus had the remarkable ability to solve crossword puzzles in English (his third language) using only the horizontal clues; see his commemorative issue of the Pacific Journal of Mathematics.

[4] Independently discovered by Möller [431] and Gallant, Lambert and Vanstone [233].

Exercise 11.2.4. Write pseudocode for multi-exponentiation using interleaving and sliding windows.

Exercise 11.2.5. Write pseusocode for multi-exponentiation using interleaving and sliding windows over NAF expansions.

Another approach, when signed expansions are being used, is to find a representation for the exponents $a_1, \ldots, a_n$ so that the j-th component of the representations of all a_i is simultaneously zero relatively often. Such a method was developed by Solinas [577] and is called a **joint sparse form**. We refer to Section 9.1.5 of [16] and Section 3.3.3 of [274].

Multi-exponentiation for Algebraic Group Quotients

In algebraic group quotients, multiplication is not well-defined and so extra information is needed to be able to compute $\prod_{i=1}^{n} g_i^{a_i}$. A large survey of exponentiation algorithms and multi-exponentiation algorithms for algebraic group quotients is give in Chapter 3 of Stam's thesis [579]. In particular, he gives the Montgomery Euclidean ladder in Section 3.3 (also see Section 4.3 of [578]). Due to lack of space we do not discuss this topic further.

11.3 Efficient Exponentiation in Specific Algebraic Groups

We now discuss some exponentiation methods that exploit specific features of algebraic groups.

11.3.1 Alternative Basic Operations

So far, all exponentiation algorithms have been based on squaring (and hence have used representations of integers to the base 2). We now briefly mention some alternatives to squaring as the basic operation. First we discuss halving and tripling. Frobenius expansions will be discussed in Section 11.3.2.

When one has several possible basic operations then one can consider **multi-base representations** of integers for exponentiation. These ideas were first proposed by Dimitrov, Jullien and Miller [181] but we do not consider them further in this book.

Point Halving on Elliptic Curves

This idea, independently discovered by Knudsen [342] and Schroeppel, applies to subgroups of odd order in ordinary elliptic curves over finite fields of characteristic two. The formulae for point halving were given in Exercise 9.1.4: Given $P = (x_P, y_P) \in E(\mathbb{F}_{2^n})$ one finds $Q = (x_Q, y_Q) \in E(\mathbb{F}_{2^n})$ such that $[2]Q = P$ by solving $\lambda_Q^2 + \lambda_Q = x_P + a_2$. For either solution let $x_Q = \sqrt{x_P(\lambda_Q + 1) + y_P} = \sqrt{x_P(\lambda_P + \lambda_Q + x_P + 1)}$ and $y_Q = x_Q(\lambda_Q + x_Q)$. One must ensure that the resulting point Q has odd order. When $2 \| \#E(\mathbb{F}_{q^n})$ this is easy as, by Exercise 9.1.4, it is sufficient to check that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x_Q) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a_2)$. In practice it is more convenient to check whether $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x_Q^2) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a_2)$.

Exercise 11.3.1. Write down the point halving algorithm.

Knudsen suggests representing points using the pair (x_P, λ_P) instead of (x_P, y_P). In any case, this can be done internally in the exponentiation algorithm. When $\mathbb{F}_{2^n}$ is represented using a normal basis over $\mathbb{F}_2$ then halving can be more efficient than doubling on such an elliptic curve. One can therefore use expansions of integers to the "base 2^{-1}" for efficient exponentiation. We refer to Section 13.3.5 of [16] and [342] for the details.

Tripling

Doche, Icart and Kohel [183] suggested to speed up the computation of $[m]P$ on E for small m by splitting it as $\hat{\phi} \circ \phi$ where $\phi : E \to E'$ is an isogeny of degree m. We refer to Exercise 9.6.30 for an example of this in the case $m = 3$, and to [183] for the details in general.

11.3.2 Frobenius Expansions

Koblitz (in Section 5 of [344]) presented a very efficient doubling formula for $E : y^2+y = x^3$ over $\mathbb{F}_2$ (see Exercise 9.1.3). Defining $\pi(x, y) = (x^2, y^2)$ one can write this as $[2]P = -\pi^2(P)$ for all $P \in E(\mathbb{F}_{2^m})$ for any integer m. We assume throughout this section that finite fields $\mathbb{F}_{p^m}$ are represented using a normal basis so that raising to the power p is very fast. Menezes and Vanstone [416] and Koblitz [346, 347] explored further how to speed up arithmetic on curves over small fields. However, the curves used in [344, 416, 346] are supersingular and so are less commonly used for cryptography.

The Frobenius map can be used to speed up elliptic curve exponentiation on more general curves. For cryptographic applications we assume that E is an elliptic curve over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_{q^m})$ has a large prime divisor r for some $m > 1$.[5] Let π be the q-power Frobenius map on E. The trick is to replace an integer a with a sequence $a_0, \ldots, a_l$ of "small" integers such that

$$[a]P = \sum_{i=0}^{l} [a_i]\pi^i(P)$$

for the point $P \in E(\mathbb{F}_{q^m})$ of interest.

Definition 11.3.2. Let E be an elliptic curve over $\mathbb{F}_q$ and let π be the q-power Frobenius map. Let $S \subset \mathbb{Z}$ be a finite set such that $0 \in S$ (the set S is usually obvious from the context). A **Frobenius expansion** with **digit set** S is an endomorphism of the form

$$\sum_{i=0}^{l} [a_i]\pi^i$$

where $a_i \in S$ and $a_l \neq 0$. The **length** of a Frobenius expansion is $l + 1$. The **weight** of a Frobenius expansion is the number of non-zero a_i.

Many papers write τ for the Frobenius map and speak of τ-adic expansions, but we will call them **π-adic expansions** in this book.

Example 11.3.3. Let $E : y^2 + xy = x^3 + ax^2 + 1$ over $\mathbb{F}_2$ where $a \in \{0, 1\}$. Consider the group $E(\mathbb{F}_{2^m})$ and write $\pi(x, y) = (x^2, y^2)$. From Exercise 9.10.11 we know that $\pi^2 + (-1)^a\pi + 2 = 0$. Hence, one can replace the computation $[2]P$ by $-\pi(\pi(P)) - (-1)^a\pi(P)$. At first sight, there is no improvement here (we have replaced a doubling with an elliptic curve addition). However, the idea is to represent an integer by a polynomial in π. For example, one can verify that

$$-T^5 + T^3 + 1 \equiv 9 \pmod{T^2 + T + 2}$$

and so one can compute $[9]P$ (normally taking 3 doublings and an addition) as $-\pi^5(P) + \pi^3(P) + P$ using only two elliptic curve additions.

[5] Note that, for any fixed elliptic curve E over $\mathbb{F}_q$ and any fixed $c \in \mathbb{R}_{>0}$, it is not known if there are infinitely many $m \in \mathbb{N}$ such that $\#E(\mathbb{F}_{q^m})$ has a prime factor r such that $r > cq^m$. However, in practice one finds a sufficient quantity of suitable examples.

This idea can be extended to any algebraic group G (in particular, an elliptic curve, the divisor class group of a hyperelliptic curve, or an algebraic torus) that is defined over a field $\mathbb{F}_q$ but for which one works in the group $G(\mathbb{F}_{q^m})$.

Exercise 11.3.4. Give an algorithm to compute $[a]P$ when $a = \sum_{i=0}^{l} a_i \pi^i(P)$ is a Frobenius expansion. What is the cost of the algorithm?

Definition 11.3.5. Let $S \subseteq \mathbb{Z}$ such that $0 \in S$ and if $a \in S$ then $-a \in S$. Let $a = \sum_{i=0}^{l} a_i \pi^i$ be a Frobenius expansion with $a_i \in S$. Then a is in **non-adjacent form** if $a_i a_{i+1} = 0$ for all $0 \leq i < l$. Such an expansion is also called a π**-NAF**.

An important task is to convert an integer n into a Frobenius expansion in non-adjacent form. In fact, to get short expansions we will need to convert a general element $n_0 + n_1\pi$ to a π-NAF, so we study the more general problem. The crucial result is the following.

Lemma 11.3.6. *Let π satisfy $\pi^2 - t\pi + q = 0$. An element $n_0 + n_1\pi$ in $\mathbb{Z}[\pi]$ is divisible by π if and only if $q \mid n_0$. In this case*

$$(n_0 + n_1\pi)/\pi = (n_1 + tn_0/q) + \pi(-n_0/q). \tag{11.1}$$

Similarly, it is divisible by π^2 if and only if $q \mid n_0$ and $qn_1 \equiv -tn_0 \pmod{q^2}$.

Proof: Note that $\pi^2 = t\pi - q$. Since

$$\pi(m_0 + m_1\pi) = -qm_1 + \pi(m_0 + tm_1)$$

it follows that $n_0 + n_1\pi = \pi(m_0 + m_1\pi)$ if and only if

$$n_0 = -qm_1, \quad \text{and} \quad n_1 = m_0 + tm_1.$$

Writing $m_1 = -n_0/q$ and $m_0 = n_1 - tm_1$ yields equation (11.1).

Repeating the argument, one can divide the element in equation (11.1) by π if and only if $q \mid (n_1 + tn_0/q)$. The result follows. □

The idea of the algorithm for computing a π-NAF, given $n_0 + n_1\pi$, is to add a suitable integer so that the result is divisible by π^2, divide by π^2, then repeat. This approach is only really practical when $q = 2$, so we restrict to this case.

Lemma 11.3.7. *Let $\pi^2 - t\pi + 2 = 0$ where $t = \pm 1$. Then $n_0 + n_1\pi$ is either divisible by π or else there is some $\epsilon = \pm 1$ such that*

$$(n_0 + \epsilon) + n_1\pi \equiv 0 \pmod{\pi^2}.$$

Indeed, $\epsilon = (n_0 + 2n_1 \pmod 4) - 2$, if one defines $n_0 + 2n_1 \pmod 4 \in \{1, 3\}$.

Proof: If $\pi \nmid (n_0 + n_1\pi)$ then n_0 is odd and so $n_0 \pm 1$ is even. One can choose the sign such that $2n_1 \equiv -(n_0 \pm 1) \pmod 4$ in which case the result follows. □

The right-to-left algorithm[6] to generate a π-NAF is then immediate (see Algorithm 8; this algorithm computes $u = -\epsilon$ in the notation of Lemma 11.3.7). To show that the algorithm terminates we introduce the norm map: for any $a, b \in \mathbb{R}$ define $\mathrm{N}(a + b\pi) = (a+b\pi)(a+b\bar{\pi}) = a^2+tab+qb^2$ where $\pi, \bar{\pi} \in \mathbb{C}$ are the roots of the polynomial $x^2-tx+q = 0$. This map agrees with the norm map with respect to the quadratic field extension $\mathbb{Q}(\pi)/\mathbb{Q}$ and so is multiplicative. Note also that $\mathrm{N}(a + b\pi) \geq 0$ and equals zero only when

[6] Solinas states that this algorithm was joint work with R. Reiter.

$a = b = 0$. Meier and Staffelbach [415] note that, if $n_0 + n_1\pi$ is divisible by π, then $\mathrm{N}((n_0 + n_1\pi)/\pi) = \frac{1}{2}\mathrm{N}(n_0 + n_1\pi)$. This suggests that the length of the π-NAF will grow like $\log_2(\mathrm{N}(n_0 + n_1\pi))$. The case $\mathrm{N}((n_0 \pm 1 + n_1\pi)/\pi)$ needs more care. Lemma 3 of Meier and Staffelbach [415] states that if $\mathrm{N}(n_0 + n_1\pi) < 2^n$ then there is a corresponding Frobenius expansion[7] of length at most n. Theorem 2 of Solinas gives a formula for the norm in terms of the length $k = l+1$ of the corresponding π-NAF, from which he deduces (equation (53) of [576])

$$\log_2(\mathrm{N}(n_0 + n_1\pi)) - 0.55 < k < \log_2(\mathrm{N}(n_0 + n_1\pi)) + 3.52$$

when $k \geq 30$.

Algorithm 8 Convert $n_0 + n_1\pi$ to non-adjacent form

INPUT: $n_0, n_1 \in \mathbb{Z}$
OUTPUT: $a_0, \ldots, a_l \in \{-1, 0, 1\}$
1: **while** $n_0 \neq 0$ and $n_1 \neq 0$ **do**
2: **if** n_0 odd **then**
3: $u = 2 - (n_0 + 2n_1 \pmod 4)$
4: $n_0 = n_0 - u$
5: **else**
6: $u = 0$
7: **end if**
8: Output u
9: $(n_0, n_1) = (n_1 + tn_0/2, -n_0/2)$
10: **end while**

Example 11.3.8. Suppose $\pi^2 + \pi + 2 = 0$. To convert $-1 + \pi$ to a π-NAF one writes $n_0 = -1$ and $n_1 = 1$. Let $u = 2 - (n_0 + 2n_1 \pmod 4) = 2 - (1) = 1$. Output 1 and set $n_0 = n_0 - 1$ to get $-2 + \pi$. Dividing by π yields $2 + \pi$. One can divide by π again (output 0 first) to get $-\pi$, output 0 and divide by π again to get -1. The π-NAF is therefore $1 - \pi^3$.

To see this directly using the equation $\pi^2 + \pi + 2 = 0$ write

$$-1 + \pi + (\pi^2 + \pi + 2)(1 - \pi) = 1 - \pi^3.$$

Exercise 11.3.9. Verify that Algorithm 8 does output a π-NAF.

Exercise 11.3.10. Let $\pi^2 - \pi + 2 = 0$. Use Algorithm 8 to convert $107 + 126\pi$ into non-adjacent form.

Exercise 11.3.11. Show, using the same methods as Lemma 11.1.14, that the average density of a π-NAF tends to $1/3$ when $q = 2$.

Reducing the Length of Frobenius Expansions

As we have seen, $\mathrm{N}(n + 0\pi) = n^2$, while the norm only decreases by a factor of roughly 2 each time we divide by π. Hence, the Frobenius expansions output by Algorithm 8 on input n have length roughly $2\log_2(n)$. Since the density is $1/3$ it follows that the weight of the Frobenius expansions is roughly $\frac{2}{3}\log_2(n)$. Exponentiation using Frobenius expansions is therefore faster than using the square-and-multiply algorithm, even with

[7] Meier and Staffelbach do not consider Frobenius expansions in non-adjacent form.

sliding windows (since the latter method always needs $\log_2(n)$ doublings and also some additions).

However, it is a pity that the expansions are so long. It is natural to seek shorter expansions that still have the same density. The crucial observation, due to Meier and Staffelbach, is that Algorithm 8 outputs a Frobenius expansion $\sum_i [a_i]\pi^i$ that acts the same as $[n]$ on all points in $E(\overline{\mathbb{F}}_q)$ whereas, for a given application, one only needs a Frobenius expansion that acts the same as $[n]$ on the specific subgroup $\langle P \rangle$ of prime order r.

Definition 11.3.12. Let E be an elliptic curve over $\mathbb{F}_p$, $P \in E(\mathbb{F}_{p^m})$, and let π be the p-power Frobenius map on E. We say that two Frobenius expansions $a(\pi), b(\pi) \in \mathbb{Z}[\pi]$ are **equivalent** with respect to P if

$$a(\pi)(P) = b(\pi)(P).$$

Exercise 11.3.13. Let the notation be as in Definition 11.3.12. Show that if $a(\pi) \equiv b(\pi) \pmod{\pi^m - 1}$ then $a(\pi)$ and $b(\pi)$ are equivalent with respect to P.

Show that if $Q \in \langle P \rangle$ and $a(\pi)$ and $b(\pi)$ are equivalent with respect to P then $a(\pi)$ and $b(\pi)$ are equivalent with respect to Q.

A simple idea is to replace all powers π^i by $\pi^{i \pmod m}$. This will reduce the length of a Frobenius expansion but it does not significantly change the weight (and hence, the cost of exponentiation does not change).

The goal is therefore to find an element $n_0 + n_1\pi$ of "small" norm that is equivalent to $[n]$ with respect to P. Then one applies Algorithm 8 to the pair (n_0, n_1), not to $(n, 0)$. There are two simple ways to find an element of small norm, both of which apply the Babai rounding method (see Section 18.2) in a suitable lattice. They differ in how one expresses the fact that $(n_0 + n_1\pi)P = [n]P$ for the point P of interest.

- Division with remainder in $\mathbb{Z}[\pi]$.

  This method was proposed by Meier and Staffelbach [415] and is also used by Solinas (Section 5.1 of [576]). Since $(\pi^m - 1)(P) = \mathcal{O}_E$ when $P \in E(\mathbb{F}_{q^m})$ one wants to determine the remainder of dividing n by $(\pi^m - 1)$. The method is to consider the element $\gamma = n/(\pi^m - 1) \in \mathbb{R}[\pi]/(\pi^2 - t\pi + q)$ and find a close vector to it (using Babai rounding) in the lattice $\mathbb{Z}[\pi]$. In other words, write $\gamma = \gamma_0 + \gamma_1\pi$ with $\gamma_0, \gamma_1 \in \mathbb{R}$ and round them to the nearest integers g_0, g_1 (in the special case of $\pi^2 \pm \pi + 2 = 0$ there is an exact description of a fundamental domain for the lattice that can be used to "correct" the Babai rounding method if it does not reach the closest lattice element). Lemma 3 of [415] and Proposition 57 of [576] state that $\mathrm{N}(\gamma - (g_0 + g_1\pi)) \leq 4/7$. One can then define

  $$n_0 + n_1\pi = n - (g_0 + g_1\pi)(\pi^m - 1) \pmod{\pi^2 - t\pi + q}.$$

- The Gallant-Lambert-Vanstone method [233].

  This method appears in a different context (see Section 11.3.3), but it is also suitable for the present application. We assume that $P \in E(\mathbb{F}_{q^m})$ has prime order r where $r \| \#E(\mathbb{F}_{q^m})$. Since $\pi(P) \in E(\mathbb{F}_{q^m})$ has order r it follows that $\pi(P) = [\lambda]P$ for some $\lambda \in \mathbb{Z}/r\mathbb{Z}$. The problem is therefore to find small integers n_0 and n_1 such that

  $$n_0 + n_1\lambda \equiv n \pmod{r}.$$

One defines the **GLV lattice**

$$L = \{(x_0, x_1) \in \mathbb{Z}^2 : x_0 + x_1\lambda \equiv 0 \pmod{r}\}.$$

A basis for L is given in Exercise 11.3.22. The idea is to find a lattice vector $(n_0', n_1') \in L$ close to $(n, 0)$. Then $|n_1'|$ is "small" and $|n - n_0'|$ is "small". Define $n_0 = n - n_0'$ and $n_1 = -n_1'$ so that

$$n_0 + n_1\lambda \equiv n \pmod{r}$$

as required.

We can compute a reduced basis for the lattice and then use Babai rounding to solve the closest vector problem (CVP). Note that the reduced basis can be precomputed. Since the dimension is two, one can use the Lagrange-Gauss lattice reduction algorithm (see Section 17.1). Alternatively, one can use Euclid's algorithm to compute (n_0, n_1) directly (as discussed in Section 17.1.1, Euclid's algorithm is closely related to the Lagrange-Gauss algorithm).

Example 11.3.14. The elliptic curve $E : y^2 + xy = x^3 + x^2 + 1$ over $\mathbb{F}_{2^{19}}$ has $2r$ points where $r = 262543$ is prime. Let $\pi(x, y) = (x^2, y^2)$. Then $\pi^2 - \pi + 2 = 0$. Let $n = 123456$. We want to write n as $n_0 + n_1\pi$ on the subgroup of $E(\mathbb{F}_{2^{19}})$ of order r.

For the "division with remainder in $\mathbb{Z}[\pi]$" method we first use Lucas sequences (as in Exercise 9.10.10) to determine that

$$\pi^{19} - 1 = -(171 + 457\pi)$$

(one can think of this as equality of complex numbers where π is a root of $x^2 - x + 2$, or as congruence of polynomials modulo $\pi^2 - \pi + 2$). It is convenient to change the sign (the method works in both cases). The norm of $171 + 457\pi$ is $\#E(\mathbb{F}_{2^{19}}) = 2r = 525086$. and so

$$\frac{n}{-\pi^{19} + 1} = \frac{n(171 + 457\bar{\pi})}{525086} \approx 147.653 - 107.448\pi.$$

(since $\bar{\pi} = 1 - \pi$). Rounding gives $148 - 107\pi$ and

$$n - (148 - 107\pi)(171 + 457\pi) \equiv 350 - 440\pi \pmod{\pi^2 - \pi + 2}.$$

This is a short representative for n, but its norm is larger than $8r/7$, which is not optimal. Section 5.1 of Solinas [576] shows how to choose a related element of smaller norm. In this case the correct choice of rounding is $147 - 107\pi$ giving

$$n - (147 - 107\pi)(171 + 457\pi) \equiv 521 + 17\pi \pmod{\pi^2 - \pi + 2},$$

which has norm less than $8r/7$.

Now for the Gallant-Lambert-Vanstone method. We compute $\gcd(x^{19} - 1, x^2 - x + 2) = (x - \lambda)$ in $\mathbb{F}_r[x]$, where $\lambda = 84450$. The lattice with (row) basis

$$\begin{pmatrix} r & 0 \\ -\lambda & 1 \end{pmatrix}$$

has LLL (or Lagrange-Gauss) reduced basis

$$B = \begin{pmatrix} 171 & 457 \\ 457 & -314 \end{pmatrix}.$$

Writing $\underline{b}_1, \underline{b}_2$ for the rows of the reduced matrix one finds $(n, 0) \approx 147.65\underline{b}_1 + 214.90\underline{b}_2$. One computes

$$(n, 0) - (148, 215)\, B = (-107, -126)\,.$$

One can verify that $-107 - 126\lambda \equiv n \pmod{r}$. (Exercise 11.3.16 shows how to get this element using remainders in $\mathbb{Z}[\pi]$.) The corresponding Frobenius expansion can be obtained from the solution to Exercise 11.3.10.

Exercise 11.3.15. Prove that both the above methods yield an element $n_0 + n_1\pi \in \mathbb{Z}[\pi]$ that is equivalent to n.

Exercise 11.3.16. Show that if $P \in E(\mathbb{F}_{q^m})$ but $P \notin E(\mathbb{F}_q)$ then instead of computing the remainder in $\mathbb{Z}[\pi]$ modulo the polynomial $(\pi^m - 1)$ one can use $(\pi^m - 1)/(\pi - 1)$. Repeat Example 11.3.14 using this polynomial.

In practice it is unnecessary to determine the minimal solution (n_0, n_1) as long as n_0 and n_1 have bit-length roughly $\frac{1}{2}\log_2(r)$ (where the point P has order r). We also stress that computing the q-power Frobenius map π is assumed to be very fast, so the main task is to minimise the *weight* of the representation, not its length.

Remark 11.3.17. In cryptographic protocols one is often computing $[a]P$, where a is a randomly chosen integer modulo r. Rather than choosing a random integer a and then converting to a Frobenius expansion, one could choose a random Frobenius expansion of given weight and length (this trick appears in Section 6 of [347] where it is attributed to H. W. Lenstra Jr.).

We have analysed π-NAFs in the case $q = 2$. Müller [443] gives an algorithm to compute Frobenius expansions for elliptic curves over $\mathbb{F}_{2^e}$ with $e > 1$ (but still small). The coefficients of the expansion lie in $\{-2^{e-1}, \ldots, 2^{e-1}\}$. Smart [571] gives an algorithm for odd q, with a similar coefficient set; see Exercise 11.3.18. Lange [368] generalises to hyperelliptic curves. In all cases, the output is not necessarily in non-adjacent form; to obtain a π-NAF in these cases seems to require much larger digit sets. In any case, the asymptotic density of π-NAFs with large digit set is not significantly smaller than $1/2$ and this can easily be bettered using window methods (see Exercise 11.3.19).

Exercise 11.3.18. Let $q > 2$. Show that Algorithm 8 can be generalised (not to compute a π-NAF, but just a π-adic expansion) by taking digit set $\{-\lfloor q/2 \rfloor, \ldots, -1, 0, 1, \ldots, \lfloor q/2 \rfloor\}$ (or this set with $-\lfloor q/2 \rfloor$ removed when $q > 2$ is even).

Exercise 11.3.19. Let E be an elliptic curve over a field $\mathbb{F}_q$, let π be the q-power Frobenius map, and let $P \in E(\mathbb{F}_{q^m})$. Let $S = \{-(q-1)/2, \ldots, -1, 0, 1 \ldots, (q-1)/2\}$ if q is odd and $S = \{-(q-2)/2, \ldots, -1, 0, 1, \ldots, q/2\}$ if q is even.

Suppose one has a Frobenius expansion

$$a(\pi) = \sum_{j=0}^{l} [a_j]\pi^j$$

with $a_j \in S$. Let $w \in \mathbb{N}$. Give a sliding window method to compute $[a(\pi)]P$ using windows of length w. Give an upper bound on the cost of this algorithm (including pre-computation) ignoring the cost of evaluating π.

Exercise 11.3.20. (Brumley and Järvinen [112]) Let E be an elliptic curve over $\mathbb{F}_q$, π be the q-power Frobenius, and $P \in E(\mathbb{F}_{q^m})$ have prime order r where $r \| \#E(\mathbb{F}_{q^m})$. Given a Frobenius expansion $a(\pi) = \sum_i [a_i]\pi^i$ show how to efficiently compute $a \in \mathbb{Z}$ such that $a(\pi)(P) = [a]P$.

Dimitrov, Järvinen, Jacobson, Chan and Huang [180] use Frobenius expansions on Koblitz curves to obtain a method for computing $[k]P$ which is provably sub-linear (i.e., using $o(\log(k))$ field operations). For a complete presentation of Frobenius expansions, and further references, we refer to Section 15.1 of [16]. For multi-exponentiation using Frobenius expansions there is also a π-adic joint sparse form; see Section 15.1.1.e of [16] for details.

11.3.3 GLV Method

This method is due to Gallant, Lambert and Vanstone [233] for elliptic curves and Stam and Lenstra (see Section 4.4 of [580]) for tori.[8] The idea is to use an "efficiently computable" (see below for a clarification of this term) group homomorphism ψ and replace the computation g^a in a group of order r by the multi-exponentiation $g^{a_0}\psi(g)^{a_1}$ for suitable integers a_0 and a_1 such that $|a_0|, |a_1| \approx \sqrt{r}$. Typical choices for ψ are an automorphism of an elliptic curve or the Frobenius map on an elliptic curve or torus over an extension field.

More precisely, let $g \in G(\mathbb{F}_q)$ be an element of prime order r in an algebraic group and let ψ be a group homomorphism such that $\psi(g) \in \langle g \rangle$ (this is automatic if $\psi : G(\mathbb{F}_q) \to G(\mathbb{F}_q)$ and $r \| \#G(\mathbb{F}_q)$). Then $\psi(g) = g^\lambda$ for some $\lambda \in \mathbb{Z}/r\mathbb{Z}$. The meaning of "efficiently computable" is essentially that computing $\psi(g)$ is much faster than computing g^λ using exponentiation algorithms. Hence, we require that λ and $r - \lambda$ are not small; in particular, the map $\psi(P) = -P$ on an elliptic curve is not interesting for this application.

Example 11.3.21. Consider $\mathbb{T}_2(\mathbb{F}_{p^2})$, with elements represented as in Definition 6.3.7 so that $u \in \mathbb{F}_{p^2}$ corresponds to $g = (u+\theta)/(u+\overline{\theta}) \in \mathbb{F}_{p^4}$. It follows by Lemma 6.3.12 that $A - u^p$ (where $\theta^2 + A\theta + B = 0$) corresponds to $g^p = (u^p + \overline{\theta})/(u^p + \theta) = \left((u^p + \theta)(u^p + \overline{\theta})\right)^{-1}$. Since computing u^p for $u \in \mathbb{F}_{p^2}$ is easy, the map $\psi(u) = A - u^p$ is a useful efficiently computable group homomorphism with respect to the torus group operation.

One can also perform exponentiation in $G_{q^2,2} \subseteq \mathbb{F}_{p^4}^*$ using Frobenius. Given an exponent a such that $1 \leq a < p^2$ one lets a_0 and a_1 be the coefficients in the base-p representation of a and computes g^a as $g^{a_0}\,(g^p)^{a_1}$. Note that g^p is efficient to compute as it is a linear map on the 4-dimensional vector space $\mathbb{F}_{p^4}$ over $\mathbb{F}_p$.

Other examples include the automorphism ζ_3 on $y^2 = x^3 + B$ in Example 9.4.2 and the automorphisms in Exercises 9.4.5 and 10.2.12. Computing the eigenvalue λ for ψ is usually easy in practice: for elliptic curves λ is a root of the characteristic polynomial of ψ modulo r.

In some applications (for example, $\mathbb{T}_2(\mathbb{F}_{p^3})$ or some automorphisms on genus 2 curves such as the one in Exercise 10.2.12) one can replace g^a by $g^{a_0}\psi(g)^{a_1} \cdots \psi^{l-1}(g)^{a_{l-1}}$ for some $l > 2$. We call this the l-dimensional GLV method. We stress that l cannot be chosen arbitrarily; in Example 11.3.21 the map ψ^2 is the identity map and so is not useful.

In the previous section we sketched, for elliptic curves, the GLV method to represent an integer as a short Frobenius expansion with relatively small coefficients. One can do the same for any endomorphism ψ as long as $\psi(P) = [\lambda]P$ (or $\psi(g) = g^\lambda$ in multiplicative notation). The **GLV lattice** is

$$L = \{(x_0, \ldots, x_l) \in \mathbb{Z}^{l+1} : x_0 + x_1\lambda + \cdots + x_l\lambda^l \equiv 0 \pmod{r}\}.$$

[8] A patent on the method was filed by Gallant, Lambert and Vanstone in 1999.

A basis for L is given in Exercise 11.3.22. As explained earlier, to convert an integer a into GLV representation one finds a lattice vector $(a'_0, a'_1, \ldots, a'_l) \in L$ close to $(a, 0, \ldots, 0)$ (using Babai rounding) then sets $a_0 = a - a'_0$ and $a_i = -a'_i$ for $1 \leq i \leq l$.

Exercise 11.3.22. Show that

$$\begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -\lambda & 1 & 0 & \cdots & 0 \\ -\lambda^2 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ -\lambda^l & 0 & 0 & \cdots & 1 \end{pmatrix}$$

is a basis for the GLV lattice L.

Exercise 11.3.23. Show how to compute the coefficients $a_0, \ldots, a_l$ for the GLV method using Babai rounding.

Exercise 11.3.24 gives a construction of homomorphisms for the GLV method that apply to a large class of curves. We refer to Galbraith, Lin and Scott [224] for implementation results that show the benefit of using this construction.

Exercise 11.3.24. (Iijima, Matsuo, Chao and Tsujii [305]) Let $p > 3$ be a prime and let $E : y^2 = x^3 + a_4x + a_6$ be an ordinary elliptic curve over $\mathbb{F}_p$ with $p + 1 - t$ points (note that $t \neq 0$). Let $u \in \mathbb{F}_{p^2}^*$ be a non-square and define $E' : Y^2 = X^3 + u^2a_4X + u^3a_6$ over $\mathbb{F}_{p^2}$. Show that E' is the quadratic twist of $E(\mathbb{F}_{p^2})$ and that $\#E'(\mathbb{F}_{p^2}) = (p-1)^2 + t^2$. Let $\phi : E \to E'$ be the isomorphism $\phi(x, y) = (ux, u^{3/2}y)$ defined over $\mathbb{F}_{p^4}$.

Let $\pi(x, y) = (x^p, y^p)$ and define

$$\psi = \phi \circ \pi \circ \phi^{-1}.$$

Show that $\psi : E' \to E'$ is an endomorphism of E' that is defined over $\mathbb{F}_{p^2}$. Show that $\psi^2 = [-1]$.

Let $r \mid \#E'(\mathbb{F}_{p^2})$ be a prime such that $r > 2p$ and $r^2 \nmid \#E'(\mathbb{F}_{p^2})$. Let $P \in E'(\mathbb{F}_{p^2})$ have order r. Show that $\psi^2(P) - [t]\psi(P) + [p]P = \mathcal{O}_{E'}$. Hence deduce that $\psi(P) = [\lambda]P$ where $\lambda = t^{-1}(p-1) \pmod{r}$. Note that it is possible for $\#E'(\mathbb{F}_{p^2})$ to be prime, since E' is not defined over $\mathbb{F}_p$.

As in Remark 11.3.17, for some applications one might be able to choose a random GLV expansion directly, rather than choosing a random integer and converting it to GLV representation.

There is a large literature on the GLV method, including several different algorithms to compute the integers $a_0, \ldots, a_l$. As noted earlier, reducing the bit-length of the a_i by one or two bits makes very little effect on the overall running time. Instead, the weight of the entries $a_0, \ldots, a_l$ is more critical. We refer to Sections 15.2.1 and 15.2.2 of [16] for further details and examples of the GLV method. Section 15.2.3 of [16] discusses combining the GLV method with Frobenius expansions.

11.4 Sampling from Algebraic Groups

A natural problem, given an algebraic group G over a finite field $\mathbb{F}_q$, is to generate a "random" element of G. By "random" we usually mean uniformly at random from $G(\mathbb{F}_q)$ although sometimes it may be appropriate to weaken this condition. The first problem is to generate a random integer in $[0, p-1]$ or $[1, p-1]$. Examples 11.4.1 and 11.4.2 give two simple approaches. Chapter 7 of Sidorenko [562] is a convenient survey.

Example 11.4.1. One way to generate a random integer in $[0, p-1]$ is to generate random binary strings x of length k (where $2^{k-1} < p \leq 2^k$) and only output those satisfying $0 \leq x \leq p-1$.

Example 11.4.2. Another method is to generate a binary string that is longer than p and then return this value reduced modulo p. We refer to Section 7.4 of Shoup [556] for a detailed analysis of this method (briefly, if $2^{k-1} < p \leq 2^k$ and one generates a $k+l$ bit string then the statistical difference of the output from uniform is $1/2^l$). Section 7.5 of [556] discusses how to generate a random k-bit prime and Section 7.7 of [556] discusses how to generate a random integer of known factorisation.

Exercise 11.4.3. Show that the expected number of trials of the algorithm in Example 11.4.1 is less than 2.

Exercise 11.4.4. Give an algorithm to generate an element of $\mathbb{F}_{p^n}^*$ uniformly at random, assuming that generating random integers modulo p is easy.

Appendix B.2.4 of Katz and Lindell [334] gives a thorough discussion of sampling randomly in $(\mathbb{Z}/N\mathbb{Z})^*$ and $\mathbb{F}_p^*$.

Algorithm 5 shows how to compute a generator for $\mathbb{F}_p^*$, when the factorisation of $p-1$ is known. Generalising this algorithm to $\mathbb{F}_{p^n}^*$, when the factorisation of $p^n - 1$ is known, is straightforward. In practice one often works in a subgroup $G \subseteq \mathbb{F}_q^*$ of prime order r. To sample uniformly from G one can generate a uniform element in $\mathbb{F}_q^*$ and then raise to the power $(q-1)/r$. This exponentiation can be accelerated using any of the techniques discussed earlier in this chapter.

Exercise 11.4.5. Let q be a prime power such that the factorisation of $q-1$ is known. Give an algorithm to determine the order of an element $g \in \mathbb{F}_q^*$.

Exercise 11.4.6. Let q be a prime power. Let G be a subgroup of $\mathbb{F}_q^*$ such that the factorisation of the order of G is known. Give an algorithm to compute a generator of G.

An alternative approach to the sampling problem for a finite Abelian group G is given in Exercise 11.4.7 (these ideas will also be used in Exercise 15.5.2). However, this method is often not secure for applications in discrete logarithm cryptography. The reason is that one usually wants to sample group elements at random such that no information about their discrete logarithm is known, whereas the construction in Exercise 11.4.7 (especially when used to define a hash function) may give an attacker a way to break the cryptosystem.

Exercise 11.4.7. Let G be a finite Abelian group. Let $g_1, \ldots, g_k$ be fixed elements that generate G. Let $m_1, \ldots, m_k$ be the orders of $g_1, \ldots, g_k$ respectively. Then one can generate an element of G at random by choosing integers $a_1, \ldots, a_k$ uniformly at random such that $0 \leq a_i < m_i$ for $1 \leq i \leq k$ and computing

$$\prod_{i=1}^{k} g_i^{a_i}. \tag{11.2}$$

Show that this process does sample from G with uniform distribution.

11.4.1 Sampling from Tori

We now mention further techniques to speed up sampling from subgroups of $\mathbb{F}_q^*$.

Example 11.4.8. Lemma 6.3.4 shows that $\mathbb{T}_2(\mathbb{F}_q)$ and $G_{2,q} \subseteq \mathbb{F}_{q^2}^*$ are in one-to-one corrrespondence with the set

$$\{1\} \cup \{(a+\theta)/(a+\overline{\theta}) : a \in \mathbb{F}_q\}.$$

Hence, one can sample from $\mathbb{T}_2(\mathbb{F}_q)$ or $G_{2,q}$ as follows: Choose uniformly $0 \leq a \leq p$ and, if $a = p$, output 1, otherwise output $(a+\theta)/(a+\overline{\theta})$.

Generating elements of $\mathbb{T}_6(\mathbb{F}_q)$ or $G_{6,q}$ uniformly at random is less simple, since the compression map does not map to the whole of $\mathbb{A}^2(\mathbb{F}_q)$. Indeed, the group $G_{6,q}$ has $q^2-q+1 < q^2$ elements. Example 6.4.4 showed, in the case $q \equiv 2, 5 \pmod 9$, how to map

$$A = \{(a,b) \in \mathbb{A}^2(\mathbb{F}_q) : a^2 - ab + b^2 \neq 1\} \tag{11.3}$$

to a subset of $\mathbb{T}_6(\mathbb{F}_q)$.

Exercise 11.4.9. Let $q \equiv 2, 5 \pmod 9$. Give an algorithm to generate points in the set A of equation (11.3) uniformly at random. Hence, show how to efficiently choose random elements of a large subset of $\mathbb{T}_6(\mathbb{F}_q)$ or $G_{6,q}$ uniformly at random.

11.4.2 Sampling from Elliptic Curves

Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve over $\mathbb{F}_q$ where q is not a power of 2. To generate points in $E(\mathbb{F}_q)$ one can proceed as follows: choose a random $x \in \mathbb{F}_q$; test whether $x^3+a_4x+a_6$ is a square in $\mathbb{F}_q$; if not then repeat, otherwise take square roots to get y and output (uniformly) one of $\pm y$. It is not surprising that an algorithm to generate random points is randomised, but something that did not arise previously is that this algorithm uses a randomised subroutine (i.e., to compute square roots efficiently) and may need to be repeated several times before it succeeds (i.e., it is a Las Vegas algorithm). Hence, only an expected run time for the algorithm can be determined.

A more serious problem is that the output is not uniform. For example, $\mathcal{O}_E$ is never output, and points $(x, 0)$ occur with probability twice the probability of (x, y) with $y \neq 0$. A solution for all elliptic curves (and also hyperelliptic curves with imaginary model) is given in Algorithm 9. For a detailed analysis and generalisation of this algorithm see von zur Gathen, Shparlinski and Sinclair [240].

Exercise 11.4.10. Determine expected number of iterations of Algorithm 9 in the case of elliptic curves and hence the expected running time.

Deterministic Sampling of Elliptic Curve Points

The above methods are randomised, not just due to the randomness that naturally arises when sampling, but also because of the use of randomised algorithms for solving quadratic equations, and because not every x in the field is an x-cordinate of an elliptic curve point. It is of interest to minimise the reliance on randomness, especially when using the above ideas to construct a hash function (otherwise, there may be timing attacks). We first give an easy example.

Exercise 11.4.11. (Boneh and Franklin [80]) Let $p \equiv 2 \pmod 3$ be prime. Consider the supersingular elliptic curve $E : y^2 = x^3 + a_6$ over $\mathbb{F}_p$. One can sample points uniformly in $E(\mathbb{F}_p) - \{\mathcal{O}_E\}$ by uniformly choosing $y \in \mathbb{F}_p$ and setting $x = (y^2 - a_6)^{1/3} \pmod p$. The cube root is computed efficiently by exponentiation to the power $(2p-1)/3 \equiv 3^{-1} \pmod{p-1}$.

Algorithm 9 Near-uniform sampling of points on curves

INPUT: $H(x), F(x) \in \mathbb{F}_q[x]$ such that $C : y^2 + H(x)y = F(x)$ has one $\mathbb{F}_q$ point at infinity
OUTPUT: $P \in C(\mathbb{F}_q)$

1: Choose uniformly $0 \leq x_0 \leq q$
2: **if** $x_0 = q$ **then**
3: $S = \{$ point at infinity $\}$
4: **else**
5: Compute $S = \{(x_0, y_0) : y_0 \in \mathbb{F}_q \text{ and } y_0^2 + H(x_0)y_0 - F(x_0) = 0\}$
6: **end if**
7: **if** $\#S = 0$ **then**
8: goto line 1
9: **end if**
10: **if** $\#S = 1$ **then**
11: Choose uniformly $b \in \{0, 1\}$
12: **if** $b = 0$ **then**
13: Let $P \in S$
14: **else**
15: goto line 1
16: **end if**
17: **end if**
18: **if** $\#S = 2$ **then**
19: Let P be chosen randomly from S
20: **end if**
21: **return** P

The first general results on deterministic methods to find points on curves over finite fields $\Bbbk$ are due to Schinzel and Skałba [514]. Given $a_6 \in \Bbbk$ (the case $\mathrm{char}(\Bbbk) = 2$ is not interesting since the curve is singular, and the case $\mathrm{char}(\Bbbk) = 3$ is easy since taking cube roots is easy, so assume $\mathrm{char}(\Bbbk) \neq 2, 3$) they give a formula, in terms of a_6, for four values $y_1, \ldots, y_4$ such that the equation $x^3 + a_6 = y_i^2$ has a solution $x \in \Bbbk$ for some $1 \leq i \leq 4$. This method therefore produces at most 12 points on any given curve.

Skałba [569] gave results for general curves $y^2 = F(x)$ where $F(x) = x^3 + a_4 x + a_6$. This method can give more than a fixed number of points for any given curve. More precisely, Skałba gives explicit rational functions $X_i(t) \in \mathbb{Q}(t)$ for $1 \leq i \leq 3$ such that there is a rational function $U(t) \in \mathbb{Q}(t)$ such that

$$F(X_1(t^2))F(X_2(t^2))F(X_3(t^2)) = U(t)^2.$$

In other words, Skałba gives a rational map from $\mathbb{A}^1$ to the variety $F(x_1)F(x_2)F(x_3) = u^2$. Evaluating at $t \in \mathbb{F}_p$, where $p > 3$ is prime, it follows that at least one of the $F(X_i(t^2))$ is a square in $\mathbb{F}_p^*$. One can therefore find a point on E by taking square roots. Note that efficient algorithms for computing square roots modulo p are randomised in general. Skałba suggests avoiding this problem by assuming that the required quadratic non-residue has been precomputed (as in Exercise 2.9.6).

Shallue and van de Woestijne [545] improve upon Skałba's algorithm in several ways. First, and most significantly, they show that a deterministic sampling algorithm does not require a quadratic non-residue modulo p. They achieve this by cleverly using all three values $F(X_1(t^2)), F(X_2(t^2))$ and $F(X_3(t^2))$. In addition, they give a simpler rational map (see Exercise 11.4.12) from $\mathbb{A}^1$ to the variety $F(x_1)F(x_2)F(x_3) = u^2$, and handle the characteristic 2 and 3 cases.

Exercise 11.4.12. (Shallue and van de Woestijne [545]) Let $F(x) = x^3 + Ax + B$ and $H(u, v) = u^2 + uv + v^2 + A(u + v) + B$. Let $V : F(x_1)F(x_2)F(x_3) = u^2$ and let $S : y^2H(u, v) = -F(u)$. Show that the map $\psi(u, v, y) \to (v, -A - u - v, u + y^2, F(u + y^2)H(u, v)/y)$ is a rational map from S to V. Let $p > 3$ be prime. Fix $u \in \mathbb{F}_p$ such that $F(u) \neq 0$ and $3u^2 + 2Au + 4B - A^2 \neq 0$. Show that the surface S for this fixed value of u is

$$[y(v + u/2 + A/2)]^2 + [3u^2/4 + Au/2 + B - A^2/4]y^2 = -F(u).$$

Hence, show there is a rational map from $\mathbb{A}^1$ to S and hence a rational map from $\mathbb{A}^1$ to V.

It is worth noting that there can be no rational map $\phi : \mathbb{P}^1 \to C$ when C is a curve of genus at least 1. This follows from the Hurwitz genus formula: if the map has degree d then we have $-2 = 2g(\mathbb{P}^1) - 2 = d(2g(C) - 2) + R \geq 0$ where R is a positive integer counting the ramification, which is a contradiction. The above maps do not contradict this fact. They are not rational maps from $\mathbb{P}^1$ (or $\mathbb{A}^1$) to an elliptic curve; there is always one part of the function (such as computing a square-root or cube-root) that is not a rational map.

Icart [303] has given a simpler map for elliptic curves $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ when $q \equiv 2 \pmod 3$. Let $u \in \mathbb{F}_q$. Define

$$v = (3A - u^4)/(6u)\ , \quad x = \left(v^2 - B - u^6/27\right)^{1/3} + u^2/3 \quad \text{and} \quad y = ux + v \qquad (11.4)$$

where the cube root is computed by exponentiating to the power $(2q-1)/3 \equiv 3^{-1} \pmod{(q-1)}$.

Exercise 11.4.13. Verify that the point (x, y) of equation (11.4) is a point on $E : y^2 = x^3+Ax+B$ over $\mathbb{F}_q$. Show that, given a point (x, y) on an elliptic curve E over $\mathbb{F}_q$ as above, one can efficiently compute $u \in \mathbb{F}_q$, if it exists, such that the process of equation (11.4) gives the point (x, y).

For elliptic or hyperelliptic curves of the form $y^2 = F(x)$ where $F(x) = x^n + Ax + B$ or $F(x) = x^n + Ax^2 + B$, Ulas [612] gives a rational map from $\mathbb{A}^1$ to the variety $F(x_1)F(x_2)F(x_3) = u^2$. Hence, it is possible to deterministically find points on hyperelliptic curves of this form.

Exercise 11.4.14. (Ulas) Let $F(x) = x^3 + Ax + B$ and define

$$\begin{array}{rclcrcl} X_1(t,u) & = & u, & & X_2(t,u) & = & -B/A(t^6F(u)^3 - 1)/(t^6F(u)^3 - t^2F(u)), \\ X_3(t,u) & = & t^2F(u)X_2(t,u), & & U(t,u) & = & t^3F(u)^2F(X_2(t,u)). \end{array}$$

Show that $U(t, u)^2 = F(X_1(t, u))F(X_2(t, u))F(X_3(t, u))$.
[Hint: Use a computer algebra package.]

Note that, for curves of genus 2 or more, a related computational problem is to deterministically find rational degree 0 divisor classes. A simple solution is to generate two points $P, Q \in C(\mathbb{F}_q)$ using the above methods and let $D = (P) - (Q)$. More care is needed to ensure that the divisor classes are distributed uniformly. We finish with an exercise that shows that a natural method to generate rational divisor classes is not useful for this application.

Exercise 11.4.15. Let $y^2 = F(x)$ be a hyperelliptic curve of genus $g \geq 2$ over $\mathbb{F}_p$ with $p > 2$ in imaginary model. Denote by P_0 the point at infinity. Let $x \in \mathbb{F}_p$ and suppose one has computed $y = \sqrt{F(x_0)} \in \mathbb{F}_{p^2}$. Let $P = (x, y)$. Show that if $y \notin \mathbb{F}_p$ then $D = (P) + (\sigma(P)) - 2(P_0)$ is principal, where σ is the non-trivial element of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$.

In most cryptographic applications we are interested in sampling from subgroups of $E(\mathbb{F}_q)$ of prime order r. As mentioned earlier, the simplest way to transform elements sampled randomly in $E(\mathbb{F}_q)$ into random elements of the subgroup is to exponentiate to the power $\#E(\mathbb{F}_q)/r$ (assuming that $r \| \#E(\mathbb{F}_q)$).

11.4.3 Hashing to Algebraic Groups

Recall that sampling from algebraic groups is the task of selecting group elements uniformly at random. On the other hand, a hash function $H : \{0,1\}^l \to G(\mathbb{F}_q)$ is a deterministic algorithm that takes an input $\mathsf{m} \in \{0,1\}^l$ and outputs a group element. It is required that the output distribution of H, corresponding to the uniform distribution of the message space, is close to uniform in the group $G(\mathbb{F}_q)$. The basic idea is to use m as the randomness required by the sampling algorithm.

Recall that a hash function is also usually required to satisfy some security requirements, such as collision-resistance. This is usually achieved by first applying a collision-resistant hash function $H' : \{0,1\}^l \to \{0,1\}^l$ and setting $\mathsf{m}' = H'(\mathsf{m})$. In this section we are only concerned with the problem of using m' as input to a sampling algorithm.

The first case to consider is hashing to $\mathbb{F}_p^*$. If $p > 2^l + 1$ then we are in trouble, since one cannot get uniform coverage of a set of size $p-1$ using fewer than $p-1$ elements. This shows that we always need $l > \log_2(\#G(\mathbb{F}_q))$ (though, in some applications, it might be possible to still have a useful cryptographic system even when the image of the hash function is a subset of the group).

Example 11.4.16. Suppose $2^l > p$ and $\mathsf{m} \in \{0,1\}^l$. The method of Example 11.4.2 gives output close to uniform (at least, if $l - \log_2(p)$ is reasonably large).

Exercise 11.4.17. Let $q = p^n < 2^l$. Give a hash function $H : \{0,1\}^l \to \mathbb{F}_q$.

It is relatively straightforward to turn the algorithms of Example 11.4.8 and Exercise 11.4.9 into hash functions. In the elliptic curve case there is a growing literature on transforming a sampling algorithm into a hash function. We do not give the details.

11.4.4 Hashing from Algebraic Groups

In some applications it is also necessary to have a hash function $H : G(\mathbb{F}_q) \to \{0,1\}^l$ where G is an algebraic group. Motivation for this problem is given in the discussion of key derivation functions in Section 20.2.3. A framework for problems of this type is **randomness extraction**. It is beyond the scope of this book to give a presentation of this topic, but some related results are given in Sections 21.7 and 21.6.

11.5 Determining Group Structure and Computing Generators for Elliptic Curves

Since $\mathbb{F}_q^*$ is cyclic, it follows that all subgroups of finite fields and tori are cyclic. However, elliptic curves and divisor class groups of hyperelliptic curves can be non-cyclic. Determining the group structure and a set of generators for an algebraic group $G(\mathbb{F}_q)$ can be necessary for some applications. It is important to remark that solutions to these problems are not expected to exist if the order $N = \#G(\mathbb{F}_q)$ is not known, or if the factorisation of N is not known.

Let E be an elliptic curve over $\mathbb{F}_q$ and let $N = \#E(\mathbb{F}_q)$. If N has no square factors then $E(\mathbb{F}_q)$ is isomorphic as a group to $\mathbb{Z}/N\mathbb{Z}$. If $r^2 \| N$ then there could be a point of

order r^2 or two "independent" points of order r (i.e., $E(\mathbb{F}_q)$ has a non-cyclic subgroup of order r^2 but exponent r).

The Weil pairing (see Section 26.2) can be used to determine the group structure of an elliptic curve. Let r be a prime and $P, Q \in E(\mathbb{F}_q)$ of order r. The key fact is that the Weil pairing is alternating and so $e_r(P, P) = 1$. It follows from the non-degeneracy of the pairing that $e_r(P, Q) = 1$ if and only if $Q \in \langle P \rangle$. The Weil pairing also shows that one can only have two independent points when r divides $(q - 1)$.

Given the factorisation of $\gcd(q - 1, \#E(\mathbb{F}_q))$, the group structure can be determined using a randomised algorithm due to Miller [427, 429]. We present this algorithm in Figure 10. Note that the algorithm of Theorem 2.15.10 is used in lines 7 and 10. The expected running time is polynomial, but we refer to Miller [429] for the details.

Algorithm 10 Miller's algorithm for group structure

INPUT: $E/\mathbb{F}_q$, $N_0, N_1 \in \mathbb{N}$ and the factorisation of N_0, where $\#E(\mathbb{F}_q) = N_0 N_1$, $\gcd(N_1, q - 1) = 1$ and all primes dividing N_0 divide $q - 1$

OUTPUT: Integers m and n such that $E(\mathbb{F}_q) \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ as a group

1: Write $N_0 = \prod_{i=1}^{k} l_i^{e_i}$ where $l_1, \ldots, l_k$ are distinct primes
2: For all $1 \leq i \leq k$ such that $e_i = 1$ set $N_0 = N_0/l_i, N_1 = N_1 l_i$
3: $m = 1$, $n = 1$
4: **while** $mn \neq N_0$ **do**
5: Choose random points $P', Q' \in E(\mathbb{F}_q)$
6: $P = [N_1]P'$, $Q = [N_1]Q'$
7: Find the exact orders m' and n' of P and Q
8: $n = \mathrm{lcm}(m', n')$
9: $\alpha = e_n(P, Q)$
10: Let m be the exact order of α in $\mu_n = \{z \in \mathbb{F}_q^* : z^n = 1\}$
11: **end while**
12: **return** m and nN_1

Exercise 11.5.1. Show that Algorithm 10 is correct.

Exercise 11.5.2. Modify Algorithm 10 so that it outputs generators for $E(\mathbb{F}_q)$.

Exercise 11.5.3. This exercise will determine the expected number of iterations of Algorithm 10. Let $N_0 = \prod_{i=1}^{k} l_i^{e_i}$ with $e_i > 1$ for all $1 \leq i \leq k$ where $l_1, \ldots, l_k$ are distinct primes.

Let $(l, e) = (l_i, e_i)$ for some $1 \leq i \leq k$. Write $E(\mathbb{F}_q)[l^e]$ for the subgroup of $E(\mathbb{F}_q)$ consisting of elements of order dividing l^e. This group may or may not be cyclic. Show that the probability that a pair of randomly chosen group elements generate $E(\mathbb{F}_q)[l^e]$ is at least

$$\left(1 - \tfrac{1}{l}\right)\left(1 - \tfrac{1}{l^2}\right).$$

Now, show that the probability of success overall in one iteration is at least

$$\frac{\varphi(N_0)}{N_0} \prod_{l \mid N_0} \left(1 - \tfrac{1}{l^2}\right)$$

where $\varphi(n)$ is the Euler phi function. Finally, apply Theorem A.3.1 and the fact that $\zeta(2) = \pi^2/6$ (this is the Riemann zeta function) to show that the algorithm requires $O(\log(\log(q)))$ iterations.

Kohel and Shparlinski [352] give a deterministic algorithm to compute the group structure and to find generators for $E(\mathbb{F}_q)$. Their algorithm requires $O(q^{1/2+\epsilon})$ bit operations.

11.6 Testing Subgroup Membership

In many cryptographic protocols it is necessary to verify that the elements received really do correspond to group elements with the right properties. There are a variety of attacks that can be performed otherwise, some of which are briefly mentioned in Section 20.4.2.

The first issue is whether a binary string corresponds to an element of the "parent group" $G(\mathbb{F}_q)$. This is usually easy to check when $G(\mathbb{F}_q) = \mathbb{F}_q^*$. In the case of elliptic curves one must parse the bitstring as a point (x, y) and determine that (x, y) does satisfy the curve equation.

The more difficult problem is testing whether a group element g lies in the desired subgroup. For example, if $r \| \#G(\mathbb{F}_q)$ and we are given a group element g, to ensure that g lies in the unique subgroup of order r one can compute g^r and check if this is the identity. Efficient exponentiation algorithms can be used, but the computational cost is still significant. In some situations one can more efficiently test subgroup membership. One notable case is when $\#G(\mathbb{F}_q)$ is prime, this is one reason why elliptic curves of prime order are so convenient for cryptography.

Example 11.6.1. Let $p = 2r + 1$ be a **safe prime** or **Sophie-Germain prime** (i.e., r and p are primes). Then an element $g \in \mathbb{F}_p^*$ lies in the subgroup of order r if and only if $(\frac{g}{p}) = 1$. Note that one can compute $(\frac{g}{p}) = 1$ in $O(\log(p)^2)$ bit operations, whereas computing g^r in this case requires $O(\log(p)M(\log(p)))$ bit operations. However, in practice computing the Legendre symbol may not be significantly faster than computing g^r. Also, there are other performance problems from using very large subgroups of F_p^* (for example, signature size).

Exercise 11.6.2. (King [339]) Let E be an elliptic curve over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = 2^m r$ where m is small and r is prime. Show how to use point halving (see Exercise 9.1.4) to efficiently determine whether a point $P \in E(\mathbb{F}_q)$ has order dividing r.

An alternative way to prevent attacks due to elements of incorrect group order is to "force" all group elements to lie in the required subgroup by exponentiating to a **cofactor** (such as $\#G(\mathbb{F}_q)/r$). When the cofactor is small this can be a more efficient way to deal with the problem than testing subgroup membership, though one must ensure the cryptographic system can function correctly in this setting.

With algebraic group quotients represented using traces (i.e., LUC and XTR) one represents a finite field element using a trace. This value corresponds to a valid element of the extension field only if certain conditions hold. In the case of LUC we represent $g \in G_{2,p}$, where p is prime, by the trace $V = \mathrm{Tr}(g)$. A value V corresponds to an element of $G_{2,q}$ if and only if the quadratic polynomial $(x-g)(x-g^p) = x^2 - Vx + 1$ is irreducible (in other words, if $(\frac{V^2-4}{p}) = -1$). Similarly, in XTR one needs to check whether the polynomial $x^3 - tx^2 + t^p x - 1$ is irreducible; Lenstra and Verheul [376] have given efficient algorithms to do this. Section 4 of [376] also discusses subgroup attacks in the context of XTR and countermeasures in this context.

11.7 Elliptic Curve Point Compression

When elements of an algebraic group are transmitted one often wants to minimise the number of bits sent. Indeed, one of the main motivations for torus/trace cryptography is compression of elements. With elliptic curves it is obvious that, given a point (x, y), one only needs to send x together with a single bit to specify the choice of y. To obtain the point the receiver then has to solve a quadratic equation over the finite field. An

alternative, suitable only for some applications, is to work in the algebraic group quotient corresponding to elliptic curve arithmetic using x-coordinates only. We briefly mention further tricks in the elliptic curve setting.

Example 11.7.1. (Seroussi [540]) Let $E : y^2+xy = x^3+a_2x^2+a_6$ be an ordinary elliptic curve over $\mathbb{F}_{2^n}$, so that $\#E(\mathbb{F}_{2^n})$ is even. Let $P \in E(\mathbb{F}_{2^n})$ be a point of odd order, so that $P = [2]Q$ for some point $Q \in E(\mathbb{F}_{2^n})$.

Recall from Exercise 9.1.4 that $P = (x_P, y_P) \in E(\mathbb{F}_{2^n})$ is of the form $P = [2]Q$ for some $Q \in E(\mathbb{F}_{2^n})$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x_P) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a_2)$. Hence, the trace of x_P is public knowledge.

Suppose $\mathbb{F}_{2^n}$ is represented using a normal basis, so that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x_P)$ is congruent modulo 2 to the Hamming weight of the representation of x_P. Then one can compress (x_P, y_P) by discarding y_P, removing the least significant bit of the representation of x_P and adding a bit to determine the choice of y_P. Hence, one needs n bits to send (x_P, y_P).

Exercise 11.7.2.★ (King [339]) Let the notation be as in Example 11.7.1 and suppose further that $\mathrm{Tr}(a_2) = 0$, where Tr denotes $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}$. Let $(x_P, y_P) \in E(\mathbb{F}_{2^n})$ be a point of odd order. Show that $\mathrm{Tr}(a_6/x_P^2) = 0$ and so $\mathrm{Tr}(\sqrt{a_6}/x_P) = 0$. Show that $(0, \sqrt{a_6})$ has order 2 and that this point can be halved (in other words, there is a point $R \in E(\mathbb{F}_{2^n})$ such that $(0, \sqrt{a_6}) = [2]R$). Show that $(x_P, y_P)+(0, \sqrt{a_6}) = (\sqrt{a_6}/x_P, (y_P\sqrt{a_6}+a_6)/x_P^2 + \sqrt{a_6}(1 + 1/x_P))$ and hence deduce that this point can also be halved.

Hence, show that one can send $(x_P, y_P) \in E(\mathbb{F}_{2^n})$ using only $n - 1$ bits by sending x_P with one bit omitted when $\mathrm{Tr}(y_P/x_P) = 0$ or $\sqrt{a_6}/x_P$ with one bit omitted when $\mathrm{Tr}(y_P/x_P) = 1$.

Exercise 11.7.3.★ (Galbraith and Eagle) Let E be an elliptic curve over $\mathbb{F}_2$ and let $P = (x_P, y_P) \in E(\mathbb{F}_{2^n})$. Explain how one might compress P to roughly $n - \log_2(n)$ bits on average.

We refer to Section 14.2 of [16] for the details of divisor compression for hyperelliptic curves.

Chapter 12

Primality Testing and Integer Factorisation using Algebraic Groups

There are numerous books about primality testing and integer factorisation, of which the most notable is Crandall and Pomerance [162]. There is no need to reproduce all the details of these topics. Hence, the purpose of this chapter is simply to sketch a few basic ideas that will be used later. In particular, we describe methods for primality testing and integer factorisation that exploit the structure of algebraic groups.

Definition 12.0.1. A **primality test** is a randomised algorithm that, on input $N \in \mathbb{N}$, outputs a single bit b such that if N is prime then $b = 1$. A composite integer that passes a primality test is called a **pseudoprime**. An algorithm **splits** $N \in \mathbb{N}$ if it outputs a pair (a, b) of integers such that $1 < a, b < N$ and $N = ab$.

12.1 Primality Testing

The simplest primality test is **trial division** (namely, testing whether N is divisible by any integer up to $\sqrt{N}$). This algorithm is not useful for factoring numbers chosen for cryptography, but the first step of most general purpose factoring algorithms is to run trial division to remove all 'small' prime factors of N before trying more elaborate methods. Hence, for the remainder of this section we may assume that N is odd (and usually that it is not divisible by any primes less than, say, 10^6).

12.1.1 Fermat Test

Let $N \in \mathbb{N}$. If N is prime then the algebraic group $G_m(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^*$ over the ring $\mathbb{Z}/N\mathbb{Z}$ has $N-1$ elements. In other words, if a is an integer such that $\gcd(a, N) = 1$ and

$$a^{N-1} \not\equiv 1 \pmod{N}$$

then N is not prime. Such a number a is called a **compositeness witness** for N. The hope is that if N is not prime then the order of the group $G_m(\mathbb{Z}/N\mathbb{Z})$ is not a divisor of $N-1$ and so a compositeness witness exists. Hence, the Fermat test is to choose random $1 < a < N$ and compute $a^{N-1} \pmod{N}$.

As is well-known, there are composite numbers N that are pseudoprimes for the Fermat test.

Definition 12.1.1. An integer $N \in \mathbb{N}$ is a **Carmichael number** if N is composite and

$$a^{N-1} \equiv 1 \pmod{N}$$

for all $a \in \mathbb{N}$ such that $\gcd(a, N) = 1$.

If $N = \prod_{i=1}^{l} p_i^{e_i}$ is composite then $G_m(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^{l} G_m(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ and has order $\varphi(N)$ and exponent $\lambda(N) = \operatorname{lcm}\{p_i^{e_i-1}(p_i - 1) : 1 \leq i \leq l\}$.

Exercise 12.1.2. Show that all Carmichael numbers are odd. Show that N is a Carmichael number if and only if $\lambda(N) \mid (N-1)$. Show that a composite number $N \in \mathbb{N}$ is a Carmichael number if and only if $N = \prod_{i=1}^{l} p_i$ is a product of distinct primes such that $(p_i - 1) \mid (N-1)$ for $i = 1, \ldots, l$.

Exercise 12.1.3. Show that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.

It was shown by Alford, Granville and Pomerance [10] in 1992 that there are infinitely many Carmichael numbers.

It is natural to replace $G_m(\mathbb{Z}/N\mathbb{Z})$ with any algebraic group or algebraic group quotient, such as the torus $\mathbb{T}_2$, the algebraic group quotient corresponding to Lucas sequences (this gives rise to the $p+1$ test) or an elliptic curve of predictable group order.

Exercise 12.1.4. Design a primality test based on the algebraic group $\mathbb{T}_2(\mathbb{Z}/N\mathbb{Z})$, which has order $N+1$ if N is prime. Also show to use Lucas sequences to test N for primality using the algebraic group quotient.

Exercise 12.1.5. Design a primality test for integers $N \equiv 3 \pmod{4}$ based on the algebraic group $E(\mathbb{Z}/N\mathbb{Z})$ where E is a suitably chosen supersingular elliptic curve.

Exercise 12.1.6. Design a primality test for integers $N \equiv 1 \pmod{4}$ based on the algebraic group $E(\mathbb{Z}/N\mathbb{Z})$ where E is a suitably chosen elliptic curve.

12.1.2 The Miller-Rabin Test

This primality test is also called the Selfridge-Miller-Rabin test or the strong prime test. It is a refinement of the Fermat test, and works very well in practice. Rather than changing the algebraic group, the idea is to make better use of the available information. It is based on the following trivial lemma, which is false if p is replaced by a composite number N (except for $N = p^a$ where p is odd).

Lemma 12.1.7. *Let p be prime. If $x^2 \equiv 1 \pmod{p}$ then $x \equiv \pm 1 \pmod{p}$.*

For the Miller-Rabin test write $N-1 = 2^b m$ where m is odd and consider the sequence $a_0 = a^m \pmod N$, $a_1 = a_0^2 = a^{2m} \pmod N$, $\ldots$, $a_b = a_{b-1}^2 = a^{N-1} \pmod N$ where $\gcd(a, N) = 1$. If N is prime then this sequence must have the form $(*, *, \ldots, *, -1, 1, \ldots, 1)$ or $(-1, 1, \ldots, 1)$ or $(1, \ldots, 1)$ (where $*$ denotes numbers whose values are not relevant). Any deviation from this form means that the number N is composite.

An integer N is called a **base-a probable prime** if the Miller-Rabin sequence has the good form and is called a **base-a pseudoprime** if it is a base-a probable prime that is actually composite.

Exercise 12.1.8. Let $N = 561$. Note that $\gcd(2, N) = 1$ and $2^{N-1} \equiv 1 \pmod N$. Show that the Miller-Rabin method with $a = 2$ demonstrates that N is composite. Show that this failure allows one to immediately split N.

Theorem 12.1.9. *Let $n > 9$ be an odd composite integer. Then N is a base-a pseudoprime for at most $\varphi(N)/4$ bases between 1 and N.*

Proof: See Theorem 3.5.4 of [162] or Theorem 10.6 of Shoup [556]. □

Hence, if a number N passes several Miller-Rabin tests for several randomly chosen bases a then one can believe that with high probability N is prime (Section 5.4.2 of Stinson [592] gives a careful analysis of the probability of success of a closely related algorithm using Bayes' theorem). Such an integer is called a **probable prime**. In practice one chooses $O(\log(N))$ random bases a and runs the Miller-Rabin test for each. The total complexity is therefore $O(\log(N)^4)$ bit operations (which can be improved to $O(\log(N)^2 M(\log(N)))$, where $M(m)$ is the cost of multiplying two m-bit integers).

12.1.3 Primality Proving

Agrawal, Kayal and Saxena [6] (AKS) discovered a deterministic algorithm that runs in polynomial-time and determines whether or not N is prime. We refer to Section 4.5 of [162] for details. The original AKS test has been improved significantly. A variant due to Bernstein requires $O(\log(N)^{4+o(1)})$ bit operations using fast arithmetic (see Section 4.5.4 of [162]).

There is also a large literature on primality proving using Gauss and Jacobi sums, and using elliptic curves. We refer to Sections 4.4 and 7.6 of [162].

In practice the Miller-Rabin test is still widely used for cryptographic applications.

12.2 Generating Random Primes

Definition 12.2.1. Let $X \in \mathbb{N}$, then $\pi(X)$ is defined to be the number of primes $1 < p < X$.

The famous **prime number theorem** states that $\pi(X)$ is asymptotically equal to $X/\log(X)$ (as always log denotes the natural logarithm). In other words, primes are rather common among the integers. If one choose a random integer $1 < p < X$ then the probability that p is prime is therefore about $1/\log(X)$ (equivalently, about $\log(X)$ trials are required to find a prime between 1 and X). In practice, this probability increases significantly if one choose p to be odd and not divisible by 3.

Theorem 12.2.2. *Random (probable) prime numbers of a given size X can be generated using the Miller-Rabin algorithm in expected $O(\log(X)^5)$ bit operations (or $O(\log(X)^3 M(\log(X)))$ using fast arithmetic).*

Exercise 12.2.3. For certain cryptosystems based on the discrete logarithm problem it is required to produce a k_1-bit prime p such that $p-1$ has a k_2-bit prime factor q. Give a method that takes integers k_1, k_2 such that $k_2 < k_1$ and outputs p and q such that p is a k_1-bit prime, q is a k_2-bit prime and $q \mid (p-1)$.

Exercise 12.2.4. For certain cryptosystems based on the discrete logarithm problem (see Chapter 6) it is required to produce a k_1-bit prime p such that $\Phi_k(p)$ has a k_2-bit prime factor q (where $\Phi_k(x)$ is the k-th cyclotomic polynomial). Give a method that takes integers k, k_1, k_2 such that $k_2 < \varphi(k)k_1$ and outputs p and q such that p is a k_1-bit prime, q is a k_2-bit prime and $q \mid \Phi_k(p)$.

Exercise 12.2.5. A **strong prime** is defined to be a prime p such that $q = (p-1)/2$ is prime, $(p+1)/2$ is prime and $(q-1)/2$ is prime (it is conjectured that infinitely many such primes exist). Some RSA systems require the RSA moduli to be a product of strong primes. Give an algorithm to generate strong primes.

12.2.1 Primality Certificates

For cryptographic applications it may be required to provide a **primality certificate**. This is a mathematical proof that can be checked in polynomial-time and that establishes the primality of a number n. Pratt [490] showed that there exists a short primality certificate for every prime. Primality certificates are not so important since the discovery of the AKS test, but primes together with certificates can be generated (and the certificates verified) more quickly than using the AKS test, so this subject could still be of interest. We refer to Section 4.1.3 of Crandall and Pomerance [162] and Maurer [403] for further details.

One basic tool for primality certificates is Lucas' converse of Fermat's little theorem.

Theorem 12.2.6. *(Lucas) Let $N \in \mathbb{N}$. If there is an integer a such that $\gcd(a, N) = 1$, $a^{N-1} \equiv 1 \pmod{N}$ and $a^{(N-1)/l} \not\equiv 1 \pmod{N}$ for all primes $l \mid (N-1)$ then N is prime.*

Exercise 12.2.7. Prove Theorem 12.2.6.

In practice one can weaken the hypothesis of Theorem 12.2.6.

Theorem 12.2.8. *(Pocklington) Suppose $N - 1 = FR$ where the complete factorisation of F is known. Suppose there is an integer a such that $a^{N-1} \equiv 1 \pmod{N}$ and*

$$a^{(N-1)/q} \not\equiv 1 \pmod{N}$$

for every prime $q \mid F$. Then every prime factor of N is congruent to 1 modulo F. Hence, if $F \geq \sqrt{N}$ then N is prime.

Exercise 12.2.9. Prove Theorem 12.2.8.

Exercise 12.2.10. A **Sophie-Germain prime** (in cryptography the name **safe prime** is commonly used) is a prime p such that $(p-1)/2$ is also prime. It is conjectured that there are infinitely many Sophie-Germain primes. Give a method to generate a k-bit Sophie-Germain prime together with a certificate of primality, such that the output is close to uniform over the set of all k-bit Sophie-Germain primes.

12.3 The $p-1$ Factoring Method

First we recall the notion of a smooth integer. These are discussed in more detail in Section 15.1.

Definition 12.3.1. Let $N = \prod_{i=1}^{r} p_i^{e_i} \in \mathbb{N}$ (where we assume the p_i are distinct primes and $e_i \geq 1$) and let $B \in \mathbb{N}$. Then N is **B-smooth** if all $p_i \leq B$ and N is **B-power smooth** (or **strongly B-smooth**) if all $p_i^{e_i} \leq B$.

Example 12.3.2. $528 = 2^4 \cdot 3 \cdot 11$ is 14-smooth but is not 14-power smooth.

The $p-1$ method was published by Pollard [485].[1] The idea is to suppose that N has prime factors p and q where $p-1$ is B-power smooth but $q-1$ is not B-power smooth. Then if $1 < a < N$ is randomly chosen we have $a^{B!} \equiv 1 \pmod{p}$ and, with high probability, $a^{B!} \not\equiv 1 \pmod{q}$. Hence $\gcd(a^{B!} - 1, N)$ splits N. Algorithm 11 gives the Pollard $p-1$ algorithm.

Example 12.3.3. Let $N = 124639$ and let $B = 8$. Choose $a = 2$. One can check that

$$\gcd(a^{B!} \pmod{N} - 1, N) = 113$$

from which one deduces that $N = 113 \cdot 1103$.

This example worked because the prime $p = 113$ satisfies $p - 1 = 2^4 \cdot 7 \mid 8!$ and so $2^{8!} \equiv 1 \pmod{p}$ while the other prime satisfies $q - 1 = 2 \cdot 19 \cdot 29$, which is not 8-smooth.

Of course, the "factor" returned from the gcd may be 1 or N. If the factor is not 1 or N then we have split N as $N = ab$. We now test each factor for primality and attempt to split any composite factors further.

Algorithm 11 Pollard $p-1$ algorithm

INPUT: $N \in \mathbb{N}$
OUTPUT: Factor of N
1: Choose a suitable value for B
2: Choose a random $1 < a < N$
3: $b = a$
4: **for** $i = 2$ to B **do**
5: $\quad b = b^i \pmod{N}$
6: **end for**
7: **return** $\gcd(b - 1, N)$

Exercise 12.3.4. Factor $N = 10028219737$ using the $p-1$ method.

Lemma 12.3.5. *The complexity of Algorithm 11 is $O(B \log(B) M(\log(N)))$ bit operations.*

Proof: The main loop is repeated B times and contains an exponentiation modulo N to a power $i < B$. The cost of the exponentiation is $O(\log(B)M(\log(N)))$ bit operations. □

The algorithm is therefore exponential in B and so is only practical if B is relatively small. If $B = O(\log(N)^i)$ then the algorithm is polynomial-time. Unfortunately, the algorithm only splits numbers of a special form (namely those for which there is a factor p such that $p-1$ is very smooth).

[1] According to [634] the first stage of the method was also known to D. N. and D. H. Lehmer, though they never published it.

Exercise 12.3.6. Show that searching only over prime power values for i in Algorithm 11 lowers the complexity to $O(BM(\log(N)))$ bit operations.

It is usual to have a **second stage** or **continuation** to the Pollard $p-1$ method. Suppose that Algorithm 11 terminates with $\gcd(b-1, N) = 1$. If there is a prime $p \mid N$ such that $p - 1 = SQ$ where S is B-smooth and Q is prime then the order of b modulo p is Q. One will therefore expect to split N by computing $\gcd(b^Q \pmod N - 1, N)$. The second stage is to find Q if it is not too big. One therefore chooses a bound $B' > B$ and wants to compute $\gcd(b^Q \pmod N - 1, N)$ for all primes $B < Q \leq B'$.

We give two methods to do this: the standard continuation (Exercise 12.3.7) has the same complexity as the first stage of the $p-1$ method, but the constants are much better; the FFT continuation (Exercise 12.3.8) has better complexity and shows that if sufficient storage is available then one can take B' to be considerably bigger than B. Further improvements are given in Sections 4.1 and 4.2 of Montgomery [436].

Exercise 12.3.7. (Standard continuation) Show that one can compute $\gcd(b^Q \pmod N - 1, N)$ for all primes $B < Q \leq B'$ in $O((B' - B)M(\log(N)))$ bit operations.

Exercise 12.3.8. (Pollard's FFT continuation) Let $w = \lceil \sqrt{B' - B} \rceil$. We will exploit the fact that $Q = B + vw - u$ for some $0 \leq u < w$ and some $1 \leq v \leq w$ (this is very similar to the baby-step-giant-step algorithm; see Section 13.3). Let $P(x) = \prod_{i=0}^{w-1}(x - b^i) \pmod N$, computed as in Section 2.16. Now compute $\gcd(P(g^{B+vw}) \pmod N, N)$ for $v = 1, 2, \ldots, w$. For the correct value v we have

$$\begin{aligned} P(g^{B+vw}) = \prod_i (g^{B+vw} - g^i) &= (g^{B+vw} - g^u) \prod_{i \neq u} (g^{B+vw} - g^i) \\ &= g^u (g^{B+vw-u} - 1) \prod_{i \neq u} (g^{B+vw} - g^i). \end{aligned}$$

Since $g^{B+vw-u} = g^Q \equiv 1 \pmod p$ then $\gcd(P(g^{B+vw}) \pmod N, N)$ is divisible by p. Show that the time complexity of this continutation is $O(M(w)\log(w)M(\log(N))$, which asymptotically is $O(\sqrt{B'}\log(B')^2 \log(\log(B'))M(\log(N)))$, bit operations. Show that the storage required is $O(w\log(w)) = O(\sqrt{B'}\log(B'))$ bits.

Exercise 12.3.9. The $p+1$ factoring method uses the same idea as the $p-1$ method, but in the algebraic group $\mathbb{T}_2$ or the algebraic group quotient corresponding to Lucas sequences. Write down the details of the $p+1$ factoring method using Lucas sequences.

12.4 Elliptic Curve Method

Let N be an integer to be factored and let $p \mid N$ be prime. One can view Pollard's $p-1$ method as using an auxiliary group (namely, $G_m(\mathbb{F}_p)$) that may have smooth order. The idea is then to obtain an element modulo N (namely, $a^{B!}$) that is congruent modulo p (but not modulo some other prime $q \mid N$) to the identity element of the auxiliary group.

Lenstra's idea was to replace the group G_m in the Pollard $p-1$ method with the group of points on an elliptic curve. The motivation was that even if $p-1$ is not smooth, it is reasonable to expect that there is an elliptic curve E over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p)$ is rather smooth. Furthermore, since there are lots of different elliptic curves over the field $\mathbb{F}_p$ we have a chance to split N by trying the method with lots of different elliptic curves. We refer to Section 9.14 for some remarks on elliptic curves modulo N.

If E is a "randomly chosen" elliptic curve modulo N with a point P on E modulo N then one hopes that the point $Q = [B!]P$ is congruent modulo p (but not modulo

some other prime q) to the identity element. One constructs E and P together, for example choosing $1 < x_P, y_P, a_4 < N$ and setting $a_6 = y_P^2 - x_P^3 - a_4 x_P \pmod N$. If one computes $Q = (x : y : z)$ using inversion-free arithmetic and projective coordinates (as in Exercise 9.1.5) then $Q \equiv \mathcal{O}_E \pmod p$ is equivalent to $p \mid z$. Here we are performing elliptic curve arithmetic over the ring $\mathbb{Z}/N\mathbb{Z}$ (see Section 9.14).

The resulting algorithm is known as the **elliptic curve method** or **ECM** and it is very widely used, both as a general-purpose factoring algorithm in computer algebra packages, and as a subroutine of the number field sieve. An important consequence of Lenstra's suggestion of replacing the group $\mathbb{F}_p^*$ by $E(\mathbb{F}_p)$ is that it motivated Miller and Koblitz to suggest using $E(\mathbb{F}_p)$ instead of $\mathbb{F}_p^*$ for public key cryptography.

Algorithm 12 gives a sketch of one round of the ECM algorithm. If the algorithm fails then one should repeat it, possibly increasing the size of B. Note that it can be more efficient to compute $[B!]P$ as a single exponentiation rather than a loop as in line 5 of Algorithm 12; see [49].

Algorithm 12 Elliptic curve factoring algorithm

INPUT: $N \in \mathbb{N}$
OUTPUT: Factor of N
1: Choose a suitable value for B
2: Choose random elements $0 \leq x, y, a_4 < N$
3: Set $a_6 = y^2 - x^3 - a_4 x \pmod N$
4: Set $P = (x : y : 1)$
5: **for** $i = 2$ to B **do**
6: Compute $P = [i]P$
7: **end for**
8: **return** $\gcd(N, z)$ where $P = (x : y : z)$

Exercise 12.4.1. Show that the complexity of Algorithm 12 is $O(B \log(B) M(\log(N)))$ bit operations.

Exercise 12.4.2. Show that the complexity of Algorithm 12 can be lowered to $O(BM(\log(N)))$ bit operations using the method of Exercise 12.3.6.

Many of the techniques used to improve the Pollard $p-1$ method (such as the standard continuation, though not Pollard's FFT continuation) also apply directly to the elliptic curve method. We refer to Section 7.4 of [162] for details. One can also employ all known techniques to speed up elliptic curve arithmetic. Indeed, the Montgomery model for elliptic curves (Section 9.12.1) was discovered in the context of ECM rather than ECC.

In practice, we repeat the algorithm a number of times for random choices of B, x, y and a_4. The difficult problems are to determine a good choice for B and to analyse the probability of success. We discuss these issues in Section 15.3 where we state Lenstra's conjecture that the elliptic curve method factors integers in subexponential time.

12.5 Pollard-Strassen Method

Pollard [485] and, independently, Strassen gave a deterministic algorithm to factor an integer N in $\tilde{O}(N^{1/4})$ bit operations. It is based on the idea[2] of Section 2.16, namely that

[2]Despite the title of this chapter, the Pollard-Strassen algorithm does not use algebraic groups, or any group-theoretic property of the integers modulo N.

one can evaluate a polynomial of degree n in $(\mathbb{Z}/N\mathbb{Z})[x]$ at n values in $O(M(n)\log(n))$ operations in $\mathbb{Z}/N\mathbb{Z}$. A different factoring algorithm with this complexity is given in Exercise 19.4.7.

The trick to let $B = \lceil N^{1/4} \rceil$, $F(x) = x(x-1)\cdots(x-B+1)$ (which has degree B) and to compute $F(jB) \pmod N$ for $1 \leq j \leq B$. Computing these values requires $O(M(B)\log(B)M(\log(N))) = O(N^{1/4}\log(N)^3\log(\log(N))^2\log(\log(\log(N))))$ bit operations. Once this list of values has been computed one computes $\gcd(N, F(jB) \pmod N)$ until one finds a value that is not 1. This will happen, for some j, since the smallest prime factor of N is of the form $jB - i$ for some $1 \leq j \leq B$ and some $0 \leq i < B$. Note that $M = \gcd(N, F(jB) \pmod N)$ may not be prime, but one can find the prime factors of it in $\tilde{O}(N^{1/4})$ bit operations by computing $\gcd(M, jB - i)$ for that value of j and all $0 \leq i < B$. Indeed, one can find all prime factors of N that are less than $N^{1/2}$ (and hence factor N completely) using this method. The overall complexity is $\tilde{O}(N^{1/4})$ bit operations.

Exercise 12.5.1.★ Show that one can determine all primes p such that $p^2 \mid N$ in $\tilde{O}(N^{1/6})$ bit operations.

Chapter 13

Basic Discrete Logarithm Algorithms

This chapter is about algorithms to solve the discrete logarithm problem (DLP) and some variants of it. We focus mainly on deterministic methods that work in any group; later chapters will present the Pollard rho and kangaroo methods, and index calculus algorithms. In this chapter we also present the concept of generic algorithms and prove lower bounds on the running time of a generic algorithm for the DLP. The starting point is the following definition (already given as Definition 2.1.1).

Definition 13.0.1. Let G be a group written in multiplicative notation. The **discrete logarithm problem** (**DLP**) is: Given $g, h \in G$ to find a, if it exists, such that $h = g^a$. We sometimes denote a by $\log_g(h)$.

As discussed after Definition 2.1.1, we intentionally do not specify a distribution on g or h or a above, although it is common to assume that g is sampled uniformly at random in G and a is sampled uniformly from $\{1, \ldots, \#G\}$.

Typically G will be an algebraic group over a finite field $\mathbb{F}_q$ and the order of g will be known. If one is considering cryptography in an algebraic group quotient then we assume that the DLP has been lifted to the covering group G. A solution to the DLP exists if and only if $h \in \langle g \rangle$ (i.e., h lies in the subgroup generated by g). We have discussed methods to test this in Section 11.6.

Exercise 13.0.2. Consider the discrete logarithm problem in the group of integers modulo p under **addition**. Show that the discrete logarithm problem in this case can be solved in polynomial-time.

Exercise 13.0.2 shows there are groups for which the DLP is easy. The focus in this book is on algebraic groups for which the DLP seems to be hard.

Exercise 13.0.3. Let N be composite. Define the discrete logarithm problem DLP-MOD-N in the multiplicative group of integers modulo N. Show that FACTOR $\leq_R$ DLP-MOD-N.

Exercise 13.0.3 gives some evidence that cryptosystems based on the DLP should be at least as secure as cryptosystems based on factoring.

13.1 Exhaustive Search

The simplest algorithm for the DLP is to sequentially compute g^a for $0 \leq a < r$ and test equality of each value with h. This requires at most $r-2$ group operations and r comparisons.

Exercise 13.1.1. Write pseudocode for the exhaustive search algorithm for the DLP and verify the claims about the worst-case number of group operations and comparisons.

If the cost of testing equality of group elements is $O(1)$ group operations then the worst-case running time of the algorithm is $O(r)$ group operations. It is natural to assume that testing equality is always $O(1)$ group operations, and this will always be true for the algebraic groups considered in this book. However, as Exercise 13.1.2 shows, such an assumption is not entirely trivial.

Exercise 13.1.2. Suppose projective coordinates are used for elliptic curves $E(\mathbb{F}_q)$ to speed up the group operations in the exhaustive search algorithm. Show that testing equality between a point in projective coordinates and a point in affine or projective coordinates requires at least one multiplication in $\mathbb{F}_q$ (and so this cost is not linear). Show that, nevertheless, the cost of testing equality is less than the cost of a group operation.

For the rest of this chapter we assume that groups are represented in a compact way and that operations involving the representation of the group (e.g., testing equality) all cost less than the cost of one group operation. This assumption is satisfied for all the algebraic groups studied in this book.

13.2 The Pohlig-Hellman Method

Let g have order N and let $h = g^a$, so that h lies in the cyclic group generated by g. Suppose $N = \prod_{i=1}^{n} l_i^{e_i}$. The idea of the Pohlig-Hellman[1] method [482] is to compute a modulo the prime powers $l_i^{e_i}$ and then recover the solution using the Chinese remainder theorem. The main ingredient is the following group homomorphism, which reduces the discrete logarithm problem to subgroups of prime power order.

Lemma 13.2.1. *Suppose g has order N and $l^e \mid N$. The function*

$$\Phi_{l^e}(g) = g^{N/l^e}$$

is a group homomorphism from $\langle g \rangle$ to the unique cyclic subgroup of $\langle g \rangle$ of order l^e. Hence, if $h = g^a$ then

$$\Phi_{l^e}(h) = \Phi_{l^e}(g)^{a \pmod{l^e}}.$$

[1] The paper [482] is authored by Pohlig and Hellman and so the method is usually referred to by this name, although R. Silver, R. Schroeppel, H. Block, and V. Nechaev also discovered it.

Exercise 13.2.2. Prove Lemma 13.2.1.

Using Φ_{l^e} one can reduce the DLP to subgroups of prime power order. To reduce the problem to subgroups of prime order we do the following: Suppose g_0 has order l^e and $h_0 = g_0^a$ then we can write $a = a_0 + a_1 l + \cdots a_{e-1} l^{e-1}$ where $0 \leq a_i < l$. Let $g_1 = g_0^{l^{e-1}}$. Raising to the power l^{e-1} gives

$$h_0^{l^{e-1}} = g_1^{a_0}$$

from which one can find a_0 by trying all possibilities (or using baby-step-giant-step or other methods).

To compute a_1 we define $h_1 = h_0 g_0^{-a_0}$ so that

$$h_1 = g_0^{a_1 l + a_2 l^2 + \cdots a_{e-1} l^{e-1}}.$$

Then a_1 is obtained by solving

$$h_1^{l^{e-2}} = g_1^{a_1}$$

To obtain the next value we set $h_2 = h_1 g_0^{-l a_1}$ and repeat. Continuing gives the full solution modulo l^e. Once a is known modulo $l_i^{e_i}$ for all $l_i^{e_i} \| N$ one computes a using the Chinese remainder theorem. The full algorithm (in a slightly more efficient variant) is given in Algorithm 13.

Algorithm 13 Pohlig-Hellman algorithm

INPUT: $g, h = g^a$, $\{(l_i, e_i) : 1 \leq i \leq n\}$ such that order of g is $N = \prod_{i=1}^n l_i^{e_i}$
OUTPUT: a

1: Compute $\{g^{N/l_i^{f_i}}, h^{N/l_i^{f_i}} : 1 \leq i \leq n, 1 \leq f_i \leq e_i\}$
2: **for** $i = 1$ to n **do**
3: $a_i = 0$
4: **for** $j = 1$ to e_i **do** ▷ Reducing DLP of order $l_i^{e_i}$ to cyclic groups
5: Let $g_0 = g^{N/l_i^j}$ and $h_0 = h^{N/l_i^j}$ ▷ These were already computed in line 1
6: Compute $u = g_0^{-a_i}$ and $h_0 = h_0 u$
7: **if** $h_0 \neq 1$ **then**
8: Let $g_0 = g^{N/l_i}$, $b = 1$, $T = g_0$ ▷ Already computed in line 1
9: **while** $h_0 \neq T$ **do** ▷ Exhaustive search
10: $b = b + 1$, $T = T g_0$
11: **end while**
12: $a_i = a_i + b l_i^{j-1}$
13: **end if**
14: **end for**
15: **end for**
16: Use Chinese remainder theorem to compute $a \equiv a_i \pmod{l_i^{e_i}}$ for $1 \leq i \leq n$
17: **return** a

Example 13.2.3. Let $p = 19, g = 2$ and $h = 5$. The aim is to find an integer a such that $h \equiv g^a \pmod{p}$. Note that $p - 1 = 2 \cdot 3^2$. We first find a modulo 2. We have $(p-1)/2 = 9$ so define $g_0 = g^9 \equiv -1 \pmod{19}$ and $h_0 = h^9 \equiv 1 \pmod{19}$. It follows that $a \equiv 0 \pmod{2}$.

Now we find a modulo 9. Since $(p-1)/9 = 2$ we first compute $g_0 = g^2 \equiv 4 \pmod{19}$ and $h_0 \equiv h^2 \equiv 6 \pmod{19}$. To get information modulo 3 we compute (this is a slight change of notation from Algorithm 13)

$$g_1 = g_0^3 \equiv 7 \pmod{19} \text{ and } h_0^3 \equiv 7 \pmod{19}.$$

It follows that $a \equiv 1 \pmod 3$. To get information modulo 9 we remove the modulo 3 part by setting $h_1 = h_0/g_0 = 6/4 \equiv 11 \pmod{19}$. We now solve $h_1 \equiv g_1^{a_1} \pmod{19}$, which has the solution $a_1 \equiv 2 \pmod 3$. It follows that $a \equiv 1 + 3 \cdot 2 \equiv 7 \pmod 9$.

Finally, by the Chinese remainder theorem we obtain $a \equiv 16 \pmod{18}$.

Exercise 13.2.4. Let $p = 31$, $g = 3$ and $h = 22$. Solve the discrete logarithm problem of h to the base g using the Pohlig-Hellman method.

We recall that an integer is B-smooth if all its prime factors are at most B.

Theorem 13.2.5. *Let $g \in G$ have order N. Let $B \in \mathbb{N}$ be such that N is B-smooth Then Algorithm 13 solves the DLP in G using $O(\log(N)^2 + B\log(N))$ group operations.*[2]

Proof: One can factor N using trial division in $O(BM(\log(N)))$ bit operations, where $M(n)$ is the cost of multiplying n-bit integers. We assume that $M(\log(N))$ is $O(1)$ group operations (this is true for all the algebraic groups of interest in this book). Hence, we may assume that the factorisation of N is known.

Computing all $\Phi_{l_i^{e_i}}(g)$ and $\Phi_{l_i^{e_i}}(h)$ can be done naively in $O(\log(N)^2)$ group operations, but we prefer to do it in $O(\log(N)\log\log(N))$ group operations using the method of Section 2.15.1.

Lines 5 to 13 run $\sum_{i=1}^n e_i = O(\log(N))$ times and, since each $l_i \geq 2$, we have $\sum_{i=1}^n e_i \leq \log_2(N)$. The computation of u in line 6 requires $O(e_i \log(l_i))$ group operations. Together this gives a bound of $O(\log(N)^2)$ group operations to the running time. (Note that when $N = 2^e$ then the cost of these lines is $e^2\log(2) = O(\log(N)^2)$ group operations.)

Solving each DLP in a cyclic group of order l_i using naive methods requires $O(l_i)$ group operations (this can be improved using the baby-step-giant-step method). There are $\leq \log_2(N)$ such computations to perform, giving $O(\log(N)B)$ group operations.

The final step is to use the Chinese remainder theorem to compute a, requiring $O(\log(N)M(\log(N)))$ bit operations, which is again assumed to cost at most $O(\log(N))$ group operations. □

Due to this method, small primes give no added security in discrete logarithm systems. Hence one generally uses elements of prime order r for cryptography.

Exercise 13.2.6. Recall the Tonelli-Shanks algorithm for computing square roots modulo p from Section 2.9. A key step of the algorithm is to find a solution j to the equation $b = y^{2j} \pmod p$ where y has order 2^e. Write down the Pohlig-Hellman method to solve this problem. Show that the complexity is $O(\log(p)^2 M(\log(p)))$ bit operations.

Exercise 13.2.7. Let $B \in \mathbb{N}_{>3}$. Let $N = \prod_{i=1}^n x_i$ where $2 \leq x_i \leq B$. Prove that $\sum_{i=1}^n x_i \leq B\log(N)/\log(B)$.

Hence, show that the Pohlig-Hellman method performs $O(\log(N)^2 + B\log(N)/\log(B))$ group operations.

Remark 13.2.8. As we will see, replacing exhaustive search by the baby-step-giant-step algorithm improves the complexity to $O(\log(N)^2 + \sqrt{B}\log(N)/\log(B))$ group operations (at the cost of more storage).

Algorithm 13 can be improved, when there is a prime power l^e dividing N with e large, by structuring it differently. Section 11.2.3 of Shoup [556] gives a method to compute the DLP in a group of order l^e in $O(e\sqrt{l} + e\log(e)\log(l))$ group operations (this is using baby-step-giant-step rather than exhaustive search). Algorithm 1 and Corollary 1 of Sutherland [598] give an algorithm that requires

$$O(e\sqrt{l} + e\log(l)\log(e)/\log(\log(e))) \tag{13.1}$$

[2] By this we mean that the constant implicit in the $O(\cdot)$ is independent of B and N.

group operations. Sutherland also considers non-cyclic groups.

If N is B-smooth then summing the improved complexity statements over the prime powers dividing N gives

$$O(\log(N)\sqrt{B}/\log(B) + \log(N)\log(\log(N))) \tag{13.2}$$

group operations for the DLP (it is not possible to have a denominator of $\log(\log(\log(N)))$ since not all the primes dividing N necessarily appear with high multiplicity).

13.3 Baby-Step-Giant-Step (BSGS) Method

This algorithm, usually credited to Shanks[3], exploits an idea called the time/memory tradeoff. Suppose g has prime order r and that $h = g^a$ for some $0 \leq a < r$. Let $m = \lceil \sqrt{r} \rceil$. Then there are integers a_0, a_1 such that $a = a_0 + ma_1$ and $0 \leq a_0, a_1 < m$. It follows that

$$g^{a_0} = h(g^{-m})^{a_1}$$

and this observation leads to Algorithm 14. The algorithm requires storing a large list of values and it is important, in the second stage of the algorithm, to be able to efficiently determine whether or not an element lies in the list. There are a number of standard solutions to this problem including using binary trees, hash tables, or sorting the list after line 7 of the algorithm (see, for example, parts II and III of [146] or Section 6.3 of [317]).

Algorithm 14 Baby-step-giant-step (BSGS) algorithm

INPUT: $g, h \in G$ of order r
OUTPUT: a such that $h = g^a$, or $\perp$
1: $m = \lceil \sqrt{r} \rceil$
2: Initialise an easily searched structure (such as a binary tree or a hash table) L
3: $x = 1$
4: **for** $i = 0$ to m **do** ▷ Compute baby steps
5: store (x, i) in L, easily searchable on the first coordinate
6: $x = xg$
7: **end for**
8: $u = g^{-m}$
9: $y = h$, $j = 0$
10: **while** $(y, \star) \notin L$ **do** ▷ Compute giant steps
11: $y = yu$, $j = j + 1$
12: **end while**
13: **if** $\exists (x, i) \in L$ such that $x = y$ **then**
14: **return** $i + mj$
15: **else**
16: **return** $\perp$
17: **end if**

Note that the BSGS algorithm is deterministic. The algorithm also solves the decision problem (is $h \in \langle g \rangle$?) though, as discussed in Section 11.6, there are usually faster solutions to the decision problem.

Theorem 13.3.1. *Let G be a group of order r. Suppose that elements of G are represented using $O(\log(r))$ bits and that the group operations can be performed in $O(\log(r)^2)$ bit*

[3]Nechaev [452] states it was known to Gel'fond in 1962.

operations. The BSGS algorithm for the DLP in G has running time $O(\sqrt{r}\log(r)^2)$ bit operations. The algorithm requires $O(\sqrt{r}\log(r))$ bits of storage.

Proof: The algorithm computes $\sqrt{r}$ group operations for the baby steps. The cost of inserting each group element into the easily searched structure is $O(\log(r)^2)$ bit operations, since comparisons require $O(\log(r))$ bit operations (this is where the assumption on the size of element representations appears). The structure requires $O(\sqrt{r}\log(r))$ bits of storage.

The computation of $u = g^{-m}$ in line 8 requires $O(\log(r))$ group operations.

The algorithm needs one group operation to compute each giant step. Searching the structure takes $O(\log(r)^2)$ bit operations. In the worst case one has to compute m giant steps. The total running time is therefore $O(\sqrt{r}\log(r)^2)$ bit operations. □

The storage requirement of the BSGS algorithm quickly becomes prohibitive. For example, one can work with primes r such that $\sqrt{r}$ is more than the number of fundamental particles in the universe!

Remark 13.3.2. When solving the DLP it is natural to implement the group operations as efficiently as possible. For example, when using elliptic curves it would be tempting to use a projective representation for group elements (see Exercise 13.1.2). However this is not suitable for the BSGS method (or the rho and kangaroo methods) as one cannot efficiently detect a match $y \in L$ when there is a non-unique representation for the group element y.

Exercise 13.3.3. On average, the baby-step-giant-step algorithm finds a match after half the giant steps have been performed. The average-case running time of the algorithm as presented is therefore approximately $1.5\sqrt{r}$ group operations. Show how to obtain an algorithm that requires, in the average case, approximately $\sqrt{2r}$ group operations and $\sqrt{r/2}$ group elements of storage.

Exercise 13.3.4. (Pollard [488]) A variant of the baby-step-giant-step algorithm is to compute the baby steps and giant steps in parallel, storing the points together in a single structure. Show that if x and y are chosen uniformly in the interval $[0, r] \cap \mathbb{Z}$ then the expected value of $\max\{x, y\}$ is approximately $\frac{2}{3}r$. Hence, show that the average-case running time of this variant of the baby-step-giant-step algorithm is $\frac{4}{3}\sqrt{r}$ group operations.

Chateauneuf, Ling and Stinson [129] have studied a combinatorial abstraction that would lead to an optimal baby-step-giant-step algorithm. However their model minimises the total number of *exponentiations* in the group, rather than the total number of group operations, and so is not faster in practice than the methods in this section.

Exercise 13.3.5. Design a variant of the BSGS method that requires $O(r/M)$ group operations if the available storage is only for $M < \sqrt{r}$ group elements.

Exercise 13.3.6. (DLP in an interval) Suppose one is given g of order r in a group G and integers $0 \leq b, w < r$. The DLP in an interval of length w is: Given $h \in \langle g \rangle$ such that $h = g^a$ for some $b \leq a < b + w$, to find a. Give a baby-step-giant-step algorithm to find a in average-case $\sqrt{2w}$ group operations and $\sqrt{w/2}$ group elements of storage.

Exercise 13.3.7. Suppose one considers the DLP in a group G where computing the inverse g^{-1} is much faster than multiplication in the group. Show how to solve the DLP in an interval of length w using a baby-step-giant-step algorithm in approximately $\sqrt{w}$ group operations in the average case.

Exercise 13.3.8. Suppose one is given $g, h \in G$ and $w, b, m \in \mathbb{N}$ such that $h = g^a$ for some integer a satisfying $0 \leq a < w$ and $a \equiv b \pmod{m}$. Show how to reduce this problem to the problem of solving a DLP in an interval of length $\lceil w/m \rceil$.

Exercise 13.3.9. Let $g \in G$ have order $N = mr$ where r is prime and m is $\log(N)$-smooth. Suppose $h = g^x$ and w are given such that $0 \leq x < w$. Show how one can compute x by combining the Pohlig-Hellman method and the BSGS algorithm in $O(\log(N)^2 + \sqrt{w/m})$ group operations.

Exercise 13.3.10. Suppose one is given $g, h \in G$ and $b_1, b_2, w \in \mathbb{Z}$ ($w > 0$) such that $b_1 + w < b_2$ and $h = g^a$ for some integer a satisfying either $b_1 \leq a < b_1 + w$ or $b_2 \leq a < b_2 + w$. Give an efficient BSGS algorithm for this problem.

Exercise 13.3.11. Let $g \in G$ where the order of g and G are not known. Suppose one is given integers b, w such that the order of g lies in the interval $[b, b + w)$. Explain how to use the BSGS method to compute the order of g.

Exercise 13.3.12.★ Suppose one is given an element g of order r and $h_1, \ldots, h_n \in \langle g \rangle$. Show that one can solve the DLP of all n elements h_i to the base g in approximately $2\sqrt{nr}$ group operations (optimised for the worst case) or approximately $\sqrt{2nr}$ (optimised for the average case).

Exercise 13.3.13.★ Suppose one is given $g \in G$ of order r, an integer w, and an instance generator for the discrete logarithm problem that outputs $h = g^a \in G$ such that $0 \leq a < w$ according to some known distribution on $\{0, 1, \ldots, w-1\}$. Assume that the distribution is symmetric with mean value $w/2$. Determine the optimal baby-step-giant-step algorithm to solve such a problem.

Exercise 13.3.14.★ Suppose one is given $g, h \in G$ and $n \in \mathbb{N}$ such that $h = g^a$ where a has a representation as a non-adjacent form NAF (see Section 11.1.1) of length $n < \log_2(r)$. Give an efficient BSGS algorithm to find a. What is the running time?

13.4 Lower Bound on Complexity of Generic Algorithms for the DLP

This section presents a lower bound for the complexity of the discrete logarithm problem in groups of prime order for algorithms that do not exploit the representation of the group; such algorithms are called generic algorithms. The main challenge is to formally model such algorithms. Babai and Szemerédi [19] defined a black box group to be a group with elements represented (not necessarily uniquely) as binary strings and where multiplication, inversion and testing whether an element is the identity are all performed using oracles. Nechaev [452] used a different model (for which equality testing does not require an oracle query) and obtained $\Omega(\sqrt{r})$ time and space complexity.

Nechaev's paper concerns deterministic algorithms, and so his result does not cover the Pollard algorithms. Shoup [553] gave yet another model for generic algorithms (his model allows randomised algorithms) and proved $\Omega(\sqrt{r})$ time complexity for the DLP and some related problems. This lower bound is often called the **birthday bound** on the DLP.

Shoup's formulation has proven to be very popular with other authors and so we present it in detail. We also describe the model of generic algorithms by Maurer [404]. Further results in this area, and extensions of the generic algorithm model (such as working with groups of composite order, working with groups endowed with pairings, providing

access to decision oracles etc), have been given by Maurer and Wolf [407], Maurer [404], Boneh and Boyen [76, 77], Boyen [95], Rupp, Leander, Bangerter, Dent and Sadeghi [507].

13.4.1 Shoup's Model for Generic Algorithms

Fix a constant $t \in \mathbb{R}_{>0}$. When G is the group of points on an elliptic curve of prime order (and log means $\log_2$ as usual) one can take $t = 2$.

Definition 13.4.1. An **encoding** of a group G of order r is an injective function $\sigma : G \to \{0,1\}^{\lceil t \log(r) \rceil}$.

A **generic algorithm** for a computational problem in a group G of order r is a probabilistic algorithm that takes as input r and $(\sigma(g_1), \ldots, \sigma(g_k))$ such that $g_1, \ldots, g_k \in G$ and returns a sequence $(a_1, \ldots, a_l, \sigma(h_1), \ldots, \sigma(h_m))$ for some $a_1, \ldots, a_l \in \mathbb{Z}/r\mathbb{Z}$ and $h_1, \ldots, h_m \in G$ (depending on the computational problem in question). The generic algorithm is given access to a perfect oracle O such that $O(\sigma(g_1), \sigma(g_2))$ returns $\sigma(g_1 g_2^{-1})$.

Note that one can obtain the encoding $\sigma(1)$ of the identity element by $O(\sigma(g_1), \sigma(g_1))$. One can then compute the encoding of g^{-1} from the encoding of g as $O(\sigma(1), \sigma(g))$. Defining $O'(\sigma(g_1), \sigma(g_2)) = O(\sigma(g_1), O(\sigma(1), \sigma(g_2)))$ gives an oracle for multiplication in G.

Example 13.4.2. A generic algorithm for the DLP in $\langle g \rangle$ where g has order r takes input $(r, \sigma(g), \sigma(h))$ and outputs a such that $h = g^a$. A generic algorithm for CDH (see Definition 20.2.1) takes input $(\sigma(g), \sigma(g^a), \sigma(g^b))$ and outputs $\sigma(g^{ab})$.

In Definition 13.4.1 we insisted that a generic algorithm take as input the order of the group, but this is not essential. Indeed, it is necessary to relax this condition if one wants to consider generic algorithms for, say, $(\mathbb{Z}/N\mathbb{Z})^*$ when N is an integer of unknown factorisation. To do this one considers an encoding function to $\{0,1\}^l$ and it follows that the order r of the group is at most 2^l. If the order is not given then one can consider a generic algorithm whose goal is to compute the order of a group. Theorem 2.3 and Corollary 2.4 of Sutherland [596] prove an $\Omega(r^{1/3})$ lower bound on the complexity of a generic algorithm to compute the order r of a group, given a bound M such that $\sqrt{M} < r < M$.

13.4.2 Maurer's Model for Generic Algorithms

Maurer's formulation of generic algorithms [404] does not use any external representation of group elements (in particular, there are no randomly chosen encodings). Maurer considers a black box containing registers, specified by indices $i \in \mathbb{N}$, that store group elements. The model considers a set of operations and a set of relations. An oracle query $O(op, i_1, \ldots, i_{t+1})$ causes register i_{t+1} to be assigned the value of the t-ary operation op on the values in registers $i_1, \ldots, i_t$. Similarly, an oracle query $O(R, i_1, \ldots, i_t)$ returns the value of the t-ary relation R on the values in registers $i_1, \ldots, i_t$.

A **generic algorithm** in Maurer's model is an algorithm that takes as input the order of the group (as with Shoup's model, the order of the group can be omitted), makes oracle queries, and outputs the value of some function of the registers (for example, the value of one of the registers; Maurer calls such an algorithm an "extraction algorithm").

Example 13.4.3. To define a generic algorithm for the DLP in Maurer's model one imagines a black box that contains in the first register the value 1 (corresponding to g) and in the second register the value a (corresponding to $h = g^a$). Note that the black box contains is viewed as containing the additive group $\mathbb{Z}/r\mathbb{Z}$. The algorithm has access

to an oracle $O(+,i,j,k)$ that assigns register k the sum of the elements in registers i and j, an oracle $O(-,i,j)$ that assigns register j the inverse of the element in register i, and an oracle $O(=,i,j)$ that returns 'true' if and only if registers i and j contain the same group element. The goal of the generic algorithm for the DLP is to output the value of the second register.

To implement the baby-step-giant-step algorithm or Pollard rho algorithm in Maurer's model it is necessary to allow a further oracle that computes a well-ordering relation on the group elements.

We remark that the Shoup and Maurer models have been used to prove the security of cryptographic protocols against adversaries that behave like generic algorithms. Jager and Schwenk [308] have shown that both models are equivalent for this purpose.

13.4.3 The Lower Bound

We present the main result of this section using Shoup's model. A similar result can be obtained using Maurer's model (except that it is necessary to either ignore the cost of equality queries or else allow a total order relation on the registers).

We start with a result attributed by Shoup to Schwarz. In this section we only use the result when $k = 1$, but the more general case is used later in the book.

Lemma 13.4.4. *Let $F(x_1,\ldots,x_k) \in \mathbb{F}_r[x_1,\ldots,x_k]$ be a non-zero polynomial of total degree d. Then for $P = (P_1,\ldots,P_k)$ chosen uniformly at random in $\mathbb{F}_r^k$ the probability that $F(P_1,\ldots,P_k) = 0$ is at most d/r.*

Proof: If $k = 1$ then the result is standard. We prove the result by induction on k. Write

$$F(x_1,\ldots,x_k) = F_e(x_1,\ldots,x_{k-1})x_k^e + F_{e-1}(x_1,\ldots,x_{k-1})x_k^{e-1} + \cdots + F_0(x_1,\ldots,x_{k-1})$$

where $F_i(x_1,\ldots,x_{k-1}) \in \mathbb{F}_r[x_1,\ldots,x_{k-1}]$ has total degree $\leq d-i$ for $0 \leq i \leq e$ and $e \leq d$. If $P = (P_1,\ldots,P_{k-1}) \in \mathbb{F}_r^{k-1}$ is such that all $F_i(P) = 0$ then all r choices for P_k lead to a solution. The probability of this happening is at most $(d-e)/r$ (this is the probability that $F_e(P) = 0$). On the other hand, if some $F_i(P) \neq 0$ then there are at most e choices for P_k that give a root of the polynomial. The total probability is therefore $\leq (d-e)/r + e/r = d/r$. □

Theorem 13.4.5. *Let G be a cyclic group of prime order r. Let A be a generic algorithm for the DLP in G that makes at most m oracle queries. Then the probability, over uniformly chosen $a \in \mathbb{Z}/r\mathbb{Z}$ and uniformly chosen encoding function $\sigma : G \to \{0,1\}^{\lceil t\log(r)\rceil}$, that $A(\sigma(g),\sigma(g^a)) = a$ is $O(m^2/r)$.*

Proof: Instead of choosing a random encoding function in advance, the method of proof is to create the encodings "on the fly". The algorithm to produce the encodings is called the simulator. We also do not choose the instance of the DLP until the end of the game. The simulation will be perfect unless a certain bad event happens, and we will analyse the probability of this event.

Let $S = \{0,1\}^{\lceil t\log(r)\rceil}$. The simulator begins by uniformly choosing two distinct σ_1, σ_2 in S and running $A(\sigma_1,\sigma_2)$. Algorithm A assumes that $\sigma_1 = \sigma(g)$ and $\sigma_2 = \sigma(h)$ for some $g, h \in G$ and some encoding function σ, but it is not necessary for the simulator to fix values for g and h.

It is necessary to ensure that the encodings are consistent with the group operations. This cannot be done perfectly without choosing g and h, but the following idea takes care of "trivial" consistency. The simulator maintains a list of pairs (σ_i, F_i) where $\sigma_i \in S$

and $F_i \in \mathbb{F}_r[x]$. The initial values are $(\sigma_1, 1)$ and (σ_2, x). Whenever A makes an oracle query on (σ_i, σ_j) the simulator computes $F = F_i - F_j$. If F appears as F_k in the list of pairs then the simulator replies with σ_k and does not change the list. Otherwise, a $\sigma \in S$ distinct from the previously used values is chosen uniformly at random, (σ, F) is added to the simulator's list, and σ is returned to A.

After making at most m oracle queries A outputs $b \in \mathbb{Z}/r\mathbb{Z}$. The simulator now chooses a uniformly at random in $\mathbb{Z}/r\mathbb{Z}$. Algorithm A wins if $b = a$.

Let the simulator's list contain precisely k polynomials $\{F_1(x), \ldots, F_k(x)\}$ for some $k \leq m + 2$. Let E be the event that $F_i(a) = F_j(a)$ for some pair $1 \leq i < j \leq k$. The probability that A wins is

$$\Pr(A \text{ wins } | E) \Pr(E) + \Pr(A \text{ wins } | \neg E) \Pr(\neg E). \tag{13.3}$$

For each pair $1 \leq i < j \leq k$ the probability that $(F_i - F_j)(a) = 0$ is $1/r$ by Lemma 13.4.4. Hence, the probability of event E is at most $k(k-1)/2r = O(m^2/r)$. On the other hand, if event E does not occur then all A 'knows' about a is that it lies in the set $\mathcal{X}$ of possible values for a for which $F_i(a) \neq F_j(a)$ for all $1 \leq i < j \leq k$. Let $N = \#\mathcal{X} \approx r - m^2/2$ Then $\Pr(\neg E) = N/r$ and $\Pr(A \text{ wins } | \neg E) = 1/N$.

Putting it all together, the probability that A wins is $O(m^2/r)$. □

Exercise 13.4.6. Prove Theorem 13.4.5 using Maurer's model for generic algorithms. [Hint: The basic method of proof is exactly the same. The difference is in formulation and analysis of the success probability.]

Corollary 13.4.7. *Let A be a generic algorithm for the DLP. If A succeeds with noticeable probability $1/\log(r)^c$ for some $c > 0$ then A must make $\Omega(\sqrt{r/\log(r)^c})$ oracle queries.*

13.5 Generalised Discrete Logarithm Problems

A number of generalisations of the discrete logarithm problem have been proposed over the years. The motivation for such problems varies: sometimes the aim is to enable new cryptographic functionalities; other times the aim is to generate hard instances of the DLP more quickly than previous methods.

Definition 13.5.1. Let G be a finitely generated Abelian group. The **multidimensional discrete logarithm problem** or **representation problem**[4] is: given $g_1, g_2, \ldots, g_l, h \in G$ and $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l \subseteq \mathbb{Z}$ to find $a_j \in \mathcal{S}_j$ for $1 \leq j \leq l$, if they exist, such that

$$h = g_1^{a_1} g_2^{a_2} \cdots g_l^{a_l}.$$

The **product discrete logarithm problem**[5] is: given $g, h \in G$ and $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l \subseteq \mathbb{Z}$ to find $a_j \in \mathcal{S}_j$ for $1 \leq j \leq l$, if they exist, such that

$$h = g^{a_1 a_2 \cdots a_l}.$$

Remark 13.5.2. A natural variant of the product DLP is to compute only the product $a_1 a_2 \cdots a_l$ rather than the l-tuple $(a_1, \ldots, a_l)$. This is just the DLP with respect to a specific instance generator (see the discussion in Section 2.1.2). Precisely, consider an instance generator that, on input a security parameter κ, outputs a group element g of prime order r and then chooses $a_j \in \mathcal{S}_j$ for $1 \leq j \leq l$ and computes $h = g^{a_1 a_2 \cdots a_l}$. The stated variant of the product DLP is the DLP with respect to this instance generator.

[4] This computational problem seems to be first explicitly stated in the work of Brands [97] from 1993, in the case $\mathcal{S}_i = \mathbb{Z}$.

[5] The idea of using product exponents for improved efficiency appears in Knuth [343] where it is called the "factor method".

Note that the representation problem can be defined whether or not $G = \langle g_1, \ldots, g_l \rangle$ is cyclic. The solution to Exercise 13.5.4 applies in all cases. However, there may be other ways to tackle the non-cyclic case (e.g., exploiting efficiently computable group homomorphisms, see [231] for example), so the main interest is the case when G is cyclic of prime order r.

Example 13.5.3. The representation problem can arise when using the GLV method (see Section 11.3.3) with intentionally small coefficients. In this case, $g_2 = \psi(g_1)$, $\langle g_1, g_2 \rangle$ is a cyclic group of order r, and $h = g_1^{a_1} g_2^{a_2}$ where $0 \leq a_1, a_2 < w \leq \sqrt{r}$).

The number of possible choices for h in both the representation problem and product DLP is at most $\prod_{j=1}^{l} \#\mathcal{S}_j$ (it could be smaller if the same h can arise from many different combinations of $(a_1, \ldots, a_l)$). If l is even and $\#\mathcal{S}_j = \#\mathcal{S}_1$ for all j then there is an easy time/memory tradeoff algorithm requiring $O(\#\mathcal{S}_1^{l/2})$ group operations.

Exercise 13.5.4. Write down an efficient BSGS algorithm to solve the representation problem. What is the running time and storage requirement?

Exercise 13.5.5. Give an efficient BSGS algorithm to solve the product DLP. What is the running time and storage requirement?

It is natural to ask whether one can do better than the naive baby-step-giant-step algorithms for these problems, at least for certain values of l. The following result shows that the answer in general turns out to be "no".

Lemma 13.5.6. *Assume l is even and $\#\mathcal{S}_j = \#\mathcal{S}_1$ for all $2 \leq j \leq l$. A generic algorithm for the representation problem with noticeable success probability $1/\log(\#\mathcal{S}_1)^c$ needs $\Omega(\#\mathcal{S}_1^{l/2}/\log(\#\mathcal{S}_1)^{c/2})$ group operations.*

Proof: Suppose A is a generic algorithm for the representation problem. Let G be a group of order r and let $g, h \in G$. Set $m = \lceil r^{1/l} \rceil$, $\mathcal{S}_j = \{a \in \mathbb{Z} : 0 \leq a < m\}$ and let $g_j = g^{m^j}$ for $0 \leq j \leq l-1$. If $h = g^a$ for some $a \in \mathbb{Z}$ then the base m-expansion $a_0 + a_1 m + \cdots + a_{l-1} m^{l-1}$ is such that

$$h = g^a = \prod_{j=0}^{l-1} g_j^{a_j}.$$

Hence, if A solves the representation problem then we have solved the DLP using a generic algorithm. Since we have shown that a generic algorithm for the DLP with success probability $1/\log(\#\mathcal{S}_1)^c$ needs $\Omega(\sqrt{r/\log(\#\mathcal{S}_1)^c})$ group operations, the result is proved. □

13.6 Low Hamming Weight DLP

Recall that the **Hamming weight** of an integer is the number of ones in its binary expansion.

Definition 13.6.1. Let G be a group and let $g \in G$ have prime order r. The **low Hamming weight DLP** is: Given $h \in \langle g \rangle$ and integers n, w to find a integer a (if it exists) whose binary expansion has length $\leq n$ and Hamming weight $\leq w$ such that $h = g^a$.

This definition makes sense even for $n > \log_2(r)$. For example, squaring is faster than multiplication in most representations of algebraic groups, so it could be more efficient to compute g^a by taking longer strings with fewer ones in their binary expansion.

Coppersmith developed a time/memory tradeoff algorithm to solve this problem. A thorough treatment of these ideas was given by Stinson in [591]. Without loss of generality we assume that n and w are even (just add one to them if not).

The idea of the algorithm is to reduce solving $h = g^a$ where a has length n and Hamming weight w to solving $hg^{-a_2} = g^{a_1}$ where a_1 and a_2 have Hamming weight $w/2$. One does this by choosing a set $B \subset I = \{0, 1, \ldots, n-1\}$ of size $n/2$. The set B is the set of possible bit positions for the bits of a_1 and $(I - B)$ is the possible bit positions for the bits of a_2. The detailed algorithm is given in Algorithm 15. Note that one can compactly represent subsets $Y \subseteq I$ as n-bit strings.

Algorithm 15 Coppersmith's baby-step-giant-step algorithm for the low Hamming weight DLP

INPUT: $g, h \in G$ of order r, n and w
OUTPUT: a of bit-length n and Hamming weight w such that $h = g^a$, or $\perp$

```
Choose B ⊂ {0,...,n-1} such that #B = n/2
Initialise an easily searched structure (such as a binary tree, a heap, or a hash table) L
for Y ⊆ B : #Y = w/2 do
    Compute b = Σ_{j∈Y} 2^j and x = g^b
    store (x, Y) in L ordered according to first coordinate
end for
for Y ⊆ (I - B) : #Y = w/2 do
    Compute b = Σ_{j∈Y} 2^j and y = hg^{-b}
    if y = x for some (x, Y_1) ∈ L then
        a = Σ_{j∈Y∪Y_1} 2^j
        return a
    end if
end for
return ⊥
```

Exercise 13.6.2. Write down an algorithm, to enumerate all $Y \subset B$ such that $\#Y = w/2$, which requires $O(\binom{n/2}{w/2}n)$ bit operations.

Lemma 13.6.3. *The running time of Algorithm 15 is $O(\binom{n/2}{w/2})$ group operations and the algorithm requires $O(\binom{n/2}{w/2})$ group elements of storage.*

Exercise 13.6.4. Prove Lemma 13.6.3.

Algorithm 15 is not guaranteed to succeed, since the set B might not exactly correspond to a splitting of the bit positions of the integer a into two sets of Hamming weight $\leq w/2$. We now give a collection of subsets of I that is guaranteed to contain a suitable B.

Definition 13.6.5. Fix even integers n and w. Let $I = \{0, \ldots, n-1\}$. A **splitting system** is a set $\mathcal{B}$ of subsets of I of size $n/2$ such that for every $Y \subset I$ such that $\#Y = w$ there is a set $B \in \mathcal{B}$ such that $\#(B \cap Y) = w/2$.

Lemma 13.6.6. *For any even integers n and w there exists a splitting system $\mathcal{B}$ of size $n/2$.*

Proof: For $0 \leq i \leq n-1$ define

$$B_i = \{i + j \pmod{n} : 0 \leq j \leq n/2 - 1\}$$

and let $\mathcal{B} = \{B_i : 0 \leq i \leq n/2 - 1\}$.

To show $\mathcal{B}$ is a splitting system, fix any $Y \subset I$ of size w. Define $\nu(i) = \#(Y \cap B_i) - \#(Y \cap (I - B_i)) \in \mathbb{Z}$ for $0 \leq i \leq n/2 - 1$. One can check that $\nu(i)$ is even, that $\nu(n/2) = -\nu(0)$ and that $\nu(i+1) - \nu(i) \in \{-2, 0, 2\}$. Hence, either $\nu(0) = 0$, or else the values $\nu(i)$ change sign at least once as i goes from 0 to $n/2$. It follows that there exists some $0 \leq i \leq n/2$ such that $\nu(i) = 0$, in which case $\#(Y \cap B_i) = w/2$. □

One can run Algorithm 15 for all $n/2$ sets B in the splitting system $\mathcal{B}$ of Lemma 13.6.6. This gives a deterministic algorithm with running time $O(n\binom{n/2}{w/2})$ group operations. Stinson proposes different splitting systems giving a deterministic algorithm requiring $O(w^{3/2}\binom{n/2}{w/2})$ group operations. A more efficient randomised algorithm (originally proposed by Coppersmith) is to randomly choose sets B from the $\binom{n}{n/2}$ possible subsets of $\{0, \ldots, n-1\}$ of size $n/2$. Theorem 13.6.9 determines the expected running time in this case.

Lemma 13.6.7. *Fix a set $Y \subset \{0, \ldots, n-1\}$ such that $\#Y = w$. The probability that a randomly chosen $B \subseteq \{0, \ldots, n-1\}$ having $\#B = n/2$ satisfies $\#(Y \cap B) = w/2$ is*

$$p_{Y,B} = \binom{w}{w/2}\binom{(n-w)}{(n-w)/2} / \binom{n}{n/2}.$$

Exercise 13.6.8. Prove Lemma 13.6.7.

Theorem 13.6.9. *The expected running time for the low Hamming weight DLP when running Algorithm 15 on randomly chosen sets B is $O(\sqrt{w}\binom{n/2}{w/2})$ exponentiations. The storage is $O(\binom{n/2}{w/2})$ group elements.*

Proof: We expect to repeat the algorithm $1/p_{Y,B}$ times. One can show, using the fact $2^k/\sqrt{2k} \leq \binom{k}{k/2} \leq 2^k\sqrt{2/\pi k}$, that $1/p_{Y,B} \leq c\sqrt{w}$ for some constant (see Stinson [591]). The result follows. □

Exercise 13.6.10. As with all baby-step-giant-step methods, the bottleneck for this method is the storage requirement. Show how to modify the algorithm for the case where only M group elements of storage are available.

Exercise 13.6.11. Adapt Coppersmith's algorithm to the DLP for low weight signed expansions (for example, NAFs, see Section 11.1.1).

All the algorithms in this section have large storage requirements. An approach due to van Oorschot and Wiener for solving such problems using less storage is presented in Section 14.8.1.

13.7 Low Hamming Weight Product Exponents

Let G be an algebraic group (or algebraic group quotient) over $\mathbb{F}_p$ (p small) and let $g \in G(\mathbb{F}_{p^n})$ with $n > 1$. Let π_p be the p-power Frobenius on G, acting on G as $g \mapsto g^p$. Hoffstein and Silverman [290] proposed computing random powers of g efficiently by taking products of low Hamming weight Frobenius expansions.

In particular, for Koblitz elliptic curves (i.e., $p = 2$) they suggested using three sets and taking $\mathcal{S}_j$ for $1 \leq j \leq 3$ to be the set of Frobenius expansions of length n and weight 7. The baby-step-giant-step algorithm in Section 13.5 applies to this problem, but the running time is not necessarily optimal since $\#\mathcal{S}_1 \#\mathcal{S}_2 \neq \#\mathcal{S}_3$. Kim and Cheon [338] generalised the results of Section 13.6 to allow a more balanced time/memory tradeoff. This gives a small improvement to the running time.

Cheon and Kim [134] give a further improvement to the attack, which is similar to the use of equivalence classes in Pollard rho (see Section 14.4). They noted that the sets $\mathcal{S}_j$ in the Hoffstein-Silverman proposal have the property that for every $a \in \mathcal{S}_j$ there is some $a' \in \mathcal{S}_j$ such that $g^{a'} = \pi_p(g^a)$. In other words, π_p permutes $\mathcal{S}_j$ and each element $a \in \mathcal{S}_j$ lies in an orbit of size n under this permutation. Cheon and Kim define a unique representative of each orbit of π_p in $\mathcal{S}_j$ and show how to speed up the BSGS algorithm in this case by a factor of n.

Exercise 13.7.1. ★ Give the details of the Cheon-Kim algorithm. How many group operations does the algorithm perform when $n = 163$ and three sets with $w = 7$ are used?

13.8 Wagner's Generalised Birthday Algorithm

This section presents an algorithm due to Wagner [625] (though a special case was discovered earlier by Camion and Patarin), which has a similar form to the baby-step-giant-step algorithm. This algorithm is not useful for solving the DLP in groups of relevance to public key cryptography, but it is an example of how a non-generic algorithm can beat the birthday bound. Further examples of non-generic algorithms that beat the birthday bound are given in Chapter 15. For reasons of space we do not present all the details.

Definition 13.8.1. Suppose one is given large sets L_j of n-bit strings, for $1 \leq j \leq l$. The **l-sum problem** is to find $x_j \in L_j$ for $1 \leq j \leq l$ such that

$$x_1 \oplus x_2 \oplus \cdots \oplus x_l = 0, \tag{13.4}$$

where 0 denotes the n-bit all zero string.

The l-sum problem is easy if $0 \in L_i$ for all $0 \leq i \leq l$. Another relatively easy case is if l is even and $L_{2i-1} \cap L_{2i} \neq \varnothing$ for all $1 \leq i \leq l/2$. Hence, the l-sum problem is of most interest when the sets L_i are chosen independently and at random. By the coupon collector theorem (Example A.14.3) one expects a solution to exist when $\#L_1 \cdots \#L_l > 2^n \log(n)$ if the L_j are sufficiently random.

Exercise 13.8.2. Give a baby-step-giant-step algorithm to solve this problem when $l = 2$.

Exercise 13.8.3. Give an example of sets L_1, L_2 of n-bit strings such that $\#L_1, \#L_2 > 2^{\lceil n/2 \rceil}$ but there is no solution to the 2-sum problem.

We now sketch the method in the case $l = 4$. Let $m = \lceil n/3 \rceil$. It will be necessary to assume that $\#L_j \#L_{j+1} \geq 2^{2m}$ (e.g., $\#L_j \geq 2^m$) for each $j = 1, 3$, so this method is not expected to work if $\#L_j \approx 2^{n/4}$ for all $1 \leq j \leq 4$. Define $\mathrm{LSB}_m(x) =$ the m-least significant bits of the bit-string x.

The first step is to form the sets

$$L_{j,j+1} = \{(x_j, x_{j+1}) \in L_j \times L_{j+1} : \mathrm{LSB}_m(x_j \oplus x_{j+1}) = 0\}$$

for $j = 1, 3$. These sets can be formed efficiently. For example, to build $L_{1,2}$: sort the list L_1 (at least, sort with respect to the m least significant bits of each string), then for

each $x_2 \in L_2$ test whether there exists $x_1 \in L_2$ such that $\mathrm{LSB}_m(x_1) = \mathrm{LSB}_m(x_2)$. If the sets L_i are sufficiently random then it is reasonable to suppose that the size of $L_{j,j+1}$ is $\#L_j \# L_{j+1}/2^m \geq 2^m$. To each pair $(x_j, x_{j+1}) \in L_{j,j+1}$ we can associate the $(n-m)$-bit string obtained by removing the m least significant bits of $x_j \oplus x_{j+1}$.

The second step is to find $(x_1, x_2) \in L_{1,2}$ and $(x_3, x_4) \in L_{3,4}$ such that $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$. This is done by sorting the $(n-m)$-bit truncated $x_1 \oplus x_2$ corresponding to $(x_1, x_2) \in L_{1,2}$ and then, for each $(x_3, x_4) \in L_{3,4}$ testing whether the $(n-m)$-bit truncated $x_3 \oplus x_4$ is in the list. Since $\#L_{1,2}, \#L_{3,4} \geq 2^m$ and $n - m \approx 2m$ then, if the sets $L_{j,j+1}$ are sufficiently random, there is a good chance that a solution will exist.

The above arguments lead to the following heuristic result.

Heuristic 13.8.4. Let $n \in \mathbb{N}$ and $m = \lceil n/3 \rceil$. Suppose the sets $L_i \subset \{0,1\}^n$ for $1 \leq i \leq 4$ are randomly chosen and that $\#L_j \# L_{j+1} \geq 2^{2m}$ for $j = 1, 3$. Then Wagner's algorithm should find a solution $(x_1, \ldots, x_4)$ to equation (13.4) in the case $l = 4$. The running time is $\tilde{O}(2^m) = \tilde{O}(2^{n/3})$ bit operations and the algorithm requires $\tilde{O}(2^m) = \tilde{O}(2^{n/3})$ bits of storage.

The algorithm has "cube root" complexity, which beats the usual square-root complexity bound for such problems. The reason is that we are working in the group $(\mathbb{F}_2^n, +)$ and the algorithm is *not* a generic algorithm: it exploits the fact that the group operation and group representation satisfy the property $\mathrm{LSB}_m(x) = \mathrm{LSB}_m(y) \Leftrightarrow \mathrm{LSB}_m(x \oplus y) = 0$.

The algorithm is not expected to succeed in the case when $\#L_j \approx 2^{n/4}$ since it is finding a solution to equation (13.4) of a very special form (namely, that $\mathrm{LSB}_m(x_1 \oplus x_2) = \mathrm{LSB}_m(x_3 \oplus x_4) = 0$).

Exercise 13.8.5. Generalise this algorithm to the case $l = 2^k$. Show that the algorithm is heuristically expected to require time and space $\tilde{O}(l 2^{n/(1+k)})$. What is the minimum size for the L_j (assuming they are all of equal size)?

Exercise 13.8.6. Wagner's algorithm is deterministic, but it is not guaranteed to succeed on a given input. How can one "randomise" Wagner's algorithm so that any instance (with large enough lists) can be solved efficiently with high probability?

The 4-sum problem can be put into a more general framework: Let $\mathcal{S}, \mathcal{S}'$ and $\mathcal{S}''$ be sets such that $\#\mathcal{S}' = N$, fix an element $0 \in \mathcal{S}''$, let $f_1, f_2 : \mathcal{S} \times \mathcal{S} \to \mathcal{S}'$ and $f : \mathcal{S}' \times \mathcal{S}' \to \mathcal{S}''$ be functions. Let $L_1, L_2, L_3, L_4 \subset \mathcal{S}$ be randomly chosen subsets of size $\#L_i \approx N^{1/3}$ and suppose one wants to find $x_j \in L_j$ for $1 \leq j \leq 4$ such that

$$f(f_1(x_1, x_2), f_2(x_3, x_4)) = 0.$$

Wagner's algorithm can be applied to solve this problem if there is a distinguished set $\mathcal{D} \subset \mathcal{S}'$ such that the following five conditions hold:

1. $\#\mathcal{D} \approx N^{2/3}$.
2. $\Pr(f(y_1, y_2) = 0 : y_1, y_2 \leftarrow \mathcal{D}) \approx N^{-2/3}$.
3. $\Pr(f_1(x_1, x_2) \in \mathcal{D} : x_1 \leftarrow L_1, x_2 \leftarrow L_2) \approx \Pr(f_2(x_3, x_4) \in \mathcal{D} : x_3 \leftarrow L_3, x_4 \leftarrow L_4) \approx N^{-1/3}$.
4. For $j = 1, 2$ one can determine, in $\tilde{O}(N^{1/3})$ bit operations, lists

$$L_{J,J+1} = \{(x_J, x_{J+1}) \in L_J \times L_{J+1} : f_j(x_J, x_{J+1}) \in \mathcal{D}\}$$

where $J = 2j - 1$.

5. Given $L_{1,2}$ and $L_{3,4}$ as above one can determine, in $\tilde{O}(N^{1/3})$ bit operations,

$$\{((x_1, x_2), (x_3, x_4)) \in L_{1,2} \times L_{3,4} : f(f_1(x_1, x_2), f_2(x_3, x_4)) = 0\}.$$

Exercise 13.8.7. Show that the original Wagner algorithm for $\mathcal{S} = \mathcal{S}' = \mathcal{S}'' = \{0,1\}^n$ fits this formulation. What is the set $\mathcal{D}$?

Exercise 13.8.8. Describe Wagner's algorithm in the more general formulation.

Exercise 13.8.9. Let $\mathcal{S} = \mathcal{S}' = \mathcal{S}''$ be the additive group $(\mathbb{Z}/N\mathbb{Z}, +)$ of integers modulo N. Let $L_1, L_2, L_3, L_4 \subset \mathbb{Z}/N\mathbb{Z}$ be such that $\#L_i \approx N^{1/3}$. Let $f_1(x_1, x_2) = f_2(x_1, x_2) = f(x_1, x_2) = x_1 + x_2 \pmod N$. Let $\mathcal{D} = \{y \in \mathbb{Z} : -N^{2/3}/2 \leq y \leq N^{2/3}/2\}$. Show that the above 5 properties hold in this setting. Can you think of any better method to solve the problem in this setting?

Exercise 13.8.10. Let $\mathcal{S} \subseteq \mathbb{Z}$ and $\mathcal{S}' = \mathcal{S}'' = \mathbb{F}_p$. Let (g_1, g_2, g_3, g_4, h) be an instance of the representation problem in $\mathbb{F}_p^*$. Consider the functions

$$f_1(x_1, x_2) = g_1^{x_1} g_2^{x_2} \pmod p, \quad f_2(x_3, x_4) = h g_3^{-x_3} g_4^{-x_4} \pmod p$$

and $f(y_1, y_2) = y_1 - y_2 \pmod p$. Finding a solution to $f(f_1(x_1, x_2), f_2(x_3, x_4)) = 0$ solves the representation problem.

Let $m = \log_2(p)/3$ and define $\mathrm{LSB}_m(y)$ for $y \in \mathbb{F}_p$ by representing y as an integer in the range $0 \leq y < p$ and outputting the m least significant bits. Let $\mathcal{D} = \{y \in \mathbb{F}_p^* : \mathrm{LSB}_m(y) = 0\}$. Explain that the property 4 of the above list does not seem to hold for this example.

Chapter 14

Factoring and Discrete Logarithms using Pseudorandom Walks

This chapter is devoted to the rho and kangaroo methods for factoring and discrete logarithms (which were invented by Pollard) and some related algorithms. These methods use pseudorandom walks and require low storage (typically a polynomial amount of storage, rather than exponential as in the time/memory tradeoff). Although the rho factoring algorithm was developed earlier than the algorithms for discrete logarithms, the latter are much more important in practice.[1] Hence we focus mainly on the algorithms for the discrete logarithm problem.

As in the previous chapter, we assume G is an algebraic group over a finite field $\mathbb{F}_q$ written in multiplicative notation. To solve the DLP in an algebraic group quotient using the methods in this chapter one would first lift the DLP to the covering group (though see Section 14.4 for a method to speed up the computation of the DLP in an algebraic group by essentially working in a quotient).

14.1 Birthday Paradox

The algorithms in this chapter rely on results in probability theory. The first tool we need is the so-called "birthday paradox". This name comes from the following application,

[1] Pollard's paper [487] contains the remark "We are not aware of any particular need for such index calculations" (i.e., computing discrete logarithms) even though [487] cites the paper of Diffie and Hellman. Pollard worked on the topic before hearing of the cryptographic applications. Hence Pollard's work is an excellent example of research pursued for its intrinsic interest, rather than motivated by practical applications.

which surprises most people: among a set of 23 or more randomly chosen people, the probability that two of them share a birthday is greater than 0.5 (see Example 14.1.4).

Theorem 14.1.1. *Let $\mathcal{S}$ be a set of N elements. If elements are sampled uniformly at random from $\mathcal{S}$ then the expected number of samples to be taken before some element is sampled twice is less than $\sqrt{\pi N/2} + 2 \approx 1.253\sqrt{N}$.*

The element that is sampled twice is variously known as a **repeat**, **match** or **collision**. For the rest of the chapter, we will ignore the +2 and say that the expected number of samples is $\sqrt{\pi N/2}$.

Proof: Let X be the random variable giving the number of elements selected from $\mathcal{S}$ (uniformly at random) before some element is selected twice. After l distinct elements have been selected then the probability that the next element selected is also distinct from the previous ones is $(1 - l/N)$. Hence the probability $\Pr(X > l)$ is given by

$$p_{N,l} = 1(1 - 1/N)(1 - 2/N) \cdots (1 - (l-1)/N).$$

Note that $p_{N,l} = 0$ when $l \geq N$. We now use the standard fact that $1 - x \leq e^{-x}$ for $x \geq 0$. Hence,

$$\begin{aligned} p_{N,l} \leq 1\, e^{-1/N} e^{-2/N} \cdots e^{-(l-1)/N} &= e^{-\sum_{j=0}^{l-1} j/N} \\ &= e^{-\frac{1}{2}(l-1)l/N} \\ &\leq e^{-(l-1)^2/2N}. \end{aligned}$$

By definition, the expected value of X is

$$\begin{aligned} \sum_{l=1}^{\infty} l \Pr(X = l) &= \sum_{l=1}^{\infty} l(\Pr(X > l-1) - \Pr(X > l)) \\ &= \sum_{l=0}^{\infty} (l + 1 - l) \Pr(X > l) \\ &= \sum_{l=0}^{\infty} \Pr(X > l) \\ &\leq 1 + \sum_{l=1}^{\infty} e^{-(l-1)^2/2N}. \end{aligned}$$

We estimate this sum using the integral

$$1 + \int_0^{\infty} e^{-x^2/2N} dx.$$

Since $e^{-x^2/2N}$ is monotonically decreasing and takes values in $[0, 1]$ the difference between the value of the sum and the value of the integral is at most 1. Making the change of variable $u = x/\sqrt{2N}$ gives

$$\sqrt{2N} \int_0^{\infty} e^{-u^2} du.$$

A standard result in analysis (see Section 11.7 of [340] or Section 4.4 of [636]) is that this integral is $\sqrt{\pi}/2$. Hence, the expected value for X is $\leq \sqrt{\pi N/2} + 2$. □

The proof only gives an upper bound on the probability of a collision after l trials. A lower bound of $e^{-l^2/2N - l^3/6N^2}$ for $N \geq 1000$ and $0 \leq l \leq 2N \log(N)$ is given in

Wiener [631]; it is also shown that the expected value of the number of trials is $> \sqrt{\pi N/2} - 0.4$. A more precise analysis of the birthday paradox is given in Example II.10 of Flajolet and Sedgewick [205] and Exercise 3.1.12 of Knuth [343]. The expected number of samples is $\sqrt{\pi N/2} + 2/3 + O(1/\sqrt{N})$.

We remind the reader of the meaning of expected value. Suppose the experiment of sampling elements of a set $\mathcal{S}$ of size N until a collision is found is repeated t times and each time we count the number l of elements sampled. Then the average of l over all trials tends to $\sqrt{\pi N/2}$ as t goes to infinity.

Exercise 14.1.2. Show that the number of elements that need to be selected from $\mathcal{S}$ to get a collision with probability 1/2 is $\sqrt{2\log(2)N} \approx 1.177\sqrt{N}$.

Exercise 14.1.3. One may be interested in the number of samples required when one is particularly unlucky. Determine the number of trials so that with probability 0.99 one has a collision. Repeat the exercise for probability 0.999.

The name "birthday paradox" arises from the following application of the result.

Example 14.1.4. In a room containing 23 or more randomly chosen people, the probability is greater than 0.5 that two people have the same birthday. This follows from $\sqrt{2\log(2)365} \approx 22.49$. Note also that $\sqrt{\pi 365/2} = 23.944\ldots$.

Finally, we mention that the expected number of samples from a set of size N until $k > 1$ collisions are found is approximately $\sqrt{2kN}$. A detailed proof of this fact is given by Kuhn and Struik as Theorem 1 of [355].

14.2 The Pollard Rho Method

Let g be a group element of prime order r and let $G = \langle g \rangle$. The discrete logarithm problem (DLP) is: Given $h \in G$ to find a, if it exists, such that $h = g^a$. In this section we assume (as is usually the case in applications) that one has already determined that $h \in \langle g \rangle$.

The starting point of the rho algorithm is the observation that if one can find $a_i, b_i, a_j, b_j \in \mathbb{Z}/r\mathbb{Z}$ such that

$$g^{a_i} h^{b_i} = g^{a_j} h^{b_j} \tag{14.1}$$

and $b_i \not\equiv b_j \pmod{r}$ then one can solve the DLP as

$$h = g^{(a_i - a_j)(b_j - b_i)^{-1} \pmod{r}}.$$

The basic idea is to generate pseudorandom sequences $x_i = g^{a_i} h^{b_i}$ of elements in G by iterating a suitable function $f : G \to G$. In other words, one chooses a starting value x_1 and defines the sequence by $x_{i+1} = f(x_i)$. A sequence $x_1, x_2, \ldots$ is called a **deterministic pseudorandom walk**. Since G is finite there is eventually a collision $x_i = x_j$ for some $1 \leq i < j$ as in equation (14.1). This is presented as a collision between two elements in the same walk, but it could also be a collision between two elements in different walks. If the elements in the walks look like uniformly and independently chosen elements of G then, by the birthday paradox (Theorem 14.1.1), the expected value of j is $\sqrt{\pi r/2}$.

It is important that the function f be designed so that one can efficiently compute $a_i, b_i \in \mathbb{Z}/r\mathbb{Z}$ such that $x_i = g^{a_i} h^{b_i}$. The next step x_{i+1} depends only on the current step x_i and not on (a_i, b_i). The algorithms all exploit the fact that when a collision

$x_i = x_j$ occurs then $x_{i+t} = x_{j+t}$ for all $t \in \mathbb{N}$. Pollard's original proposal used a cycle-finding method due to Floyd to find a self-collision in the sequence; we present this in Section 14.2.2. A better approach is to use distinguished points to find collisions; we present this in Section 14.2.4.

14.2.1 The Pseudorandom Walk

A true random walk in a finite set $\mathcal{S}$ chooses elements uniformly at random at each stage. In contrast we are concerned with walks whose next step is determined by the current position. Such a walk is given by a function $f : \mathcal{S} \to \mathcal{S}$. Hence, a truly random walk on a finite set means a uniformly chosen function from the set of all functions from $\mathcal{S}$ to itself.

Pollard simulates a random function from G to itself as follows. The first step is to decompose G into n_S disjoint subsets (usually of roughly equal size) so that $G = \mathcal{S}_0 \cup \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_{n_S-1}$. Traditional textbook presentations use $n_S = 3$ but, as explained in Section 14.2.5, it is better to take larger values for n_S; typical values in practice are 32, 256 or 2048.

The sets $\mathcal{S}_i$ are defined using a selection function $S : G \to \{0, \ldots, n_S - 1\}$ by $\mathcal{S}_i = \{g \in G : S(g) = i\}$. For example, in any computer implementation of G one represents an element $g \in G$ as a unique[2] binary string $b(g)$ and interpreting $b(g)$ as an integer one could define $S(g) = b(g) \pmod{n_S}$ (taking n_S to be a power of 2 makes this computation especially easy). To obtain different choices for S one could apply an $\mathbb{F}_2$-linear map L to the sequence of bits $b(g)$, so that $S(g) = L(b(g)) \pmod{n_S}$. These simple methods can be a poor choice in practice, as they are not "sufficiently random". Some other ways to determine the partition are suggested in Section 2.3 of Teske [605] and Bai and Brent [24]. The strongest choice is to apply a hash function or randomness extractor to $b(g)$, though this may lead to an undesirable computational overhead.

Definition 14.2.1. The **rho walks** are defined as follows. Precompute $g_j = g^{u_j} h^{v_j}$ for $0 \leq j \leq n_S - 1$ where $0 \leq u_j, v_j < r$ are chosen uniformly at random. Set $x_1 = g$. The **original rho walk** is

$$x_{i+1} = f(x_i) = \begin{cases} x_i^2 & \text{if } S(x_i) = 0 \\ x_i g_j & \text{if } S(x_i) = j,\ j \in \{1, \ldots, n_S - 1\} \end{cases} \tag{14.2}$$

The **additive rho walk** is

$$x_{i+1} = f(x_i) = x_i g_{S(x_i)}. \tag{14.3}$$

An important feature of the walks is that each step requires only one group operation.

Once the selection function S and the values u_j and v_j are chosen, the walk is deterministic. Even though these values may be chosen uniformly at random, the function f itself is not a random function as it has a compact description. Hence, the rho walks can only be described as pseudorandom. To analyse the algorithm we will consider the expectation of the running time over different choices for the pseudorandom walk. Many authors consider the expectation of the running time over all problem instances and random choices of the pseudorandom walk; they therefore write "expected running time" for what we are calling "average-case expected running time".

It is necessary to keep track of the decomposition

$$x_i = g^{a_i} h^{b_i}.$$

[2] One often uses projective coordinates to speed up elliptic curve arithmetic, so it is natural to use projective coordinates when implementing these algorithms. But to define the pseudorandom walk one needs a unique representation for points, so projective coordinates are not appropriate. See Remark 13.3.2.

The values $a_i, b_i \in \mathbb{Z}/r\mathbb{Z}$ are obtained by setting $a_1 = 1, b_1 = 0$ and updating (for the original rho walk)

$$a_{i+1} = \begin{cases} 2a_i \pmod r & \text{if } S(x_i) = 0 \\ a_i + u_{S(x_i)} \pmod r & \text{if } S(x_i) > 0 \end{cases} \quad \text{and} \quad b_{i+1} = \begin{cases} 2b_i \pmod r & \text{if } S(x_i) = 0 \\ b_i + v_{S(x_i)} \pmod r & \text{if } S(x_i) > 0. \end{cases} \tag{14.4}$$

Putting everything together, we write

$$(x_{i+1}, a_{i+1}, b_{i+1}) = \mathsf{walk}(x_i, a_i, b_i)$$

for the random walk function. But it is important to remember that x_{i+1} only depends on x_i and not on (x_i, a_i, b_i).

Exercise 14.2.2. Give the analogue of equation (14.4) for the additive walk.

14.2.2 Pollard Rho Using Floyd Cycle Finding

We present the original version of Pollard rho. A single sequence $x_1, x_2, \ldots$ of group elements is computed. Eventually there is a collision $x_i = x_j$ with $0 \leq i < j$. One pictures the walk as having a **tail** (which is the part $x_1, \ldots, x_i$ of the walk that is not cyclic) followed by the **cycle** or **head** (which is the part $x_{i+1}, \ldots, x_j$). Drawn appropriately this resembles the shape of the greek letter ρ. The tail and cycle (or head) of such a random walk have expected length $\sqrt{\pi N/8}$ (see Flajolet and Odlyzko [204] for proofs of these, and many other, facts).

The goal is to find integers i and j such that $x_i = x_j$. It might seem that the only approach is to store all the x_i and, for each new value x_j, to check if it appears in the list. This approach would use more memory and time than the baby-step-giant-step algorithm. If one were using a truly random walk then one would have to use this approach. The whole point of using a deterministic walk which eventually becomes cyclic is to enable better methods to find a collision.

Let l_t be the length of the **tail** of the "rho" and l_h be the length of the **cycle** of the "rho". In other words the first collision is

$$x_{l_t + l_h} = x_{l_t}. \tag{14.5}$$

Floyd's cycle finding algorithm[3] is to compare x_i and x_{2i}. Lemma 14.2.3 shows that this will find a collision in at most $l_t + l_h$ steps. The crucial advantage of comparing x_{2i} and x_i is that it only requires storing two group elements. The rho algorithm with Floyd cycle finding is given in Algorithm 16.

Lemma 14.2.3. *Let the notation be as above. Then $x_{2i} = x_i$ if and only if $l_h \mid i$ and $i \geq l_t$. Further, there is some $l_t \leq i < l_t + l_h$ such that $x_{2i} = x_i$.*

Proof: If $x_i = x_j$ then we must have $l_h \mid (i - j)$. Hence the first statement of the Lemma is clear. The second statement follows since there is some multiple of l_h between l_t and $l_t + l_h$. □

Exercise 14.2.4. Let $p = 347$, $r = 173$, $g = 3, h = 11 \in \mathbb{F}_p^*$. Let $n_S = 3$. Determine l_t and l_h for the values $(u_1, v_1) = (1, 1)$, $(u_2, v_2) = (13, 17)$. What is the smallest of i for which $x_{2i} = x_i$?

Exercise 14.2.5. Repeat Exercise 14.2.4 for $g = 11$, $h = 3$ $(u_1, v_1) = (4, 7)$ and $(u_2, v_2) = (23, 5)$.

[3] Apparently this algorithm first appears in print in Knuth [343], but is credited there to Floyd.

Algorithm 16 The rho algorithm

INPUT: $g, h \in G$
OUTPUT: a such that $h = g^a$, or $\perp$

```
Choose randomly the function walk as explained above
x_1 = g, a_1 = 1, b_1 = 0
(x_2, a_2, b_2) = walk(x_1, a_1, b_1)
while (x_1 ≠ x_2) do
    (x_1, a_1, b_1) = walk(x_1, a_1, b_1)
    (x_2, a_2, b_2) = walk(walk(x_2, a_2, b_2))
end while
if b_1 ≡ b_2 (mod r) then
    return ⊥
else
    return (a_2 − a_1)(b_1 − b_2)^{-1} (mod r)
end if
```

The smallest index i such that $x_{2i} = x_i$ is called the **epact**. The expected value of the epact is conjectured to be approximately $0.823\sqrt{\pi r/2}$; see Heuristic 14.2.9.

Example 14.2.6. Let $p = 809$ and consider $g = 89$ which has prime order 101 in $\mathbb{F}_p^*$. Let $h = 799$ which lies in the subgroup generated by g.

Let $n_S = 4$. To define $S(g)$ write g in the range $1 \leq g < 809$, represent this integer in its usual binary expansion and then reduce modulo 4. Choose $(u_1, v_1) = (37, 34), (u_2, v_2) = (71, 69), (u_3, v_3) = (76, 18)$ so that $g_1 = 343, g_2 = 676, g_3 = 627$. One computes the table of values (x_i, a_i, b_i) as follows:

i	x_i	a_i	b_i	$S(x_i)$
1	89	1	0	1
2	594	38	34	2
3	280	8	2	0
4	736	16	4	0
5	475	32	8	3
6	113	7	26	1
7	736	44	60	0

It follows that $l_t = 4$ and $l_h = 3$ and so the first collision detected by Floyd's method is $x_6 = x_{12}$. We leave as an exercise to verify that the discrete logarithm in this case is 50.

Exercise 14.2.7. Let $p = 569$ and let $g = 262$ and $h = 5$ which can be checked to have order 71 modulo p. Use the rho algorithm to compute the discrete logarithm of h to the base g modulo p.

Exercise 14.2.8. One can simplify Definition 14.2.1 and equation (14.4) by replacing g_j by either g^{u_j} or h^{v_j} (independently for each j). Show that this saves one modular addition in each iteration of the algorithm. Explain why this optimisation should not affect the success of the algorithm, as long as the walk uses all values for $S(x_i)$ with roughly equal probability.

Algorithm 16 always terminates, but there are several things that can go wrong:

- The value $(b_1 - b_2)$ may not be invertible modulo r.

Hence, we can only expect to prove that the algorithm succeeds with a certain probability (extremely close to 1).

- The cycle may be very long (as big as r) in which case the algorithm is slower than brute force search.

  Hence, we can only expect to prove an expected running time for the algorithm. We recall that the expected running time in this case is the average, over all choices for the function walk, of the worst-case running time of the algorithm over all problem instances.

Note that the algorithm always halts, but it may fail to output a solution to the DLP. Hence, this is a Monte Carlo algorithm.

It is an open problem to give a rigorous running time analysis for the rho algorithm. Instead it is traditional to make the heuristic assumption that the pseudorandom walk defined above behaves sufficiently close to a random walk. The rest of this section is devoted to showing that the heuristic running time of the rho algorithm with Floyd cycle finding is $(3.093 + o(1))\sqrt{r}$ group operations (asymptotic as $r \to \infty$).

Before stating a precise heuristic we determine an approximation to the expected value of the epact in the case of a truly random walk.[4]

Heuristic 14.2.9. Let x_i be a sequence of elements of a group G of order r obtained as above by iterating a random function $f : G \to G$. Then the expected value of the epact (i.e., the smallest positive integer i such that $x_{2i} = x_i$) is approximately $(\zeta(2)/2)\sqrt{\pi r/2} \approx 0.823\sqrt{\pi r/2}$, where $\zeta(2) = \pi^2/6$ is the value of the Riemann zeta function at 2.

Argument: Fix a specific sequence x_i and let l be the length of the rho, so that x_{l+1} lies in $\{x_1, x_2, \ldots, x_l\}$. Since x_{l+1} can be any one of the x_i, the cycle length l_h can be any value $1 \leq l_h \leq l$ and each possibility happens with probability $1/l$.

The epact is the smallest multiple of l_h which is bigger than $l_t = l - l_h$. Hence, if $l/2 \leq l_h \leq l$ then the epact is l_h, if $l/3 \leq l_h < l/2$ then the epact is $2l_h$. In general, if $l/(k+1) \leq l_h < l/k$ then the epact is kl_h. The largest possible value of the epact is $l - 1$, which occurs when $l_h = 1$.

The expected value of the epact when the rho has length l is therefore

$$E_l = \sum_{k=1}^{\infty} \sum_{l_h=1}^{l} k l_h P_l(k, l_h)$$

where $P_l(k, l_h)$ is the probability that kl_h is the epact. By the above discussion, $P(k, l_h) = 1/l$ if $l/(k+1) \leq l_h < l/k$ or $(k, l_h) = (1, l)$ and zero otherwise. Hence

$$E_l = \frac{1}{l} \sum_{k=1}^{l-1} k \sum_{\substack{l/(k+1) \leq l_h < l/k \\ \text{or } (k,l_h)=(1,l)}} l_h$$

Approximating the inner sum as $\frac{1}{2}\left((l/k)^2 - (l/(k+1))^2\right)$ gives

$$E_l \approx \frac{l}{2} \sum_{k=1}^{\infty} k \left(\frac{1}{k^2} - \frac{1}{(k+1)^2} \right).$$

[4] I thank John Pollard for showing me this argument.

Now, $k(1/k^2 - 1/(k+1)^2) = 1/k - 1/(k+1) + 1/(k+1)^2$ and

$$\sum_{k=1}^{\infty}(1/k - 1/(k+1)) = 1 \qquad \text{and} \qquad \sum_{k=1}^{\infty} 1/(k+1)^2 = \zeta(2) - 1.$$

Hence $E_l \approx l/2(1 + \zeta(2) - 1)$. It is well-known that $\zeta(2) \approx 1.645$. Finally, write $\Pr(e)$ for the probability the epact is e, $\Pr(l)$ for the probability the rho length is l, and $\Pr(e \mid l)$ for the conditional probability that the epact is e given that the rho has length l. The expectation of e is then

$$\begin{aligned} E(e) &= \sum_{e=1}^{\infty} e \Pr(e) = \sum_{e=1}^{\infty} e \sum_{l=1}^{\infty} \Pr(e \mid l) \Pr(l) \\ &= \sum_{l=1}^{\infty} \Pr(l) \left(\sum_{e=1}^{\infty} e \Pr(e \mid l) \right) \\ &= \sum_{l=1}^{\infty} \Pr(l) E_l \approx (\zeta(2)/2) E(l) \end{aligned}$$

which completes the argument. □

We can now give a heuristic analysis of the running time of the algorithm. We make the following assumption, which we believe is reasonable when r is sufficiently large, $n_S > \log(r)$ and when the function walk is chosen at random (from the set of all walk functions specified in Section 14.2.1).

Heuristic 14.2.10.

1. The expected value of the epact is $(0.823 + o(1))\sqrt{\pi r/2}$.
2. The value $\sum_{i=l_t}^{l_t+l_h-1} v_{S(x_i)} \pmod r$ is uniformly distributed in $\mathbb{Z}/r\mathbb{Z}$.

Theorem. *Let the notation be as above and assume Heuristic 14.2.10. Then the rho algorithm with Floyd cycle finding has expected running time of* $(3.093 + o(1))\sqrt{r}$ *group operations. The probability the algorithm fails is negligible.*

Proof: The number of iterations of the main loop in Algorithm 16 is the epact. By Heuristic 14.2.10 the expected value of the epact is $(0.823 + o(1))\sqrt{\pi r/2}$.

Algorithm 16 performs three calls to the function walk in each iteration. Each call to walk results in one group operation and two additions modulo r (we ignore these additions as they cost significantly less than a group operation). Hence the expected number of group operations is $3(0.823 + o(1))\sqrt{\pi r/2} \approx (3.093 + o(1))\sqrt{r}$ as claimed.

The algorithm fails only if $b_{2i} \equiv b_i \pmod r$. We have $g^{a_{l_t}} h^{b_{l_t}} = g^{a_{l_t+l_h}} h^{b_{l_t+l_h}}$ from which it follows that $a_{l_t+l_h} = a_{l_t} + u$, $b_{l_t+l_h} = b_{l_t} + v$ where $g^u h^v = 1$. Precisely, $v \equiv b_{l_t+l_h} - b_{l_t} \equiv \sum_{i=l_t}^{l_t+l_h-1} v_{S(x_i)} \pmod r$.

Write $i = l_t + i'$ for some $0 \leq i' < l_h$ and $b_i = b_{l_t} + w$. Assume $l_h \geq 2$ (the probability that $l_h = 1$ is negligible). Then $2i = l_t + xl_h + i'$ for some integer $1 \leq x < (l_t + 2l_h)/l_h < r$ and so $b_{2i} = b_{l_t} + xv + w$. It follows that $b_{2i} \equiv b_i \pmod r$ if and only if $r \mid v$.

According to Heuristic 14.2.10 the value v is uniformly distributed in $\mathbb{Z}/r\mathbb{Z}$ and so the probability it is zero is $1/r$, which is a negligible quantity in the input size of the problem. □

14.2.3 Other Cycle Finding Methods

Floyd cycle finding is not a very efficient way to find cycles. Though any cycle finding method requires computing at least $l_t + l_h$ group operations, Floyd's method needs on average $2.47(l_t + l_h)$ group operations (2.47 is three times the expected value of the epact). Also, the "slower" sequence x_i is visiting group elements which have already been computed during the walk of the "faster" sequence x_{2i}. Brent [98] has given an improved cycle finding method[5] that still only requires storage for two group elements but which requires fewer group operations. Montgomery has given an improvement to Brent's method in [436].

One can do even better by using more storage, as was shown by Sedgewick, Szymanski and Yao [535], Schnorr and Lenstra [527] (also see Teske [603]) and Nivasch [467]. The rho algorithm using Nivasch cycle finding has the optimal expected running time of $\sqrt{\pi r/2} \approx 1.253\sqrt{r}$ group operations and is expected to require polynomial storage.

Finally, a very efficient way to find cycles is to use distinguished points. More importantly, distinguished points allow us to think about the rho method in a different way and this leads to a version of the algorithm that can be parallelised. We discuss this in the next section. Hence, in practice one always uses distinguished points.

14.2.4 Distinguished Points and Pollard Rho

The idea of using distinguished points in search problems apparently goes back to Rivest. The first application of this idea to computing discrete logarithms is by van Oorschot and Wiener [473].

Definition 14.2.11. An element $g \in G$ is a **distinguished point** if its binary representation $b(g)$ satisfies some easily checked property. Denote by $\mathcal{D} \subset G$ the set of distinguished points. The probability $\#\mathcal{D}/\#G$ that a uniformly chosen group element is a distinguished point is denoted θ.

A typical example is the following.

Example 14.2.12. Let E be an elliptic curve over $\mathbb{F}_p$. A point $P \in E(\mathbb{F}_p)$ that is not the point at infinity is represented by an x-coordinate $0 \leq x_P < p$ and a y-coordinate $0 \leq y_P < p$. Let H be a hash function, whose output is interpreted as being in $\mathbb{Z}_{\geq 0}$.

Fix an integer n_D. Define $\mathcal{D}$ to be the points $P \in E(\mathbb{F}_p)$ such that the n_D least significant bits of $H(x_P)$ are zero. Note that $\mathcal{O}_E \notin \mathcal{D}$. In other words

$$\mathcal{D} = \{P = (x_P, y_P) \in E(\mathbb{F}_p) : H(x_P) \equiv 0 \pmod{2^{n_D}} \text{ where } 0 \leq x_P < p\}.$$

Then $\theta \approx 1/2^{n_D}$.

The rho algorithm with distinguished points is as follows. First, choose integers $0 \leq a_1, b_1 < r$ uniformly and independently at random, compute the group element $x_1 = g^{a_1}h^{b_1}$ and run the usual deterministic pseudorandom walk until a distinguished point $x_n = g^{a_n}h^{b_n}$ is found. Store (x_n, a_n, b_n) in some easily searched data structure (searchable on x_n). Then choose a fresh randomly chosen group element $x_1 = g^{a_1}h^{b_1}$ and repeat. Eventually two walks will visit the same group element, in which case their paths will continue to the same distinguished point. Once a distinguished group element is found twice then the DLP can be solved with high probability.

Exercise 14.2.13. Write down pseudocode for this algorithm.

[5] This was originally developed to speed up the Pollard rho factoring algorithm.

We stress the most significant difference between this method and the method of the previous section: the previous method had one long walk with a tail and a cycle, whereas the new method has many short walks. Note that this algorithm does not require self-collisions in the walk and so there is no ρ shape anymore; the word "rho" in the name of the algorithm is therefore a historical artifact, not an intuition about how the algorithm works.

Note that, since the group is finite, collisions must eventually occur, and so the algorithm halts. But the algorithm may fail to solve the DLP (with low probability). Hence, this is a Monte Carlo algorithm.

In the analysis we assume that we are sampling group elements (we sometimes call them "points") uniformly and independently at random. It is important to determine the expected number of steps before landing on a distinguished point.

Lemma 14.2.14. *Let θ be the probability that a randomly chosen group element is a distinguished point. Then*

1. *The probability that one chooses α/θ group elements, none of which are distinguished, is approximately $e^{-\alpha}$ when $1/\theta$ is large.*

2. *The expected number of group elements to choose before getting a distinguished point is $1/\theta$.*

3. *If one has already chosen i group elements, none of which are distinguished, then the expected number of group elements to further choose before getting a distinguished point is $1/\theta$.*

Proof: The probability that i chosen group elements are not distinguished is $(1-\theta)^i$. So the probability of choosing α/θ points, none of which are distinguished, is

$$(1-\theta)^{\alpha/\theta} \leq \left(e^{-\theta}\right)^{\alpha/\theta} = e^{-\alpha}.$$

The second statement is the standard formula for the expected value of a geometric random variable, see Example A.14.1.

For the final statement[6], suppose one has already sampled i points without finding a distinguished point. Since the trials are independent, the probability of choosing a further j points which are not distinguished remains $(1-\theta)^j$. Hence the expected number of extra points to be chosen is still $1/\theta$. □

We now make the following assumption. We believe this is reasonable when r is sufficiently large, $n_S > \log(r)$, distinguished points are sufficiently common and specified using a good hash function (and hence, $\mathcal{D}$ is well distributed), $\theta > \log(r)/\sqrt{r}$ and when the function walk is chosen at random.

Heuristic 14.2.15.

1. Walks reach a distinguished point in significantly fewer than $\sqrt{r}$ steps (in other words, there are no cycles in the walks and walks are not excessively longer than $1/\theta$).[7]
2. The expected number of group elements sampled before a collision is $\sqrt{\pi r/2}$.

[6] This is the "apparent paradox" mentioned in footnote 7 of [473].

[7] More realistically, one could assume that only a negligibly small proportion of the walks fall into a cycle before hitting a distinguished point.

Theorem 14.2.16. *Let the notation be as above and assume Heuristic 14.2.15. Then the rho algorithm with distinguished points has expected running time of* $(\sqrt{\pi/2}+o(1))\sqrt{r} \approx (1.253+o(1))\sqrt{r}$ *group operations. The probability the algorithm fails is negligible.*

Proof: Heuristic 14.2.15 states there are no cycles or "wasted" walks (in the sense that their steps do not contribute to potential collisions). Hence, before the first collision, after N steps of the algorithm we have visited N group elements. By Heuristic 14.2.15, the expected number of group elements to be sampled before the first collision is $\sqrt{\pi r/2}$. The collision is not detected until walks hit a distinguished point, which adds a further $2/\theta$ to the number of steps. Hence, the total number of steps (calls to the function walk) in the algorithm is $\sqrt{\pi r/2}+2/\theta$. Since $2/\theta < 2\sqrt{r}/\log(r) = o(1)\sqrt{r}$, the result follows.

Let $x = g^{a_i}h^{b_i} = g^{a_j}h^{b_j}$ be the collision. Since the starting values $g^{a_0}h^{b_0}$ are chosen uniformly and independently at random, the values b_i and b_j are uniformly and independently random. It follows that $b_i \equiv b_j \pmod{r}$ with probability $1/r$, which is a negligible quantity in the input size of the problem. □

Exercise 14.2.17. Show that if $\theta = \log(r)/\sqrt{r}$ then the expected storage of the rho algorithm, assuming it takes $O(\sqrt{r})$ steps, is $O(\log(r))$ group elements (which is typically $O(\log(r)^2)$ bits).

Exercise 14.2.18. The algorithm requires storing a triple (x_n, a_n, b_n) for each distinguished point. Give some strategies to reduce the number of bits that need to be stored.

Exercise 14.2.19. Let $G = \langle g_1, g_2 \rangle$ be a group of order r^2 and exponent r. Design a rho algorithm that, on input $h \in G$ outputs (a_1, a_2) such that $h = g_1^{a_1}g_2^{a_2}$. Determine the complexity of this algorithm.

Exercise 14.2.20. Show that the Pollard rho algorithm with distinguished points has better average-case running time than the baby-step-giant-step algorithm (see Exercises 13.3.3 and 13.3.4).

Exercise 14.2.21. Explain why taking $\mathcal{D} = G$ (i.e., all group elements distinguished) leads to an algorithm that is much slower than the baby-step-giant-step algorithm.

Suppose one is given $g, h_1, \ldots, h_L$ (where $1 < L < r^{1/4}$) and is asked to find all a_i for $1 \leq i \leq L$ such that $h_i = g^{a_i}$. Kuhn and Struik [355] propose and analyse a method to solve all L instances of the DLP, using Pollard rho with distinguished points, in roughly $\sqrt{2rL}$ group operations. A crucial trick, attributed to Silverman and Stapleton, is that once the i-th DLP is known one can re-write all distinguished points $g^a h_i^b$ in the form $g^{a'}$. As noted by Hitchcock, Montague, Carter and Dawson [287] one must be careful to choose a random walk function that does not depend on the elements h_i (however, the random starting points do depend on the h_i).

Exercise 14.2.22. Write down pseudocode for the Kuhn-Struik algorithm for solving L instances of the DLP, and explain why the algorithm works.

Section 14.2.5 explains why the rho algorithm with distinguished points can be easily parallelised. That section also discusses a number of practical issues relating to the use of distinguished points.

Cheon, Hong and Kim [133] sped up Pollard rho in $\mathbb{F}_p^*$ by using a "look ahead" strategy; essentially they determine in which partition the next value of the walk lies, without performing a full group operation. A similar idea for elliptic curves has been used by Bos, Kaihara and Kleinjung [89].

14.2.5 Towards a Rigorous Analysis of Pollard Rho

Theorem 14.2.16 is not satisfying since Heuristic 14.2.15 is essentially equivalent to the statement "the rho algorithm has expected running time $(1 + o(1))\sqrt{\pi r/2}$ group operations". The reason for stating the heuristic is to clarify exactly what properties of the pseudorandom walk are required. The reason for believing Heuristic 14.2.15 is that experiments with the rho algorithm (see Section 14.4.3) confirm the estimate for the running time.

Since the algorithm is fundamental to an understanding of elliptic curve cryptography (and torus/trace methods) it is natural to demand a complete and rigorous treatment of it. Such an analysis is not yet known, but in this section we mention some partial results on the problem. The methods used to obtain the results are beyond the scope of this book, so we do not give full details. Note that all existing results are in an idealised model where the selection function S is a random function.

We stress that, in practice, the algorithm behaves as the heuristics predict. Furthermore, from a cryptographic point of view, it is sufficient for the task of determining key sizes to have a lower bound on the running time of the algorithm. Hence, in practice, the absence of proved running time is not necessarily a serious issue.

The main results for the original rho walk (with $n_S = 3$) are due to Horwitz and Venkatesan [294], Miller and Venkatesan [426], and Kim, Montenegro, Peres and Tetali [337, 336]. The basic idea is to define the **rho graph**, which is a directed graph with vertex set $\langle g \rangle$ and an edge from x_1 to x_2 if x_2 is the next step of the walk when at x_1. Fix an integer n. Define the distribution $\mathcal{D}_n$ on $\langle g \rangle$ obtained by choosing uniformly at random $x_1 \in \langle g \rangle$, running the walk for n steps, and recording the final point in the walk. The crucial property to study is the **mixing time** which, informally, is the smallest integer n such that $\mathcal{D}_n$ is "sufficiently close" to the uniform distribution. For these results, the squaring operation in the original walk is crucial. We state the main result of Miller and Venkatesan [426] below.

Theorem 14.2.23. *(Theorem 1.1 of [426]) Fix $\epsilon > 0$. Then the rho algorithm using the original rho walk with $n_S = 3$ finds a collision in $O_\epsilon(\sqrt{r}\log(r)^3)$ group operations with probability at least $1 - \epsilon$, where the probability is taken over all partitions of $\langle g \rangle$ into three sets S_1, S_2 and S_3. The notation O_ϵ means that the implicit constant in the O depends on ϵ.*

Kim, Montenegro, Peres and Tetali improved this result in [336] to the desired $O_\epsilon(\sqrt{r})$ group operations. Note that all these works leave the implied constant in the O unspecified.

Note that the idealised model of S being a random function is not implementable with constant (or even polynomial) storage. Hence, these results cannot be applied to the algorithm presented above, since our selection functions S are very far from uniformly chosen over all possible partitions of the set $\langle g \rangle$. The number of possible partitions of $\langle g \rangle$ into three subsets of equal size is (for convenience suppose that $3 \mid r$)

$$\binom{r}{r/3}\binom{2r/3}{r/3}$$

which, using $\binom{a}{b} \geq (a/b)^b$, is at least $6^{r/3}$. On the other hand, a selection function parameterised by a "key" of $c\log_2(r)$ bits (e.g., a selection function obtained from a keyed hash function) only leads to r^c different partitions.

Sattler and Schnorr [513] and Teske [604] have considered the additive rho walk. One key feature of their work is to discuss the effect of the number of partitions n_S. Sattler

and Schnorr show (subject to a conjecture) that if $n_S \geq 8$ then the expected running time for the rho algorithm is $c\sqrt{\pi r/2}$ group operations for an explicit constant c. Teske shows, using results of Hildebrand, that the additive walk should approximate the uniform distribution after fewer than $\sqrt{r}$ steps once $n_S \geq 6$. She recommends using the additive walk with $n_S \geq 20$ and, when this is done, conjectures that the expected cycle length is $\leq 1.3\sqrt{r}$ (compared with the theoretical $\approx 1.2533\sqrt{r}$).

Further motivation for using large n_S is given by Brent and Pollard [99], Arney and Bender [13] and Blackburn and Murphy [59]. They present heuristic arguments that the expected cycle length when using n_S partitions is $\sqrt{c_{n_S}\pi r/2}$ where $c_{n_S} = n_S/(n_S - 1)$. This heuristic is supported by the experimental results of Teske [604]. Let $G = \langle g \rangle$. Their analysis considers the directed graph formed from iterating the function $\mathsf{walk} : G \to G$ (i.e., the graph with vertex set G and an edge from g to $\mathsf{walk}(g)$). Then, for a randomly chosen graph of this type, $n_S/(n_S - 1)$ is the variance of the in-degree for this graph, which is the same as the expected value of $n(x) = \#\{y \in G : y \neq x,\ \mathsf{walk}(y) = \mathsf{walk}(x)\}$.

Finally, when using equivalence classes (see Section 14.4) there are further advantages in taking n_S to be large.

14.3 Distributed Pollard Rho

In this section we explain how the Pollard rho algorithm can be parallelised. Rather than a parallel computing model we consider a **distributed computing** model. In this model there is a **server** and $N_P \geq 1$ **clients** (we also refer to the clients as **processors**). There is no shared storage or direct communication between the clients. Instead, the server can send messages to clients and each client can send messages to the server. In general we prefer to minimise the amount of communication between server and clients.[8]

To solve an instance of the discrete logarithm problem the server will activate a number of clients, providing each with its own individual initial data. The clients will run the rho pseudorandom walk and occasionally send data back to the server. Eventually the server will have collected enough information to solve the problem, in which case it sends all clients a termination instruction. The rho algorithm with distinguished points can very naturally be used in this setting.

The best one can expect for any distributed computation is a linear speedup compared with the serial case (since if the overall total work in the distributed case was less than the serial case then this would lead to a faster algorithm in the serial case). In other words, with N_P clients we hope to achieve a running time proportional to $\sqrt{r}/N_P$.

14.3.1 The Algorithm and its Heuristic Analysis

All processors perform the same pseudorandom walk $(x_{i+1}, a_{i+1}, b_{i+1}) = \mathsf{walk}(x_i, a_i, b_i)$ as in Section 14.2.1, but each processor starts from a different random starting point. Whenever a processor hits a distinguished point then it sends the triple (x_i, a_i, b_i) to the server and re-starts its walk at a new random point (x_0, a_0, b_0). If one processor ever visits a point visited by another processor then the walks from that point agree and both walks end at the same distinguished point. When the server receives two triples (x, a, b) and (x, a', b') for the same group element x but with $b \not\equiv b' \pmod{r}$ then it has $g^a h^b = g^{a'} h^{b'}$ and can solve the DLP as in the serial (i.e., non-parallel) case. The server therefore computes the discrete logarithm problem and sends a terminate signal to all processors.

[8] There are numerous examples of such distributed computation over the internet. Two notable examples are the Great Internet Mersenne Primes Search (GIMPS) and the Search for Extraterrestrial Intelligence (SETI). One observes that the former search has been more successful than the latter.

Pseudocode for both server and clients are given by Algorithms 17 and 18. By design, if the algorithm halts then the answer is correct.

Algorithm 17 The distributed rho algorithm: Server side

INPUT: $g, h \in G$
OUTPUT: c such that $h = g^c$

```
1: Randomly choose a walk function walk(x, a, b)
2: Initialise an easily searched structure L (sorted list, binary tree etc) to be empty
3: Start all processors with the function walk
4: while DLP not solved do
5:     Receive triples (x, a, b) from clients and insert into L
6:     if first coordinate of new triple (x, a, b) matches existing triple (x, a', b') then
7:         if b' ≢ b (mod r) then
8:             Send terminate signal to all clients
9:             return (a − a')(b' − b)^{-1} (mod r)
10:        end if
11:    end if
12: end while
```

Algorithm 18 The distributed rho algorithm: Client side

INPUT: $g, h \in G$, function walk

```
1: while terminate signal not received do
2:     Choose uniformly at random 0 ≤ a, b < r
3:     Set x = g^a h^b
4:     while x ∉ D do
5:         (x, a, b) = walk(x, a, b)
6:     end while
7:     Send (x, a, b) to server
8: end while
```

We now analyse the performance of this algorithm. To get a clean result we assume that no client ever crashes, that communications between server and client are perfectly reliable, that all clients have the same computational efficiency and are running continuously (in other words, each processor computes the same number of group operations in any given time period).

It is appropriate to ignore the computation performed by the server and instead to focus on the number of group operations performed by each client running Algorithm 18. Each execution of the function walk(x, a, b) involves a single group operation. We must also count the number of group operations performed in line 3 of Algorithm 18; though this term is negligible if walks are long on average (i.e., if $\mathcal{D}$ is a sufficiently small subset of G).

It is an open problem to give a rigorous analysis of the distributed rho method. Hence, we make the following heuristic assumption. We believe this assumption is reasonable when r is sufficiently large, n_S is sufficiently large, $\log(r)/\sqrt{r} < \theta$, the set $\mathcal{D}$ of distinguished points is determined by a good hash function, the number N_P of clients is sufficiently small (e.g., $N_P < \theta\sqrt{\pi r/2}/\log(r)$, see Exercise 14.3.3), the function walk is chosen at random.

Heuristic 14.3.1.

1. The expected number of group elements to be sampled before the same element is sampled twice is $\sqrt{\pi r/2}$.
2. Walks reach a distinguished point in significantly fewer than $\sqrt{r}/N_P$ steps (in other words, there are no cycles in the walks and walks are not excessively long). More realistically, one could assume that only a negligible proportion of the walks fall into a cycle before hitting a distinguished point.

Theorem 14.3.2. *Let the notation be as above, in particular, let N_P be the (fixed, independent of r) number of clients. Let θ the probability that a group element is a distinguished point and suppose $\log(r)/\sqrt{r} < \theta$. Assume Heuristic 14.3.1 and the above assumptions about the the reliability and equal power of the processors hold. Then the expected number of group operations performed by each client of the distributed rho method is $(1 + 2\log(r)\theta)\sqrt{\pi r/2}/N_P + 1/\theta$ group operations. This is $(\sqrt{\pi/2}/N_P + o(1))\sqrt{r}$ group operations when $\theta < 1/\log(r)^2$. The storage requirement on the server is $\theta\sqrt{\pi r/2} + N_P$ points.*

Proof: Heuristic 14.3.1 states that we expect to sample $\sqrt{\pi r/2}$ group elements in total before a collision arises. Since this work is distributed over N_P clients of equal speed it follows that each client is expected to call the function walk about $\sqrt{\pi r/2}/N_P$ times. The total number of group operations is therefore $\sqrt{\pi r/2}/N_P$ plus $2\log(r)\theta\sqrt{\pi r/2}/N_P$ for the work of line 3 of Algorithm 18. The server will not detect the collision until the second client hits a distinguished point, which is expected to take $1/\theta$ further steps by the heuristic (part 3 of Lemma 14.2.14). Hence each client needs to run an expected $\sqrt{\pi r/2}/N_P + 1/\theta$ steps of the walk.

Of course, a collision $g^a h^b = g^{a'} h^{b'}$ can be useless in the sense that $b' \equiv b \pmod r$. A collision implies $a' + cb' \equiv a + cb \pmod r$ where $h = g^c$; there are r such pairs (a', b') for each pair (a, b). Since each walk starts with uniformly random values (a_0, b_0) it follows that the values (a, b) are uniformly distributed over the r possibilities. Hence the probability of a collision being useless is $1/r$ and the expected number of collisions required is 1.

Each processor runs for $\sqrt{\pi r/2}/N_P + 1/\theta$ steps and therefore is expected to send $\theta\sqrt{\pi r/2}/N_P + 1$ distinguished points in its lifetime. The total number of points to store is therefore $\theta\sqrt{\pi r/2} + N_P$. □

Exercise 14.2.17 shows that the complexity in the case $N_P = 1$ can be taken to be $(1 + o(1))\sqrt{\pi r/2}$ group operations with polynomial storage.

Exercise 14.3.3. When distributing the algorithm it is important to ensure that, with very high probability, each processor finds at least one distinguished point in less than its total expected running time. Show that this will be the case if $1/\theta \leq \sqrt{\pi r/2}/\left(N_P \log(r)\right)$.

Schulte-Geers [533] analyses the choice of θ and shows that Heuristics 14.2.15 and 14.3.1 are not valid asymptotically if $\theta = o(1/\sqrt{r})$ as $r \to \infty$ (for example, walks in this situation are more likely to fall into a cycle than to hit a distinguished point). In any case, since each processor only travels a distance of $\sqrt{\pi r/2}/N_P$ it follows we should take $\theta > N_P/\sqrt{r}$. In practice one tends to determine the available storage first (say, c group elements where $c > 10^9$) and to set $\theta = c/\sqrt{\pi r/2}$ so that the total number of distinguished points visited is expected to be c. The results of [533] validate this approach. In particular, it is extremely unlikely that there is a self-collision (and hence a cycle) before hitting a distinguished point.

14.4 Speeding up the Rho Algorithm using Equivalence Classes

Gallant, Lambert and Vanstone [232] and Wiener and Zuccherato [632] showed that one can speed up the rho method in certain cases by defining the pseudorandom walk not on the group $\langle g \rangle$ but on a set of equivalence classes. This is essentially the same thing as working in an algebraic group quotient instead of the algebraic group.

Suppose there is an equivalence relation on $\langle g \rangle$. Denote by $\overline{x}$ the equivalence class of $x \in \langle g \rangle$. Let N_C be the size of a generic equivalence class. We require the following properties:

1. One can define a unique representative $\hat{x}$ of each equivalence class $\overline{x}$.
2. Given (x_i, a_i, b_i) such that $x_i = g^{a_i} h^{b_i}$ then one can efficiently compute $(\hat{x}_i, \hat{a}_i, \hat{b}_i)$ such that $\hat{x}_i = g^{\hat{a}_i} h^{\hat{b}_i}$.

We give some examples in Section 14.4.1 below.

One can implement the rho algorithm on equivalence classes by defining a pseudorandom walk function $\mathsf{walk}(x_i, a_i, b_i)$ as in Definition 14.2.1. More precisely, set $x_1 = g, a_1 = 1, b_1 = 0$ and define the sequence x_i by (this is the "original walk")

$$x_{i+1} = f(x_i) = \begin{cases} \hat{x}_i^2 & \text{if } S(\hat{x}_i) = 0 \\ \hat{x}_i g_j & \text{if } S(\hat{x}_i) = j,\ j \in \{1, \ldots, n_S - 1\} \end{cases} \tag{14.6}$$

where the selection function S and the values $g_j = g^{u_j} h^{v_j}$ are as in Definition 14.2.1. When using distinguished points one defines an equivalence class to be distinguished if the unique equivalence class representative has the distinguished property.

There is a very serious problem with cycles that we do not discuss yet; See Section 14.4.2 for the details.

Exercise 14.4.1. Write down the formulae for updating the values a_i and b_i in the function walk.

Exercise 14.4.2. Write pseudocode for the distributed rho method on equivalence classes.

Theorem 14.4.3. *Let G be a group and $g \in G$ of order r. Suppose there is an equivalence relation on $\langle g \rangle$ as above. Let N_C be the generic size of an equivalence class. Let C_1 be the number of bit operations to perform a group operation in $\langle g \rangle$ and C_2 the number of bit operations to compute a unique equivalence class representative $\hat{x}_i$ (and to compute $\hat{a}_i, \hat{b}_i$).*

Consider the rho algorithm as above (ignoring the possibility of useless cycles, see Section 14.4.2 below). Under a heuristic assumption for equivalence classes analogous to Heuristic 14.2.15 the expected time to solve the discrete logarithm problem is

$$\left(\sqrt{\frac{\pi}{2N_C}} + o(1) \right) \sqrt{r}\ (C_1 + C_2)$$

bit operations. As usual, this becomes $(\sqrt{\pi/2N_C} + o(1))\sqrt{r}/N_P(C_1 + C_2)$ bit operations per client when using N_P processors of equal computational power.

Exercise 14.4.4. Prove this theorem.

Theorem 14.4.3 assumes a perfect random walk. For walks defined on n_S partitions of the set of equivalence classes it is shown in Appendix B of [25] (also see Section 2.2 of [91]) that one predicts a slightly improved constant than the usual factor $c_{n_S} = n_S/(n_S - 1)$ mentioned at the end of Section 14.2.5.

We mention a potential "paradox" with this idea. In general, computing a unique equivalence class representative involves listing all elements of the equivalence class, and hence needs $\tilde{O}(N_C)$ bit operations. Hence, naively, the running time is $\tilde{O}(\sqrt{N_C \pi r/2})$ bit operations, which is worse than doing the rho algorithm without equivalence classes. However, in practice one only uses this method when $C_2 < C_1$, in which case the speedup can be significant.

14.4.1 Examples of Equivalence Classes

We now give some examples of useful equivalence relations on some algebraic groups.

Example 14.4.5. For a group G with efficiently computable inverse (e.g., elliptic curves $E(\mathbb{F}_q)$ or algebraic tori $\mathbb{T}_n$ with $n > 1$ (e.g., see Section 6.3)) one can define the equivalence relation $x \equiv x^{-1}$. We have $N_C = 2$ (though note that some elements, namely the identity and elements of order 2, are equal to their inverse so these classes have size 1). If $x_i = g^{a_i} h^{b_i}$ then clearly $x^{-1} = g^{-a_i} h^{-b_i}$. One defines a unique representative $\hat{x}$ for the equivalence class by, for example, imposing a lexicographical ordering on the binary representation of the elements in the class.

We can generalise this example as follows.

Example 14.4.6. Let G be an algebraic group over $\mathbb{F}_q$ with an automorphism group $\mathrm{Aut}(G)$ of size N_C (see examples in Sections 9.4 and 11.3.3). Suppose that for $g \in G$ of order r one has $\psi(g) \in \langle g \rangle$ for each $\psi \in \mathrm{Aut}(G)$. Furthermore, assume that for each $\psi \in \mathrm{Aut}(G)$ one can efficiently compute the eigenvalue $\lambda_\psi \in \mathbb{Z}$ such that $\psi(g) = g^{\lambda_\psi}$. Then for $x \in G$ one can define $\overline{x} = \{\psi(x) : \psi \in \mathrm{Aut}(G)\}$.

Again, one defines $\hat{x}$ by listing the elements of $\overline{x}$ as bitstrings and choosing the first one under lexicographical ordering.

Another important class of examples comes from orbits under the Frobenius map.

Example 14.4.7. Let G be an algebraic group defined over $\mathbb{F}_q$ but with group considered over $\mathbb{F}_{q^d}$ (for examples see Sections 11.3.2 and 11.3.3). Let π_q be the q-power Frobenius map on $G(\mathbb{F}_{q^d})$. Let $g \in G(\mathbb{F}_{q^d})$ and suppose that $\pi_q(g) = g^\lambda \in \langle g \rangle$ for some known $\lambda \in \mathbb{Z}$.

Define the equivalence relation on $G(\mathbb{F}_{q^d})$ so that the equivalence class of $x \in G(\mathbb{F}_{q^d})$ is the set $\overline{x} = \{\pi_q^i(x) : 0 \leq i < d\}$. We assume that, for elements x of interest, $\overline{x} \subseteq \langle g \rangle$. Then $N_C = d$, though there can be elements defined over proper subfields for which the equivalence class is smaller.

If one uses a normal basis for $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$ then one can efficiently compute the elements $\pi_q^i(x)$ and select a unique representative of each equivalence class using a lexicographical ordering of binary strings.

Example 14.4.8. For some groups (e.g., Koblitz elliptic curves $E/\mathbb{F}_2$ considered as a group over $\mathbb{F}_{2^m}$; see Exercise 9.10.11) we can combine both equivalence classes above. Let m be prime, $\#E(\mathbb{F}_{2^m}) = hr$ for some small cofactor h, and $P \in E(\mathbb{F}_{2^m})$ of order r. Then $\pi_2(P) \in \langle P \rangle$ and we define the equivalence class $\overline{P} = \{\pm \pi_2^i(P) : 0 \leq i < m\}$ of size $2m$. Since m is odd, this class can be considered as the orbit of P under the map $-\pi_2$. The distributed rho algorithm on equivalence classes for such curves is expected to require approximately $\sqrt{\pi 2^m/(4m)}$ group operations.

14.4.2 Dealing with Cycles

One problem that can arise is walks that fall into a cycle before they reach a distinguished point. We call these **useless cycles**.

Exercise 14.4.9. Suppose the equivalence relation is such that $x \equiv x^{-1}$. Fix $x_i = \hat{x}_i$ and let $x_{i+1} = \hat{x}_i g$. Suppose $\hat{x}_{i+1} = x_{i+1}^{-1}$ and that $S(\hat{x}_{i+1}) = S(\hat{x}_i)$. Show that $x_{i+2} \equiv x_i$ and so there is a cycle of order 2. Suppose the equivalence classes generically have size N_C. Show, under the assumptions that the function S is perfectly random and that $\hat{x}$ is a randomly chosen element of the equivalence class, that the probability that a randomly chosen x_i leads to a cycle of order 2 is $1/(N_C n_S)$.

A theoretical discussion of cycles was given in [232] and by Duursma, Gaudry and Morain [186]. An obvious way to reduce the probability of cycles is to take n_S to be very large compared with the average length $1/\theta$ of walks. However, as argued by Bos, Kleinjung and Lenstra [91], large values for n_S can lead to slower algorithms (for example, due to the fact that the precomputed steps do not all fit in cache memory). Hence, as Exercise 14.4.9 shows, useless cycles will be regularly encountered in the algorithm. There are several possible ways to deal with this issue. One approach is to use a "look-ahead" technique to avoid falling in 2-cycles. Another approach is to detect small cycles (e.g., by storing a fixed number of previous values of the walk or, at regular intervals, using a cycle-finding algorithm for a small number of steps) and to design a well-defined exit strategy for short cycles; Gallant, Lambert and Vanstone call this **collapsing the cycle**; see Section 6 of [232]. To collapse a cycle one must be able to determine a well-defined element in it; from there one can take a step (different to the steps used in the cycle from that point) or use squaring to exit the cycle. All these methods require small amounts of extra computation and storage, though Bernstein, Lange and Schwabe [56] argue that the additional overhead can be made negligible. We refer to [56, 91] for further discussion of these issues.

Gallant, Lambert and Vanstone [232] presented a different walk that does not, in general, lead to short cycles. Let G be an algebraic group with an efficiently computable endomorphism ψ of order m (i.e., $\psi^m = \psi \circ \cdots \circ \psi$ is the identity map). Let $g \in G$ of order r be such that $\psi(g) = g^\lambda$ so that $\psi(x) = x^\lambda$ for all $x \in \langle g \rangle$. Define the equivalence classes $\overline{x} = \{\psi^j(x) : 0 \leq j < m\}$. We define a pseudorandom sequence $x_i = g^{a_i} h^{b_i}$ by using $\hat{x}$ to select an endomorphism $(1 + \psi^j)$ and then acting on x_i with this map. More precisely, j is some function of $\hat{x}$ (e.g., the function S in Section 14.2.1) and

$$x_{i+1} = (1 + \psi^j)x_i = x_i \psi^j(x_i) = x_i^{1+\lambda^j}$$

(the above equation looks more plausible when the group operation is written additively: $x_{i+1} = x_i + \psi^j(x_i) = (1 + \lambda^j)x_i$). One can check that the map is well-defined on equivalence classes and that $x_{i+1} = g^{a_{i+1}} h^{b_{i+1}}$ where $a_{i+1} = (1 + \lambda^j)a_i \pmod r$ and $b_{i+1} = (1 + \lambda^j)b_i \pmod r$.

We stress that this approach still requires finding a unique representative of each equivalence class in order to define the steps of the walk in a well-defined way. Hence, one can still use distinguished points by defining a class to be distinguished if its representative is distinguished. One suggestion, originally due to Harley, is to use the Hamming weight of the x-coordinate to derive the selection function.

One drawback of the Gallant, Lambert, Vanstone idea is that there is less flexibility in the design of the pseudorandom walk.

Exercise 14.4.10. Generalise the Gallant-Lambert-Vanstone walk to use $(c + \psi^j)$ for any $c \in \mathbb{Z}$. Why do we prefer to only use $c = 1$?

Exercise 14.4.11. Show that taking $n_S = \log(r)$ means the total overhead from handling cycles is $o(\sqrt{r})$, while the additional storage (group elements for the random walks) is $O(\log(r))$ group elements.

Exercise 14.4.11 together with Exercise 14.2.17 shows that (as long as computing equivalence class representatives is fast) one can solve the discrete logarithm problem using equivalence classes of generic size N_C in $(1 + o(1))\sqrt{\pi r/(2N_C)}$ group operations and $O(\log(r))$ group elements storage.

14.4.3 Practical Experience with the Distributed Rho Algorithm

Real computations are not as simple as the idealised analysis above: one doesn't know in advance how many clients will volunteer for the computation; not all clients have the same performance or reliability; clients may decide to withdraw from the computation at any time; the communications between client and server may be unreliable etc. Hence, in practice one needs to choose the distinguished points to be sufficiently common that even the weakest client in the computation can hit a distinguished point within a reasonable time (perhaps after just one or two days). This may mean that the stronger clients are finding many distinguished points every hour.

The largest discrete logarithm problems solved using the distributed rho method are mainly the Certicom challenge elliptic curve discrete logarithm problems. The current records are for the groups $E(\mathbb{F}_p)$ where $p \approx 2^{108} + 2^{107}$ (by a team coordinated by Chris Monico in 2002) and where $p = (2^{128} - 3)/76439 \approx 2^{111} + 2^{110}$ (by Bos, Kaihara and Montgomery in 2009) and for $E(\mathbb{F}_{2^{109}})$ (again by Monico's team in 2004). None of these computations used the equivalence class $\{P, -P\}$.

We briefly summarise the parameters used for these large computations. For the 2002 result the curve $E(\mathbb{F}_p)$ has prime order so $r \approx 2^{108} + 2^{107}$. The number of processors was over 10,000 and they used $\theta = 2^{-29}$. The number of distinguished points found was 68228567 which is roughly 1.32 times the expected number $\theta\sqrt{\pi r/2}$ of points to be collected. Hence, this computation was unlucky in that it ran about 1.3 times longer than the expected time. The computation ran for about 18 months.

The 2004 result is for a curve over $\mathbb{F}_{2^{109}}$ with group order $2r$ where $r \approx 2^{108}$. The computation used roughly 2000 processors, $\theta = 2^{-30}$ and the number of distinguished points found was 16531676. This is about 0.79 times the expected number $\theta\sqrt{\pi 2^{108}/2}$. This computation took about 17 months.

The computation by Bos, Kaihara and Montgomery [90] was innovative in that the work was done using a cluster of 200 computer game consoles. The random walk used $n_S = 16$ and $\theta = 1/2^{24}$. The total number of group operations performed was 8.5×10^{16} (which is 1.02 times the expected value) and 5×10^9 distinguished points were stored.

Exercise 14.4.12. Verify that the parameters above satisfy the requirements that θ is much larger than $1/\sqrt{r}$ and N_P is much smaller than $\theta\sqrt{r}$.

There is a close fit between the actual running time for these examples and the theoretical estimates. This is evidence that the heuristic analysis of the running time is not too far from the performance in practice.

14.5 The Kangaroo Method

This algorithm is designed for the case where the discrete logarithm is known to lie in a short interval. Suppose $g \in G$ has order r and that $h = g^a$ where a lies in a short interval

$b \leq a < b + w$ of width w. We assume that the values of b and w are known. Of course, one can solve this problem using the rho algorithm, but if w is much smaller than the order of g then this will not necessarily be optimal.

The kangaroo method was originally proposed by Pollard [487]. Van Oorschot and Wiener [473] greatly improved it by using distinguished points. We present the improved version in this section.

For simplicity, compute $h' = hg^{-b}$. Then $h' \equiv g^x \pmod{p}$ where $0 \leq x < w$. Hence, there is no loss of generality by assuming that $b = 0$. Thus, from now on our problem is: Given g, h, w to find a such that $h = g^a$ and $0 \leq a < w$.

As with the rho method, the kangaroo method relies on a deterministic pseudorandom walk. The steps in the walk are pictured as the "jumps" of the kangaroo, and the group elements visited are the kangaroo's "footprints". The idea, as explained by Pollard, is to "catch a wild kangaroo using a tame kangaroo". The "tame kangaroo" is a sequence $x_i = g^{a_i}$ where a_i is known. The "wild kangaroo" is a sequence $y_j = hg^{b_j}$ where b_j is known. Eventually, a footprint of the tame kangaroo will be the same as a footprint of the wild kangaroo (this is called the "collision"). After this point, the tame and wild footprints are the same.[9] The tame kangaroo lays "traps" at regular intervals (i.e., at distinguished points) and, eventually, the wild kangaroo falls in one of the traps.[10] More precisely, at the first distinguished point after the collision, one finds a_i and b_j such that $g^{a_i} = hg^{b_j}$ and the DLP is solved as $h = g^{a_i - b_j}$.

There are two main differences between the kangaroo method and the rho algorithm.

- Jumps are "small". This is natural since we want to stay within (or at least, not too far outside) the interval.
- When a kangaroo lands on a distinguished point one **continues** the pseudorandom walk (rather than restarting the walk at a new randomly chosen position).

14.5.1 The Pseudorandom Walk

The pseudorandom walk for the kangaroo method has some significant differences to the rho walk: steps in the walk correspond to known small increments in the exponent (in other words, kangaroos make small jumps of known distance in the exponent). We therefore do not include the squaring operation $x_{i+1} = x_i^2$ (as the jumps would be too big) or multiplication by h (we would not know the length of the jump in the exponent). We now describe the walk precisely.

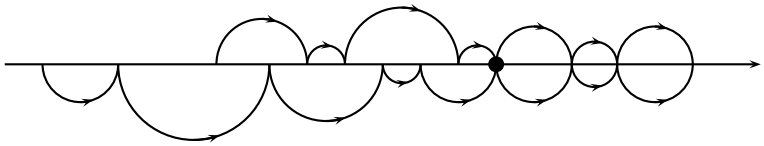
- As in Section 14.2.1 we use a function $S : G \to \{0, \ldots, n_S - 1\}$ which partitions G into sets $\mathcal{S}_i = \{g \in G : S(g) = i\}$ of roughly similar size.
- For $0 \leq j < n_S$ choose exponents $1 \leq u_j \leq \sqrt{w}$ Define $m = (\sum_{j=0}^{n_S-1} u_j)/n_S$ to be the **mean step size**. As explained below we will take $m \approx \sqrt{w}/2$.

  Pollard [487, 488] suggested taking $u_j = 2^j$ as this minimises the chance that two different short sequences of jumps add to the same value. This seems to give good results in practice. An alternative is to choose most of the values u_i to be random and the last few to ensure that m is very close to $c_1\sqrt{w}$.

[9] A collision between two different walks can be drawn in the shape of the letter λ. Hence Pollard also suggested this be called the "lambda method". However, other algorithms (such as the distributed rho method) have collisions between different walks, so this naming is ambiguous. The name "kangaroo method" emphasises the fact that the jumps are small. Hence, as encouraged by Pollard, we do not use the name "lambda method" in this book.

[10] Actually, the wild kangaroo can be in front of the tame kangaroo, in which case it is better to think of each kangaroo trying to catch the other.

Figure 14.1: Kangaroo walk. Tame kangaroo walk pictured above the axis and wild kangaroo walk pictured below. The dot indicates the first collision.



- The pseudorandom walk is a sequence $x_0, x_1, \ldots$ of elements of G defined by an initial value x_0 (to be specified later) and the formula

$$x_{i+1} = x_i g_{S(x_i)}.$$

The algorithm is not based on the birthday paradox, but instead on the following observations. Footprints are spaced, on average, distance m apart, so along a region traversed by a kangaroo there is, on average, one footprint in any interval of length m. Now, if a second kangaroo jumps along the same region and if the jumps of the second kangaroo are independent of the jumps from the first kangaroo, then the probability of a collision is roughly $1/m$. Hence, one expects a collision between the two walks after about m steps.

14.5.2 The Kangaroo Algorithm

We need to specify where to start the tame and wild kangaroos, and what the mean step size should be. The wild kangaroo starts at $y_0 = h = g^a$ with $0 \leq a < w$. To minimise the distance between the tame and wild kangaroos at the start of the algorithm, we start the tame kangaroo at $x_0 = g^{\lfloor w/2 \rfloor}$, which is the middle of the interval. We take alternate jumps and store the values (x_i, a_i) and (y_i, b_i) as above (i.e., so that $x_i = g^{a_i}$ and $y_i = hg^{b_i}$). Whenever x_i (respectively, y_i) is distinguished we store (x_i, a_i) (resp., (y_i, b_i)) in an easily searched structure. The storage can be reduced by using the ideas of Exercise 14.2.18.

When the same distinguished point is visited twice then we have two entries (x, a) and (x, b) in the structure and so either $hg^a = g^b$ or $g^a = hg^b$. The ambiguity is resolved by seeing which of $a - b$ and $b - a$ lies in the interval (or just testing if $h = g^{a-b}$ or not).

As we will explain in Section 14.5.3, the optimal choice for the mean step size is $m = \sqrt{w}/2$.

Exercise 14.5.1. Write this algorithm in pseudocode.

We visualise the algorithm not in the group G but on a line representing exponents. The tame kangaroo starts at $\lfloor w/2 \rfloor$. The wild kangaroo starts somewhere in the interval $[0, w)$. Kangaroo jumps are small steps to the right. See Figure 14.1 for the picture.

Example 14.5.2. Let $g = 3 \in \mathbb{F}_{263}^*$ which has prime order 131. Let $h = 181 \in \langle g \rangle$ and suppose we are told that $h = g^a$ with $0 \leq a < w = 53$. The kangaroo method can be used in this case.

Since $\sqrt{w}/2 \approx 3.64$ it is appropriate to take $n_S = 4$ and choose steps $\{1, 2, 4, 8\}$. The mean step size is 3.75. The function $S(x)$ is $x \pmod 4$ (where elements of $\mathbb{F}^*_{263}$ are represented by integers in the set $\{1, \ldots, 262\}$).

The tame kangaroo starts at $(x_1, a_1) = (g^{26}, 26) = (26, 26)$. The sequence of points visited in the walk is listed below. A point is distinguished if its representation as an integer is divisible by 3; the distinguished points are written in bold face in the table.

i	0	1	2	3	4
x_i	26	2	**162**	235	**129**
a_i	26	30	34	38	46
$S(x_i)$	2	2	2	3	1
y_i	181	**51**	**75**	2	**162**
b_i	0	2	10	18	22
$S(y_i)$	1	3	3	2	2

The collision is detected when the distinguished point 162 is visited twice. The solution to the discrete logarithm problem is therefore $34 - 22 = 12$.

Exercise 14.5.3. Using the same parameters as Example 14.5.2, solve the DLP for $h = 78$.

14.5.3 Heuristic Analysis of the Kangaroo Method

The analysis of the algorithm does not rely on the birthday paradox; instead, the mean step size is the crucial quantity. We sketch the basic probabilistic argument now. A more precise analysis is given in Section 14.5.6. The following heuristic assumption seems to be reasonable when w is sufficiently large, $n_S > \log(w)$, distinguished points are sufficiently common and specified using a good hash function (and hence are well distributed), $\theta > \log(w)/\sqrt{w}$ and when the function walk is chosen at random.

Heuristic 14.5.4.

1. Walks reach a distinguished point in significantly fewer than $\sqrt{w}$ steps (in other words, there are no cycles in the walks and walks are not excessively longer than $1/\theta$).
2. The footprints of a kangaroo are uniformly distributed in the region over which it has walked with, on average, one footprint in each interval of length m.
3. The footsteps of tame and wild kangaroos are independent of one another before the time when the walks collide.

Theorem 14.5.5. *Let the notation be as above and assume Heuristic 14.5.4. Then the kangaroo algorithm with distinguished points has average case expected running time of* $(2 + o(1))\sqrt{w}$ *group operations. The probability the algorithm fails is negligible.*

Proof: We don't know whether the discrete logarithm of h is greater or less than $w/2$. So, rather than speaking of "tame" and "wild" kangaroos we will speak of the "front" and "rear" kangaroos. Since one kangaroo starts in the middle of the interval, the distance between the starting point of the rear kangaroo and the starting point of the front kangaroo is between 0 and $w/2$ and is, on average, $w/4$. Hence, on average, $w/(4m)$ jumps are required for the rear kangaro to pass the starting point of the front kangaroo.

After this point, the rear kangaroo is travelling over a region that has already been jumped over by the front kangaroo. By our heuristic assumption, the footprints of the

tame kangaroo are uniformly distributed over the region with, on average, one footprint in each interval of length m. Also, the footprints of the wild kangaroo are independent, and with one footprint in each interval of length m. The probability, at each step, that the wild kangaroo does not land on any of the footprints of the tame kangaroo is therefore heuristically $1 - 1/m$. By exactly the same arguments as Lemma 14.2.14 it follows that the expected number of jumps until a collision is m.

Note that there is a miniscule possibility that the walks never meet (this does not require working in an infinite group, it can even happen in a finite group if the "orbits" of the tame and wild walks are disjoint subsets of the group). If this happens then the algorithm never halts. Since the walk function is chosen at random, the probability of this eventuality is negligible. On the other hand, if the algorithm halts then its result is correct. Hence, this is a Las Vegas algorithm.

The overall number of jumps made by the rear kangaroo until the first collision is therefore, on average, $w/(4m) + m$. One can easily check that this is minimised by taking $m = \sqrt{w}/2$. The kangaroo is also expected to perform a further $1/\theta$ steps to the next distinguished point. Since there are two kangaroos the expected total number of group operations performed is $2\sqrt{w} + 2/\theta = (2 + o(1))\sqrt{w}$. □

This result is proved by Montenegro and Tetali [434] under the assumption that S is a random function and that the distinguished points are well-distributed. Pollard [488] shows it is valid when the $o(1)$ is replaced by ϵ for some $0 \leq \epsilon < 0.06$.

Note that the expected distance, on average, travelled by a kangaroo is $w/4 + m^2 = w/2$ steps. Hence, since the order of the group is greater than w, we do not expect any self-collisions in the kangaroo walk.

We stress that, as with the rho method, the probability of success is considered over the random choice of pseudorandom walk, not over the space of problem instances. Exercise 14.5.6 considers a different way to optimise the expected running time.

Exercise 14.5.6. Show that, with the above choice of m, the expected number of group operations performed for the worst-case of problem instances is $(3 + o(1))\sqrt{w}$. Determine the optimal choice of m to minimise the expected worst-case running time. What is the expected worst-case complexity?

Exercise 14.5.7. A card trick known as **Kruskal's principle** is as follows. Shuffle a deck of 52 playing cards and deal face up in a row. Define the following walk along the row of cards: If the number of the current card is i then step forward i cards (if the card is a King, Queen or Jack then step 5 cards). The magician runs this walk (in their mind) from the first card and puts a coin on the last card visited by the walk. The magician invites their audience to choose a number j between 1 and 10, then runs the walk from the j-th card. The magician wins if the walk also lands on the card with the coin. Determine the probability of success of this trick.

Exercise 14.5.8. Show how to use the kangaroo method to solve Exercises 13.3.8, 13.3.10 and 13.3.11 of Chapter 13.

Pollard's original proposal did not use distinguished points and the algorithm only had a fixed probability of success. In contrast, the method we have described keeps on running until it succeeds (indeed, if the DLP is insoluble then the algorithm would never terminate). Van Oorschot and Wiener (see page 12 of [473]) have shown that repeating Pollard's original method until it succeeds leads to a method with expected running time of approximately $3.28\sqrt{w}$ group operations.

Exercise 14.5.9. Suppose one is given $g \in G$ of order r, an integer w, and an instance generator for the discrete logarithm problem that outputs $h = g^a \in G$ such that $0 \leq a < w$

according to some known distribution on $\{0, 1, \ldots, w-1\}$. Assume that the distribution is symmetric with mean value $w/2$. How should one modify the kangaroo method to take account of this extra information? What is the running time?

14.5.4 Comparison with the Rho Algorithm

We now consider whether one should use the rho or kangaroo algorithm when solving a general discrete logarithm problem (i.e., where the width w of the interval is equal to, or close to, r). If $w = r$ then the rho method requires roughly $1.25\sqrt{r}$ group operations while the kangaroo method requires roughly $2\sqrt{r}$ group operations. The heuristic assumptions underlying both methods are similar, and in practice they work as well as the theory predicts. Hence, it is clear that the rho method is preferable, unless w is much smaller than r.

Exercise 14.5.10. Determine the interval size below which it is preferable to use the kangaroo algorithm over the rho algorithm.

14.5.5 Using Inversion

Galbraith, Ruprai and Pollard [226] showed that one can improve the kangaroo method by exploiting inversion in the group.[11] Suppose one is given g, h, w and told that $h = g^a$ with $0 \leq a < w$. We also require that the order r of g is odd (this will always be the case, due to the Pohlig-Hellman algorithm). Suppose, for simplicity, that w is even. Replacing h by $hg^{-w/2}$ we have $h = g^a$ with $-w/2 \leq a < w/2$. One can perform a version of the kangaroo method with three kangaroos: One tame kangaroo starting from g^u for an appropriate value of u and two wild kangaroos starting from h and h^{-1} respectively.

The algorithm uses the usual kangaroo walk (with mean step size to be determined later) to generate three sequences $(x_i, a_i), (y_i, b_i), (z_i, c_i)$ such that $x_i = g^{a_i}$, $y_i = hg^{b_i}$ and $z_i = h^{-1}g^{c_i}$. The crucial observation is that a collision between any two sequences leads to a solution to the DLP. For example, if $x_i = y_j$ then $h = g^{a_i - b_j}$ and if $y_i = z_j$ then $hg^{b_i} = h^{-1}g^{c_j}$ and so, since g has odd order r, $h = g^{(c_j - b_i)2^{-1} \pmod r}$. The algorithm uses distinguished points to detect a collison. We call this the **three-kangaroo algorithm**.

Exercise 14.5.11. Write down pseudocode for the three-kangaroo algorithm using distinguished points.

We now give a brief heuristic analysis of the three-kangaroo algorithm. Without loss of generality we assume $0 \leq a \leq w/2$ (taking negative a simply swaps h and h^{-1}, so does not affect the running time). The distance between the starting points of the tame and wild kangaroos is $2a$. The distance between the starting points of the tame and right-most wild kangaroo is $|a - u|$. The extreme cases (in the sense that the closest pair of kangaroos are as far apart as possible) are when $2a = u - a$ or when $a = w/2$. Making all these cases equal leads to the equation $2a = u - a = w/2 - u$. Calling this distance l it follows that $w/2 = 5l/2$ and $u = 3w/10$. The average distance between the closest pair of kangaroos is then $w/10$ and the closest pair of kangaroos can be thought of as performing the standard kangaroo method in an interval of length $2w/5$. Following the analysis of the standard kangaroo method it is natural to take the mean step size to be $m = \frac{1}{2}\sqrt{2w/5} = \sqrt{w/10} \approx 0.316\sqrt{w}$. The average-case expected number of group operations (only considering the closest pair of kangaroos) would be $\frac{3}{2}2\sqrt{2w/5} \approx 1.897\sqrt{w}$. A more careful analysis takes into account the possibility of collisions between any pair of kangaroos. We refer to [226]

[11] This research actually grew out of writing this chapter. Sometimes it pays to work slowly.

for the details and merely remark that the correct mean step size is $m \approx 0.375\sqrt{w}$ and the average-case expected number of group operations is approximately $1.818\sqrt{w}$.

Exercise 14.5.12. The distance between $-a$ and a is even, so a natural trick is to use jumps of even length. Since we don't know whether a is even or odd, if this is done we don't know whether to start the tame kangaroo at g^u or g^{u+1}. However, one can consider a variant of the algorithm with two wild kangaroos (one starting from h and one from h^{-1}) and two tame kangaroos (one starting from g^u and one from g^{u+1}) and with jumps of even length. This is called the **four-kangaroo algorithm**. Explain why the correct choice for the mean step size is $m = 0.375\sqrt{2w}$ and why the heuristic average-case expected number of group operations is approximately $1.714\sqrt{w} = \frac{2\sqrt{2}}{3}1.818\sqrt{w}$.

Galbraith, Pollard and Ruprai [226] have combined the idea of Exercise 14.5.12 and the Gaudry-Schost algorithm (see Section 14.7) to obtain an algorithm for the discrete logarithm problem in an interval of length w that performs $(1.660 + o(1))\sqrt{w}$ group operations.

14.5.6 Towards a Rigorous Analysis of the Kangaroo Method

Montenegro and Tetali [434] have analysed the kangaroo method using jumps which are powers of 2, under the assumption that the selection function S is random and that the distinguished points are well-distributed. They prove that the average-case expected number of group operations is $(2 + o(1))\sqrt{w}$ group operations. It is beyond the scope of this book to present their methods.

We now present Pollard's analysis of the kangaroo method from his paper [488], though these results have been superseded by [434]. We restrict to the case where the selection function S maps G to $\{0, 1, \ldots, n_S - 1\}$ and the kangaroo jumps are taken to be $2^{S(x)}$ (i.e., the set of jumps is $\{1, 2, 4, \ldots, 2^{n_S-1}\}$ and the mean of the jumps is $m = (2^{n_S} - 1)/n_S$). We assume $n_S > 2$. Pollard argues in [488] that if one only uses two jumps $\{1, 2^n\}$ (for some n) then the best one can hope for is an algorithm with running time $O(w^{2/3})$ group operations.

Pollard also makes the usual assumption that S is a truly random function.

As always we visualise the kangaroos in terms of their exponents, and so we study a pseudorandom walk on $\mathbb{Z}$. The tame kangaroo starts at w. The wild kangaroo starts somewhere in $[0, w)$. We begin the analysis when the wild kangaroo first lands at a point $\geq w$. Let $w + i$ be the first wild kangaroo footprint $\geq w$. Define $q(i)$ to be the probability (over all possible starting positions for the wild kangaroo) that this first footstep is at $w+i$. Clearly $q(i) = 0$ when $i \geq 2^{n_S-1}$. The wild kangaroo footprints are chosen uniformly at random with mean m, hence $q(0) = 1/m$. For $i > 0$ then only jumps of length $> i$ could be useful, so the probability is

$$q(i) = \#\{0 \leq j < n_S : 2^j > i\}/mn_S.$$

To summarise $q(1) = (n_S - 1)/mn_S, q(2) = (n_S - 2)/mn_S$ and for $i > 2$, $q(i) = (n_S - 1 - \lfloor \log_2(i) \rfloor)/mn_S$.

We now want to analyse how many further steps the wild kangaroo makes before landing on a footprint of the tame kangaroo. We abstract the problem to the following: Suppose the front kangaroo is at i and the rear kangaroo is at 0 and run the pseudorandom walk. Define $F(i)$ to be the expected number of steps made by the front kangaroo to the collision and $B(i)$ the expected number of steps made by the rear kangaroo to the collision.

We can extend the functions to F and B to $i = 0$ by taking a truly random and independent step from $\{1, 2, 4, \ldots, 2^{n_S-1}\}$ (i.e., not using the deterministic pseudorandom walk function).

We can now obtain formulae relating the functions $F(i)$ and $B(i)$. Consider one jump by the rear kangaroo. Suppose the jump has distance s where $s < i$. Then the rear kangaroo remains the rear kangaroo, but the front kangaroo is now only $i - s$ ahead. If $F(i-s) = n_1$ and $B(i-s) = n_2$ then we have $F(i) = n_1$ and $B(i) = 1 + n_2$. On the other hand, suppose the jump has distance $s \geq i$. Then the front and rear kangaroo swap roles and the front kangaroo is now $s - i$ ahead. We have $B(i) = 1 + F(s-i)$ and $F(i) = B(s-i)$. Since the steps are chosen uniformly with probability $1/n_S$ we get

$$F(i) = \tfrac{1}{n_S}\left(\sum_{j=0,2^j<i}^{n_S-1} F(i-2^j) + \sum_{j=0,2^j\geq i}^{n_S-1} B(2^j - i)\right)$$

and

$$B(i) = 1 + \tfrac{1}{n_S}\left(\sum_{j=0,2^j<i}^{n_S-1} B(i-2^j) + \sum_{j=0,2^j\geq i}^{n_S-1} F(2^j - i)\right)$$

Pollard then considers the expected value of the number of steps of the wild kangaroo to a collision, namely

$$\sum_{i=1}^{2^{(n_S-1)}-1} q(i)F(i)$$

which we write as $mC(n_S)$ for some $C(n_S) \in \mathbb{R}$. In [488] one finds numerical data for $C(n_S)$ which suggest that it is between 1 and 1.06 when $n_S \geq 12$. Pollard also conjectures that $\lim_{n_S\to\infty} C(n_S) = 1$.

Given an interval of size w one chooses n_S such that the mean $m = (2^{n_S} - 1)/n_S$ is as close as possible to $\sqrt{w}/2$. One runs the tame Kangaroo, starting at w, for $mC(n_S)$ steps and sets the trap. The wild kangaroo is expected to need $w/2m$ steps to pass the start of the tame kangaroo followed by $mC(n_S)$ steps to fall into the trap. Hence, the expected number of group operations for the kangaroo algorithm (for a random function S) is

$$w/2m + 2mC(n_S).$$

Taking $m = \sqrt{w}/2$ gives expected running time

$$(1 + C(n_S))\sqrt{w}$$

group operations.

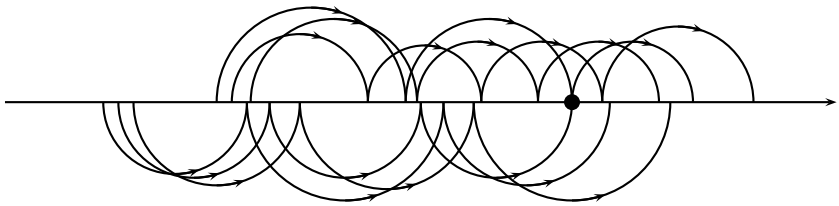
In practice one would slightly adjust the jumps $\{1, 2, 4, \ldots, 2^{n_S-1}\}$ (while hoping that this does not significantly change the value of $C(n_S)$) to arrange that $m = \sqrt{w/C(n_S)}/2$.

14.6 Distributed Kangaroo Algorithm

Let N_P be the number of processors or clients. A naive way to parallelise the the kangaroo algorithm is to divide the interval $[0, w)$ into N_P sub-intervals of size w/N_P and then run the kangaroo algorithm in parallel on each sub-interval. This gives an algorithm with running time $O(\sqrt{w/N_P})$ group operations per client, which is not a linear speedup.

Since we are using distinguished points one should be able to do better. But the kangaroo method is not as straightforward to parallelise as the rho method (a good exercise is to stop reading now and think about it for a few minutes). The solution is to use a herd of $N_P/2$ tame kangaroos and a herd of $N_P/2$ wild kangaroos. These are super-kangaroos in the sense that they take much bigger jumps (roughly $N_P/2$ times

Figure 14.2: Distributed kangaroo walk (van Oorschot and Wiener version). The herd of tame kangaroos is pictured above the axis and the herd of wild kangaroos is pictured below. The dot marks the collision.



longer) than in the serial case. The goal is to have a collision between one of the wild kangaroos and one of the tame kangaroos. We imagine that both herds are setting traps, each trying to catch a kangaroo from the other herd (regrettably, they may sometimes catch one of their own kind).

When a kangaroo lands on a distinguished point one continues the pseudorandom walk (rather than restarting the walk at a new randomly chosen position). In other words, the herds march ever onwards with an occasional individual hitting a distinguished point and sending information back to the server. See Figure 14.2 for a picture of the herds in action.

There are two versions of the distributed algorithm, one by van Oorschot and Wiener [473] and another by Pollard [488]. The difference is how they handle the possibility of collisions between kangaroos of the same herd. The former has a mechanism to deal with this, which we will explain later. The latter paper elegantly ensures that there will not be collisions between individuals of the same herd.

14.6.1 Van Oorschot and Wiener Version

We first present the algorithm of van Oorschot and Wiener. The herd of tame kangaroos starts around the midpoint of the interval $[0, w)$, and the kangaroos are spaced a (small) distance s apart (as always, we describe kangaroos by their exponent). Similarly, the wild kangaroos start near $a = \log_g(h)$, again spaced a distance s apart. As we will explain later, the mean step size of the jumps should be $m \approx N_P\sqrt{w}/4$.

Here $\mathsf{walk}(x_i, a_i)$ is the function which returns $x_{i+1} = x_i g_{S(x_i)}$ and $a_{i+1} = a_i + u_{S(x_i)}$. Each client has a variable type which takes the value 'tame' or 'wild'.

If there is a collision between two kangaroos of the same herd then it will eventually be detected when the second one lands on the same distinguished point as the first. In [473] it is suggested that in this case the server should instruct the second kangaroo to take a jump of random length so that it no longer follows the path of the front kangaroo. Note that Teske [606] has shown that the expected number of collisions within the same herd is 2, so this issue can probably be ignored in practice.

We now give a very brief heuristic analysis of the running time. The following assumption seems to be reasonable when w is sufficiently large, n_S is sufficiently large, $\log(w)/\sqrt{w} < \theta$, the set $\mathcal{D}$ of distinguished points is determined by a good hash function, the number N_P of clients is sufficiently small (e.g., $N_P < \theta\sqrt{\pi r/2}/\log(r)$, see Exercise 14.3.3), the spacing s is independent of the steps in the random walk and is sufficiently large, the function walk is chosen at random.

Algorithm 19 The distributed kangaroo algorithm (van Oorschot and Wiener version): Server side

INPUT: $g, h \in G$, interval length w, number of clients N_P
OUTPUT: a such that $h = g^a$

Choose n_S, a random function $S : G \to \{0, \ldots, n_S - 1\}$, $m = N_P\sqrt{w}/4$, jumps $\{u_0, \ldots, u_{n_S-1}\}$ with mean m, spacing s
for $i = 1$ to $N_P/2$ **do** ▷ Start $N_P/2$ tame kangaroo clients
    Set $a_i = \lfloor w/2 \rfloor + is$
    Initiate client on $(g^{a_i}, a_i, \text{'tame'})$ with function walk
end for
for $j = 1$ to $N_P/2$ **do** ▷ Start $N_P/2$ wild kangaroo clients
    Set $a_j = js$
    Initiate client on $(hg^{a_j}, a_j, \text{'wild'})$ with function walk
end for
Initialise an easily sorted structure L (sorted list, binary tree etc) to be empty
while DLP not solved **do**
    Receive triples $(x_i, a_i, \mathsf{type}_i)$ from clients and insert into L
    if first coordinate of new triple $(x, a_2, \mathsf{type}_2)$ matches existing triple $(x, a_1, \mathsf{type}_1)$ **then**
        if $\mathsf{type}_2 = \mathsf{type}_1$ **then**
            Send message to the sender of $(x, a_2, \mathsf{type}_2)$ to take a random jump
        else
            Send terminate signal to all clients
            if $\mathsf{type}_1 =$'tame' **then**
                return $(a_1 - a_2) \pmod r$
            else
                return $(a_2 - a_1) \pmod r$
            end if
        end if
    end if
end while

Algorithm 20 The distributed kangaroo algorithm (van Oorschot and Wiener version): Client side

INPUT: $(x_1, a_1, \mathsf{type}) \in G \times \mathbb{Z}/r\mathbb{Z}$, function walk

while terminate signal not received **do**
    $(x_1, a_1) = \mathsf{walk}(x_1, a_1)$
    if $x_1 \in \mathcal{D}$ **then**
        Send $(x_1, a_1, \mathsf{type})$ to server
        if Receive jump instruction **then**
            Choose random $1 < u < 2m$ (where m is the mean step size)
            Set $a_1 = a_1 + u$, $x_1 = x_1 g^u$
        end if
    end if
end while

Heuristic 14.6.1.

1. Walks reach a distinguished point in significantly fewer than $\sqrt{w}$ steps (in other words, there are no cycles in the walks and walks are not excessively longer than $1/\theta$).
2. When two kangaroos with mean step size m walk over the same interval, the expected number of group elements sampled before a collision is m.
3. Walks of kangaroos in the same herd are independent.[12]

Theorem 14.6.2. *Let N_P be the number of clients (fixed, independent of w). Assume Heuristic 14.6.1 and that all clients are reliable and have the same computing power. The average-case expected number of group operations performed by the distributed kangaroo method for each client is $(2 + o(1))\sqrt{w}/N_P$.*

Proof: Since we don't know where the wild kangaroo is, we speak of the front herd and the rear herd. The distance (in the exponent) between the front herd and the rear herd is, on average, $w/4$. So it takes $w/(4m)$ steps for the rear herd to reach the starting point of the front herd.

We now consider the footsteps of the rear herd in the region already visited by the front herd of kangaroos. Assuming the $N_P/2$ kangaroos of the front herd are independent, the region already covered by these kangaroos is expected to have $N_P/2$ footprints in each interval of length m. Hence, under our heuristic assumptions, the probability that a random footprint of one of the rear kangaroos lands on a footprint of one of the front kangaroos is $N_P/(2m)$. Since there are $N_P/2$ rear kangaroos, all mutually independent, the probability of one of the rear kangaroos landing on a tame footprint is $N_P^2/(4m)$. By the heuristic assumption, the expected number of footprints to be made before a collision occurs is $4m/N_P^2$.

Finally, the collision will not be detected until a distinguished point is visited. Hence, one expects a further $1/\theta$ steps to be made.

The expected number of group operations made by each client in the average case is therefore $w/(4m) + 4m/N_P^2 + 1/\theta$. Ignoring the $1/\theta$ term, this expression is minimised by taking $m = N_P\sqrt{w}/4$. The result follows. □

The remarks made in Section 14.3.1 about parallelisation (for example, Exercise 14.3.3) apply equally for the distributed kangaroo algorithm.

Exercise 14.6.3. The above analysis is optimised for the average-case running time. Determine the mean step size to optimise the worst-case expected running time. Show that the heuristic optimal running time is $(3 + o(1))\sqrt{w}/N_P$ group operations.

Exercise 14.6.4. Give distributed versions of the three-kangaroo and four-kangaroo algorithms of Section 14.5.5.

14.6.2 Pollard Version

Pollard's version reduces the computation to essentially a collection of serial versions, but in a clever way so that a linear speed-up is still obtained. One merit of this approach is

[12] This assumption is very strong, and indeed is false in general (since there is a chance that walks collide). The assumption is used for only two purposes. First, to "amplify" the second assumption in the heuristic from any pair of kangaroos to the level of herds. Second, to allow us to ignore collisions between kangaroos in the same herd (Teske, in Section 7 of [606], has argued that such collisions are rare). One could replace the assumption of independence by these two consequences.

that the analysis of the serial kangaroo algorithm can be applied; we no longer need the strong heuristic assumption that kangaroos in the same herd are mutually independent.

Let N_P be the number of processors and suppose we can write $N_P = U + V$ where $\gcd(U, V) = 1$ and $U, V \approx N_P/2$. The number of tame kangaroos is U and the number of wild kangaroos is V. The (super) kangaroos perform the usual pseudorandom walk with steps $\{UVu_0, \ldots, UVu_{n-1}\}$ having mean $m \approx N_P\sqrt{w}/4$ (this is UV times the mean step size for solving the DLP in an interval of length $w/UV \approx 4w/N_P^2$). As usual we choose either $u_j \approx 2^j$ or else random values between 0 and $2m/UV$.

The U tame kangaroos start at

$$g^{\lfloor w/2 \rfloor + iV}$$

for $0 \leq i < U$. The V wild kangaroos start at hg^{jU} for $0 \leq j < V$. Each kangaroo then uses the pseudorandom walk to generate a sequence of values (x_n, a_n) where $x_n = g^{a_n}$ or $x_n = hg^{a_n}$. Whenever a distinguished point is hit the kangaroo sends data to the server and continues the same walk.

Lemma 14.6.5. *Suppose the walks do not cover the whole group, i.e., $0 \leq a_n < r$. Then there is no collision between two tame kangaroos or two wild kangaroos. There is a unique pair of tame and wild kangaroos who can collide.*

Proof: Each element of the sequence generated by the ith tame kangaroo is of the form

$$g^{\lfloor w/2 \rfloor + iV + lUV}$$

for some $l \in \mathbb{Z}$. To have a collision between two different tame kangaroos one would need

$$\lfloor w/2 \rfloor + i_1 V + l_1 UV = \lfloor w/2 \rfloor + i_2 V + l_2 UV$$

and reducing modulo U implies $i_1 \equiv i_2 \pmod{U}$ which is a contradiction. To summarise, the values a_n for the tame kangaroos all lie in disjoint equivalence classes modulo U. A similar argument shows that wild kangaroos do not collide.

Finally, if $h = g^a$ then $i = (\lfloor w/2 \rfloor - a)V^{-1} \pmod{U}$ and $j = (a - \lfloor w/2 \rfloor)U^{-1} \pmod{V}$ are the unique pair of indices such that the ith tame kangaroo and the jth wild kangaroo can collide. □

The analysis of the algorithm therefore reduces to the serial case, since we have one tame kangaroo and one wild kangaroo who can collide. This makes the heuristic analysis simple and immediate.

Theorem 14.6.6. *Let the notation be as above. Assume Heuristic 14.5.4 and that all clients are reliable and have the same computational power. Then the average-case expected running time for each client is $(1 + o(1))\sqrt{w/UV} = (2 + o(1))\sqrt{w}/N_P$ group operations.*

Proof: The action is now constrained to an equivalence class modulo UV, so the clients behave like the serial kangaroo method in an interval of size w/UV (see Exercise 14.5.8 for reducing a DLP in a congruence class to a DLP in a smaller interval). The mean step size is therefore $m \approx UV\sqrt{w/UV}/2 \approx N_P\sqrt{w}/4$. Applying Theorem 14.5.5 gives the result. □

14.6.3 Comparison of the Two Versions

Both versions of the distributed kangaroo method have the same heuristic running time of $(2 + o(1))\sqrt{w}/N_P$ group operations.[13] So which is to be preferred in practice? The

[13] Though the analysis by van Oorschot and Wiener needs the stronger assumption that the kangaroos in the same herd are mutually independent.

answer depends on the context of the computation. For genuine parallel computation in a closed system (e.g., using special-purpose hardware) then either could be used.

In distributed environments then both methods have drawbacks. For example, the van Oorschot-Wiener method needs a communication from server to client in response to uploads of distinguished point information (the "take a random jump" instruction); though Teske [606] has remarked that this can probably be ignored.

More significantly, both methods require knowing the number N_P of processors at the start of the computation, since this value is used to specify the mean step size. This causes problems if a large number of new clients join the computation after it has begun.

With the van Oorschot and Wiener method, if further clients want to join the computation after it has begun, then they can be easily added (half the new clients tame and half wild) by starting them at further shifts from the original starting points of the herds. With Pollard's method it is less clear how to add new clients. Even worse, since only one pair of "lucky" clients has the potential to solve the problem, if either of them crashes or withdraws from the computation then the problem will not be solved. As mentioned in Section 14.4.3 these are serious issues which do arise in practice.

On the other hand, these issues can be resolved by over-estimating N_P and by issuing clients with fresh problem instances once they have produced sufficiently many distinguished points from their current instance. Note that this also requires communication from server to client.

14.7 The Gaudry-Schost Algorithm

Gaudry and Schost [249] give a different approach to solving discrete logarithm problems using pseudorandom walks. As we see in Exercise 14.7.6, this method is slower than the rho method when applied to the whole group. However, the approach leads to low-storage algorithms for the multi-dimensional discrete logarithm problems (see Definition 13.5.1); and the discrete logarithm problem in an interval using equivalence classes. This is interesting since, for both problems, it is not known how to adapt the rho or kangaroo methods to give a low-memory algorithm with the desired running time.

The basic idea of the Gaudry-Schost algorithm is as follows. One has pseudorandom walks in two (or more) subsets of the group such that a collision between walks of different types leads to a solution to the discrete logarithm problem. The sets are smaller than the whole group, but they must overlap (otherwise, there is no chance of a collision). Typically, one of the sets is called a "tame set" and the other a "wild set". The pseudorandom walks are deterministic, so that when two walks collide they continue along the same path until they hit a distinguished point and stop. Data from distinguished points is held in an easily searched database held by the server. After reaching a distinguished point, the walks re-start at a freshly chosen point.

14.7.1 Two-Dimensional Discrete Logarithm Problem

Suppose we are given $g_1, g_2, h \in G$ and $N \in \mathbb{N}$ (where we assume N is even) and asked to find integers $0 \leq a_1, a_2 < N$ such that $h = g_1^{a_1} g_2^{a_2}$. Note that the size of the solution space is N^2, so we seek a low-storage algorithm with number of group operations proportional to N. The basic Gaudry-Schost algorithm for this problem is as follows.

Define the tame set

$$T = \{(x, y) \in \mathbb{Z}^2 : 0 \leq x, y < N\}$$

and the wild set

$$W = (a_1 - N/2, a_2 - N/2) + T = \{(a_1 - N/2 + x, a_2 - N/2 + y) \in \mathbb{Z}^2 : 0 \leq x, y < N\}.$$

In other words, T and W are $N \times N$ boxes centered on $(N/2-1, N/2-1)$ and (a_1, a_2) respectively. It follows that $\#W = \#T = N^2$ and if $(a_1, a_2) = (N/2-1, N/2-1)$ then $T = W$, otherwise $T \cap W$ is a proper non-empty subset of T.

Define a pseudorandom walk as follows: First choose $n_S > \log(N)$ random pairs of integers $-M < m_i, n_i < M$ where M is an integer to be chosen later (typically, $M \approx N/(1000\log(N))$) and precompute elements of the form $w_i = g_1^{m_i} g_2^{n_i}$ for $0 \leq i < n_S$. Then choose a selection function $S : G \to \{0, 1, \ldots, n_S - 1\}$. The walk is given by the function

$$\mathsf{walk}(g, x, y) = (g w_{S(g)}, x + m_{S(g)}, y + n_{S(g)}).$$

Tame walks are started at $(g_1^x g_2^y, x, y)$ for random elements $(x, y) \in T$ and wild walks are started at $(h g_1^{x-N/2+1} g_2^{y-N/2+1}, x - N/2 + 1, y - N/2 + 1)$ for random elements $(x, y) \in T$. Walks proceed by iterating the function walk until a distinguished element of G is visited; at which time the data (g, x, y), together with the type of walk, is stored in a central database. When a distinguished point is visited, the walk is re-started at a uniformly chosen group element (this is like the rho method, but different from the behaviour of kangaroos). Once two walks of different types visit the same distinguished group element we have a collision of the form

$$g_1^x g_2^y = h g_1^{x'} g_2^{y'}$$

and the two-dimensional DLP is solved.

Exercise 14.7.1. Write pseudocode, for both the client and server, for the distributed Gaudry-Schost algorithm.

Exercise 14.7.2. Explain why the algorithm can be modified to omit storing the the type of walk in the database. Show that the methods of Exercise 14.2.18 to reduce storage can also be used in the Gaudry-Schost algorithm.

Exercise 14.7.3. What modifications are required to solve the problem $h = g_1^{a_1} g_2^{a_2}$ such that $0 \leq a_1 < N_1$ and $0 \leq a_2 < N_2$ for $0 < N_1 < N_2$?

An important practical consideration is that walks will sometimes go outside the tame or wild regions. One might think that this issue can be solved by simply taking the values x and y into account and altering the walk when close to the boundary, but then the crucial property of the walk function (that once two walks collide, they follow the same path) would be lost. By taking distinguished points to be quite common (i.e., increasing the storage) and making M relatively small one can minimise the impact of this problem. Hence, we ignore it in our analysis.

We now briefly explain the heuristic complexity of the algorithm. The key observation is that a collision can only occur in the region where the two sets overlap. Let $A = T \cap W$. If one samples uniformly at random in A, alternately writing elements down on a "tame" and "wild" list, the expected number of samples until the two lists have an element in common is $\sqrt{\pi \# A} + O(1)$ (see, for example, Selivanov [536] or [223]).

The following heuristic assumption seems to be reasonable when N is sufficiently large, $n_S > \log(N)$, distinguished points are sufficiently common and specified using a good hash function (and hence are well-distributed), $\theta > \log(N)/N$, walks are sufficiently "local" that they do not go outside T (respectively, W) but also not too local, and when the function walk is chosen at random.

Heuristic 14.7.4.

1. Walks reach a distinguished point in significantly fewer than N steps (in other words, there are no cycles in the walks and walks are not excessively longer than $1/\theta$).
2. Walks are uniformly distributed in T (respectively, W).

Theorem 14.7.5. *Let the notation be as above, and assume Heuristic 14.7.4. Then the average-case expected number of group operations performed by the Gaudry-Schost algorithm is* $(\sqrt{\pi}(2(2-\sqrt{2}))^2 + o(1))N \approx (2.43 + o(1))N$.

Proof: We first compute $\#(T \cap W)$. When $(a_1, a_2) = (N/2, N/2)$ then $W = T$ and so $\#(T \cap W) = N^2$. In all other cases the intersection is less. The extreme case is when $(a_1, a_2) = (0, 0)$ (similar cases are $(a_1, a_2) = (N-1, N-1)$ etc). Then $W = \{(x, y) \in \mathbb{Z}^2 : -N/2 \leq x, y < N/2\}$ and $\#(T \cap W) = N^2/4$. By symmetry it suffices to consider the case $0 \leq a_1, a_2 < N/2$ in which case we have $\#(T \cap W) \approx (N/2 + a_1)(N/2 + a_2)$ (here we are approximating the number of integer points in a set by its area).

Let $A = T \cap W$. To sample $\sqrt{\pi \# A}$ elements in A it is necessary to sample $\#T/\#A$ elements in T and W. Hence, the number of group elements to be selected overall is

$$\frac{\#T}{\#A}\big(\sqrt{\pi \# A} + O(1)\big) \;=\; (\#T + o(1))\sqrt{\pi}(\#A)^{-1/2}.$$

The average-case number of group operations is

$$(N^2 + o(1))\sqrt{\pi}\big(\tfrac{2}{N}\big)^2 \int_0^{N/2} \int_0^{N/2} (N-x)^{-1/2}(N-y)^{-1/2} dx dy.$$

Note that

$$\int_0^{N/2} (N-x)^{-1/2} dx \;=\; \sqrt{N}(2-\sqrt{2}).$$

The average-case expected number of group operations is therefore

$$\big(\sqrt{\pi}(2(2-\sqrt{2}))^2 + o(1)\big)N$$

as stated. □

The Gaudry-Schost algorithm has a number of parameters that can be adjusted (such as the type of walks, the sizes of the tame and wild regions etc). This gives it a lot of flexibility and makes it suitable for a wide range of variants of the DLP. Indeed, Galbraith and Ruprai [227] have improved the running time to $(2.36 + o(1))N$ group operations by using smaller tame and wild sets (also, the wild set is a different shape). One drawback is that it is hard to fine-tune all these parameters to get an implementation that achieves the theoretically optimal running time.

Exercise 14.7.6. Determine the complexity of the Gaudry-Schost algorithm for the standard DLP in G, when one takes $T = W = G$.

Exercise 14.7.7. Generalise the Gaudry-Schost algorithm to the n-dimensional DLP (see Definition 13.5.1). What is the heuristic average-case expected number of group operations?

14.7.2 Discrete Logarithm Problem in an Interval using Equivalence Classes

Galbraith and Ruprai [228] used the Gaudry-Schost algorithm to solve the DLP in an interval of length $N < r$ faster than is possible using the kangaroo method when the group has an efficiently computable inverse (e.g., elliptic curves or tori). First, shift the discrete logarithm problem so that it is of the form $h = g^a$ with $-N/2 < a \leq N/2$. Define the equivalence relation $u \equiv u^{-1}$ for $u \in G$ as in Section 14.4 and determine a rule that leads to a unique representative of each equivalence class. Design a pseudorandom walk on the set of equivalence classes. The tame set is the set of equivalence classes coming from elements of the form g^x with $-N/2 < x \leq N/2$. Note that the tame set has $1 + N/2$ elements and every equivalence class $\{g^x, g^{-x}\}$ arises in two ways, except the singleton class $\{1\}$ and the class $\{-N/2, N/2\}$.

A natural choice for the wild set is the set of equivalence classes coming from elements of the form hg^x with $-N/2 < x \leq N/2$. Note that the size of the wild set now depends on the discrete logarithm problem: if $h = g^0 = 1$ then the wild set has $1 + N/2$ elements while if $h = g^{N/2}$ then the wild set has N elements. Even more confusingly, sampling from the wild set by uniformly choosing x does not, in general, lead to uniform sampling from the wild set. This is because the equivalence class $\{hg^x, (hg^x)^{-1}\}$ can arise in either one or two ways, depending on h. To analyse the algorithm it is necessary to use a non-uniform version of the birthday paradox (see, for example, Galbraith and Holmes [223]). The main result of [228] is an algorithm that solves the DLP in heuristic average-case expected $(1.36 + o(1))\sqrt{N}$ group operations.

14.8 Parallel Collision Search in Other Contexts

Van Oorschot and Wiener [473] propose a general method, motivated by Pollard's rho algorithm, for finding collisions of functions using distinguished points and parallelisation. They give applications to cryptanalysis of hash functions and block ciphers that are beyond the scope of this book. But they also give applications of their method for algebraic meet-in-the-middle attacks, so we briefly give the details here.

First we sketch the parallel collision search method. Let $f : \mathcal{S} \to \mathcal{S}$ be a function mapping some set $\mathcal{S}$ of size N to itself. Define a set $\mathcal{D}$ of distinguished points in $\mathcal{S}$. Each client chooses a random starting point $x_1 \in \mathcal{S}$, iterates $x_{n+1} = f(x_n)$ until it hits a distinguished point, and sends (x_1, x_n, n) to the server. The client then restarts with a new random starting point. Eventually the server gets two triples (x_1, x, n) and (x_1', x, n') for the same distinguished point. As long as we don't have a "Robin Hood"[14] (i.e., one walk is a subsequence of another) the server can use the values (x_1, n) and (x_1', n') to efficiently find a collision $f(x) = f(y)$ with $x \neq y$. The expected running time for each client is $\sqrt{\pi N/2}/N_P + 1/\theta$, using the notation of this chapter. The storage requirement depends on the choice of θ.

We now consider the application to meet-in-the-middle attacks. A general meet-in-the-middle attack has two sets $\mathcal{S}_1$ and $\mathcal{S}_2$ and functions $f_i : \mathcal{S}_i \to \mathcal{R}$ for $i = 1, 2$. The goal is to find $a_1 \in \mathcal{S}_1$ and $a_2 \in \mathcal{S}_2$ such that $f_1(a_1) = f_2(a_2)$. The standard solution (as in baby-step-giant-step) is to compute and store all $(f_1(a_1), a_1)$ in an easily searched structure and then test for each $a_2 \in \mathcal{S}_2$ whether $f_2(a_2)$ is in the structure. The running time is $\#\mathcal{S}_1 + \#\mathcal{S}_2$ function evaluations and the storage is proportional to $\#\mathcal{S}_1$.

[14] Robin Hood is a character of English folklore who is expert in archery. His prowess allows him to shoot a second arrow on exactly the same trajectory as the first, so that the second arrow splits the first. Chinese readers may substitute the name Houyi.

The idea of [473] is to phrase this as a collision search problem for a single function f. For simplicity we assume that $\#\mathcal{S}_1 = \#\mathcal{S}_2 = N$. We write $I = \{0, 1, \ldots, N-1\}$ and assume one can construct bijective functions $\sigma_i : I \to \mathcal{S}_i$ for $i = 1, 2$. One defines a surjective map

$$\rho : \mathcal{R} \to I \times \{1, 2\}$$

and a set $\mathcal{S} = I \times \{1, 2\}$. Finally, define $f : \mathcal{S} \to \mathcal{S}$ as $f(x, i) = \rho(f_i(\sigma_i(x)))$. Clearly, the desired collision $f_1(a_1) = f_2(a_2)$ can arise from $f(\sigma_1^{-1}(a_1), 1) = f(\sigma_2^{-1}(a_2), 2)$, but collisions can also arise in other ways (for example, due to collisions in ρ). Indeed, since $\#\mathcal{S} = 2N$ one expects there to be roughly $2N$ pairs $(a_1, a_2) \in \mathcal{S}^2$ such that $a_1 \neq a_2$ but $f(a_1) = f(a_2)$. In many applications there is only one collision (van Oorschot and Wiener call it the "golden collision") that actually leads to a solution of the problem. It is therefore necessary to analyse the algorithm carefully to determine the expected time until the problem is solved.

Let N_P be the number of clients and let N_M be the total number of group elements that can be stored on the server. Van Oorschot and Wiener give a heuristic argument that the algorithm finds a useful collision after $2.5\sqrt{(2N)^3/N_M}/N_P$ group operations per client. This is taking $\theta = 2.25\sqrt{N_M/2N}$ for the probability of a distinguished point. We refer to [473] for the details.

14.8.1 The Low Hamming Weight DLP

Recall the low Hamming weight DLP: Given g, h, n, w find x of bit-length n and Hamming weight w such that $h = g^x$. The number of values for x is $M = \binom{n}{w}$ and there is a naive low storage algorithm running in time $\tilde{O}(M)$. We stress that the symbol w here means the Hamming weight; rather than its meaning earlier in this chapter.

Section 13.6 gave baby-step-giant-step algorithms for the low Hamming weight DLP that perform $O(\sqrt{w}\binom{n/2}{w/2})$ group operations. Hence these methods require time and space roughly proportional to $\sqrt{wM}$.

To solve the low Hamming weight DLP using parallel collision search one sets $\mathcal{R} = \langle g \rangle$ and $\mathcal{S}_1, \mathcal{S}_2$ to be sets of integers of binary length $n/2$ and Hamming weight roughly $w/2$. Define the functions $f_1(a) = g^a$ and $f_2(a) = hg^{-2^{n/2}a}$ so that a collision $f_1(a_1) = f_2(a_2)$ solves the problem. Note that there is a unique choice of (a_1, a_2) such that $f_1(a_1) = f_2(a_2)$ but when one uses the construction of van Oorschot and Wiener to get a single function f then there will be many useless collisions in f. We have $N = \#\mathcal{S}_1 = \#\mathcal{S}_2 \approx \binom{n/2}{w/2} \approx \sqrt{M}$ and so get an algorithm whose number of group operations is proportional to $N^{3/2} = M^{3/4}$ yet requires low storage. This is a significant improvement over the naive low-storage method, but still slower than baby-step-giant-step.

Exercise 14.8.1. Write this algorithm in pseudocode and give a more careful analysis of the running time.

It remains an open problem to give a low memory algorithm for the low Hamming weight DLP with complexity proportional to $\sqrt{wM}$ as with the BSGS methods.

14.9 Pollard Rho Factoring Method

This algorithm was proposed in [486] and was the first algorithm invented by Pollard that exploited pseudorandom walks. As more powerful factoring algorithms exist, we keep the presentation brief. For further details see Section 5.6.2 of Stinson [592] or Section 5.2.1 of Crandall and Pomerance [162].

Let N be a composite integer to be factored and let $p \mid N$ be a prime (usually p is the smallest prime divisor of N). We try to find a relation that holds modulo p but not modulo other primes dividing N.

The basic idea of the rho factoring algorithm is to consider the pseudorandom walk $x_1 = 2$ and

$$x_{i+1} = f(x_i) \pmod{N}$$

where the usual choice for $f(x)$ is $x^2 + 1$ (or $f(x) = x^2 + a$ for some small integer a). Consider the values $x_i \pmod{p}$ where $p \mid N$. The sequence $x_i \pmod{p}$ is a pseudorandom sequence of residues modulo p, and so after about $\sqrt{\pi p/2}$ steps we expect there to be indicies i and j such that $x_i \equiv x_j \pmod{p}$. We call this a **collision**. If $x_i \not\equiv x_j \pmod{N}$ then we can split N as $\gcd(x_i - x_j, N)$.

Example 14.9.1. Let $p = 11$. Then the rho iteration modulo p is

$$2,\ 5,\ 4,\ 6,\ 4,\ 6,\ 4,\ \ldots$$

Let $p = 19$. Then the sequence is

$$2,\ 5,\ 7,\ 12,\ 12,\ 12,\ \ldots$$

As with the discrete logarithm algorithms, the walk is deterministic in the sense that a collision leads to a cycle. Let l_t be the length of the tail and l_h be the length of the cycle. Then the first collision is

$$x_{l_t+l_h} \equiv x_{l_t} \pmod{p}.$$

We can use Floyd's cycle finding algorithm to detect the collision. The details are given in Algorithm 21. Note that it is not efficient to compute the gcd in line 5 of the algorithm for each iteration; Pollard [486] gave a solution to reduce the number of gcd computations and Brent [98] gave another.

Algorithm 21 The rho algorithm for factoring

INPUT: N
OUTPUT: A factor of N
1: $x_1 = 2$, $x_2 = f(x_1) \pmod{N}$
2: **repeat**
3: $\quad x_1 = f(x_1) \pmod{N}$
4: $\quad x_2 = f(f(x_2)) \pmod{N}$
5: $\quad d = \gcd(x_2 - x_1, N)$
6: **until** $1 < d < N$
7: **return** d

We now briefly discuss the complexity of the algorithm. Note that the "algorithm" may not terminate, for example if the length of the cycle and tail are the same for all $p \mid N$ then the gcd will always be either 1 or N. In practice one would stop the algorithm after a certain number of steps and repeat with a different choice of x_1 and/or $f(x)$. Even if it terminates, the length of the cycle of the rho may be very large. Hence, the usual approach is to make the heuristic assumption that the rho pseudorandom walk behaves like a random walk. To have meaningful heuristics one should analyse the algorithm when the function $f(x)$ is randomly chosen from a large set of possible functions.

Note that the rho method is more general than the $p - 1$ method (see Section 12.3), since a random $p \mid N$ is not very likely to be $\sqrt{p}$-smooth.

Theorem 14.9.2. *Let N be composite, not a prime power and not "too smooth". Assume that the Pollard rho walk modulo p behaves like a pseudorandom walk for all $p \mid N$. Then the rho algorithm factors N in $O(N^{1/4}\log(N)^2)$ bit operations.*

Proof: (Sketch) Let p be a prime dividing N such that $p \leq \sqrt{N}$. Define the values l_t and l_h corresponding to the sequence $x_i \pmod p$. If the walk behaves sufficiently like a random walk then, by the birthday paradox, we will have $l_h, l_t \approx \sqrt{\pi p/8}$. Similarly, for some other prime $q \mid N$ one expects that the walk modulo q has different values l_h and l_t. Hence, after $O(\sqrt{p})$ iterations of the loop one expects to split N. □

Bach [21] has given a rigorous analysis of the rho factoring algorithm. He proves that if $0 \leq x, y < N$ are chosen randomly and the iteration is $x_1 = x$, $x_{i+1} = x_i^2 + y$, then the probability of finding the smallest prime factor p of N after k steps is at least $k(k-1)/2p + O(p^{-3/2})$ as p goes to infinity, where the constant in the O depends on k. Bach's method cannot be used to analyse the rho algorithm for discrete logarithms.

Example 14.9.3. Let $N = 144493$. The values (x_i, x_{2i}) for $i = 1, 2, \ldots, 7$ are

$$(2,5), (5,677), (26,9120), (677,81496), (24851,144003), (9120,117992), (90926,94594)$$

and one can check that $\gcd(x_{14} - x_7, N) = 131$.

The reason for this can be seen by considering the values x_i modulo $p = 131$. The sequence of values starts

$$2,\ 5,\ 26,\ 22,\ 92,\ 81,\ 12,\ 14,\ 66,\ 34,\ 109,\ 92$$

and we see that $x_{12} = x_5 = 92$. The tail has length $l_t = 5$ and the head has length $l_h = 7$. Clearly, $x_{14} \equiv x_7 \pmod p$.

Exercise 14.9.4. Factor the number 576229 using the rho algorithm.

Exercise 14.9.5. The rho algorithm usually uses the function $f(x) = x^2 + 1$. Why do you think this function is used? Why are the functions $f(x) = x^2$ and $f(x) = x^2 - 2$ less suitable?

Exercise 14.9.6. Show that if N is known to have a prime factor $p \equiv 1 \pmod m$ for $m > 2$ then it is preferable to use the polynomial $f(x) = x^m + 1$.

Exercise 14.9.7. Floyd's and Brent's cycle finding methods are both useful for the rho factoring algorithm. Explain why one cannot use the other cycle finding methods listed in Section 14.2.2 (Sedgewick-Szymanski-Yao, Schnorr-Lenstra, Nivasch, distinguished points) for the rho factoring method.

14.10 Pollard Kangaroo Factoring

One can also use the kangaroo method to obtain a factoring algorithm. This is a much more direct application of the discrete logarithm algorithm we have already presented. Let $N = pq$ be a product of two n-bit primes. Then $\sqrt{N} < p + q < 3\sqrt{N}$. Let $g \in \mathbb{Z}_N^*$ be chosen at random. Since $g^{\varphi(N)/2} \equiv 1 \pmod N$ we have

$$g^{(N+1)/2} \equiv g^x \pmod N$$

for $x = (p+q)/2$. In other words, we have a discrete logarithm problem in $\mathbb{Z}_N^*$ an interval of width $\sqrt{N}$. Using the standard kangaroo algorithm in the group $\mathbb{Z}_N^*$ one expects to find x (and hence split N) in time $\tilde{O}(N^{1/4})$.

Exercise 14.10.1. The above analysis was for integers N which are a product of two primes of very similar size. Let N now be a general composite integer and let $p \mid N$ be the smallest prime dividing N. Then $p < \sqrt{N}$. Choose $g \in \mathbb{Z}_N^*$ and let $h = g^N \pmod N$. Then $h \equiv g^x \pmod p$ for some $1 \leq x < p$. It is natural to try to use the kangaroo method to find x in time $O(\sqrt{p}\log(N)^2)$. If x were found then $g^{N-x} \equiv 1 \pmod p$ and so one can split N as $\gcd(g^{N-x} - 1 \pmod N, N)$. However, it seems to be impossible to construct an algorithm based on this idea. Explain why.

Chapter 15

Factoring and Discrete Logarithms in Subexponential Time

One of the most powerful tools in mathematics is linear algebra, and much of mathematics is devoted to solving problems by reducing them to it. It is therefore natural to try to solve the integer factorisation and discrete logarithm problems (DLP) in this way. This chapter briefly describes a class of algorithms that exploit a notion called "smoothness", to reduce factoring or DLP to linear algebra. We present such algorithms for integer factorisation, the DLP in the multiplicative group of a finite field, and the DLP in the divisor class group of a curve.

It is beyond the scope of this book to give all the details of these algorithms. Instead, the aim is to sketch the basic ideas. We mainly present algorithms with nice theoretical properties (though often still requiring heuristic assumptions) rather than the algorithms with the best practical performance. We refer to Crandall and Pomerance [162], Shoup [556] and Joux [317] for further reading.

The chapter is arranged as follows. First we present results on smooth integers, and then sketch Dixon's random squares factoring algorithm. Section 15.2.3 then summarises the important features of all algorithms of this type. We then briefly describe a number of algorithms for the discrete logarithm problem in various groups.

15.1 Smooth Integers

Recall from Definition 12.3.1 that an integer is B-smooth if all its prime divisors are at most B. We briefly recall some results on smooth integers; see Granville [267] for a survey of this subject and for further references.

Definition 15.1.1. Let $X, Y \in \mathbb{N}$ be such that $2 \leq Y < X$. Define

$$\Psi(X,Y) = \#\{n \in \mathbb{N} : 1 \leq n \leq X,\ n \text{ is } Y\text{-smooth}\}.$$

It is important for this chapter to have good bounds on $\Psi(X,Y)$. Let $u = \log(X)/\log(Y)$ (as usual log denotes the natural logarithm), so that $u > 1$, $Y = X^{1/u}$ and $X = Y^u$. There is a function $\rho : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ called the **Dickman-de Bruijn function** (for the exact definition of this function see Section 1.4.5 of [162]) such that, for fixed $u > 1$, $\Psi(X, X^{1/u}) \sim X\rho(u)$, where $f(X) \sim g(X)$ means $\lim_{X\to\infty} f(X)/g(X) = 1$. A crude estimate for $\rho(u)$, as $u \to \infty$ is $\rho(u) \approx 1/u^u$. For further details and references see Section 1.4.5 of [162].

The following result of Canfield, Erdös and Pomerance [117] is the main tool in this subject. This is a consequence of Theorem 3.1 (and the corollary on page 15) of [117].

Theorem 15.1.2. *Let $N \in \mathbb{N}$. Let $\epsilon, u \in \mathbb{R}$ be such that $\epsilon > 0$ and $3 \leq u \leq (1-\epsilon)\log(N)/\log(\log(N))$. Then there is a constant c_ϵ (that does not depend on u) such that*

$$\Psi(N, N^{1/u}) = N\exp(-u(\log(u) + \log(\log(u)) - 1 + (\log(\log(u)) - 1)/\log(u) + E(N,u))) \tag{15.1}$$

where $|E(N,u)| \leq c_\epsilon(\log(\log(u))/\log(u))^2$.

Corollary 15.1.3. *Let the notation be as in Theorem 15.1.2. Then $\Psi(N, N^{1/u}) = Nu^{-u+o(u)} = Nu^{-u(1+o(1))}$ uniformly as $u \to \infty$ and $u \leq (1-\epsilon)\log(N)/\log(\log(N))$ (and hence also $N \to \infty$).*

Exercise 15.1.4. Prove Corollary 15.1.3.
[Hint: Show that the expression inside the exp in equation (15.1) is of the form $-u\log(u) + o(u)\log(u)$.]

We will use the following notation throughout the book.

Definition 15.1.5. Let $0 \leq a \leq 1$ and $c \in \mathbb{R}_{>0}$. The **subexponential function** for the parameters a and c is

$$L_N(a,c) = \exp(c\log(N)^a \log(\log(N))^{1-a}).$$

Note that taking $a = 0$ gives $L_N(0,c) = \log(N)^c$ (polynomial) while taking $a = 1$ gives $L_N(1,c) = N^c$ (exponential). Hence $L_N(a,c)$ interpolates exponential and polynomial growth. A complexity $O(L_N(a,c))$ with $0 < a < 1$ is called **subexponential**.

Lemma 15.1.6. *Let $0 < a < 1$ and $0 < c$.*

1. *$L_N(a,c)^m = L_N(a, mc)$ for $m \in \mathbb{R}_{>0}$.*
2. *Let $0 < a_1, a_2 < 1$ and $0 < c_1, c_2$. Then, where the term $o(1)$ is as $N \to \infty$,*

$$L_N(a_1,c_1) \cdot L_N(a_2,c_2) = \begin{cases} L_N(a_1, c_1 + o(1)) & \text{if } a_1 > a_2, \\ L_N(a_1, c_1 + c_2) & \text{if } a_1 = a_2, \\ L_N(a_2, c_2 + o(1)) & \text{if } a_2 > a_1. \end{cases}$$

3.

$$L_N(a_1,c_1) + L_N(a_2,c_2) = \begin{cases} O(L_N(a_1,c_1)) & \text{if } a_1 > a_2, \\ O(L_N(a_1, \max\{c_1,c_2\} + o(1))) & \text{if } a_1 = a_2, \\ O(L_N(a_2,c_2)) & \text{if } a_2 > a_1. \end{cases}$$

4. *Let $0 < b < 1$ and $0 < d$. If $M = L_N(a, c)$ then $L_M(b, d) = L_N(ab, dc^b a^{1-b} + o(1))$ as $N \to \infty$.*
5. *$\log(N)^m = O(L_N(a, c))$ for any $m \in \mathbb{N}$.*
6. *$L_N(a, c)\log(N)^m = O(L_N(a, c + o(1)))$ as $N \to \infty$ for any $m \in \mathbb{N}$. Hence, one can always replace $\tilde{O}(L_N(a, c))$ by $O(L_N(a, c + o(1)))$.*
7. *$\log(N)^m \leq L_N(a, o(1))$ as $N \to \infty$ for any $m \in \mathbb{N}$.*
8. *If $F(N) = O(L_N(a, c))$ then $F(N) = L_N(a, c + o(1))$ as $N \to \infty$.*
9. *$L_N(1/2, c) = N^{c\sqrt{\log(\log(N))/\log(N)}}$.*

Exercise 15.1.7. Prove Lemma 15.1.6.

Corollary 15.1.8. *Let $c > 0$. As $N \to \infty$, the probability that a randomly chosen integer $1 \leq x \leq N$ is $L_N(1/2, c)$-smooth is $L_N(1/2, -1/(2c) + o(1))$.*

Exercise 15.1.9. Prove Corollary 15.1.8 (using Corollary 15.1.3).

Exercise 15.1.10. Let $0 < b < a < 1$. Let $1 \leq x \leq L_N(a, c)$ be a randomly chosen integer. Show that the probability that x is $L_N(b, d)$-smooth is $L_N(a-b, -c(a-b)/d+o(1))$ as $N \to \infty$.

15.2 Factoring using Random Squares

The goal of this section is to present a simple version of Dixon's random squares factoring algorithm. This algorithm is easy to describe and analyse, and already displays many of the important features of the algorithms in this chapter. Note that the algorithm is not used in practice. We give a complexity analysis and sketch how subexponential running times naturally arise. Further details about this algorithm can be found in Section 16.3 of Shoup [556] and Section 19.5 of von zur Gathen and Gerhard [238].

Let $N \in \mathbb{N}$ be an integer to be factored. We assume in this section that N is odd, composite and not a perfect power. As in Chapter 12 we focus on splitting N into a product of two smaller numbers (neither of which is necessarily prime). The key idea is that if one can find congruent squares

$$x^2 \equiv y^2 \pmod{N}$$

such that $x \not\equiv \pm y \pmod{N}$ then one can split N by computing $\gcd(x - y, N)$.

Exercise 15.2.1. Let N be an odd composite integer and m be the number of distinct primes dividing N. Show that the equation $x^2 \equiv 1 \pmod{N}$ has 2^m solutions modulo N.

A general way to find congruent squares is the following.[1] Select a **factor base** $\mathcal{B} = \{p_1, \ldots, p_s\}$ consisting of the primes $\leq B$ for some $B \in \mathbb{N}$. Choose uniformly at random an integer $1 \leq x < N$, compute $a = x^2 \pmod{N}$ reduced to the range $1 \leq a < N$ and try to factor a as a product in $\mathcal{B}$ (e.g., using trial division).[2] If a is B-smooth then this succeeds, in which case we have a **relation**

$$x^2 \equiv \prod_{i=1}^{s} p_i^{e_i} \pmod{N}. \tag{15.2}$$

[1] This idea goes back to Kraitchik in the 1920s; see [489] for some history.

[2] To obtain non-trivial relations one should restrict to integers in the range $\sqrt{N} < x < N - \sqrt{N}$. But it turns out to be simpler to analyse the algorithm for the case $1 \leq x < N$. Note that the probability that a randomly chosen integer $1 \leq x < N$ satisfies $1 \leq x < \sqrt{N}$ is negligible.

The values x for which a relation is found are stored as $x_1, x_2, \ldots, x_t$. The corresponding exponent vectors $\underline{e}_j = (e_{j,1}, \ldots, e_{j,s})$ for $1 \leq j \leq t$ are also stored. When enough relations have been found we can use linear algebra modulo 2 to obtain congruent squares. More precisely, compute $\lambda_j \in \{0, 1\}$ such that not all $\lambda_j = 0$ and

$$\sum_{j=1}^{t} \lambda_j \underline{e}_j \equiv (0, 0, \ldots, 0) \pmod 2.$$

Equivalently, this is an integer linear combination

$$\sum_{j=1}^{t} \lambda_j \underline{e}_j = (2f_1, \ldots, 2f_s) \tag{15.3}$$

with not all the f_i equal to zero. Let

$$X \equiv \prod_{j=1}^{t} x_j^{\lambda_j} \pmod N, \qquad Y \equiv \prod_{i=1}^{s} p_i^{f_i} \pmod N. \tag{15.4}$$

One then has $X^2 \equiv Y^2 \pmod N$ and one can hope to split N by computing $\gcd(X - Y, N)$ (note that this gcd could be 1 or N, in which case the algorithm has failed). We present the above method as Algorithm 22.

Algorithm 22 Random squares factoring algorithm

INPUT: $N \in \mathbb{N}$
OUTPUT: Factor of N

1: Select a suitable $B \in \mathbb{N}$ and construct the **factor base** $\mathcal{B} = \{p_1, \ldots, p_s\}$ consisting of all primes $\leq B$
2: **repeat**
3: Choose an integer $1 \leq x < N$ uniformly at random and compute $a = x^2 \pmod N$ reduced to the range $1 \leq a < N$
4: Try to factor a as a product in $\mathcal{B}$ (e.g., using trial division)
5: **if** a is B-smooth **then**
6: store the value x and the exponent row vector $\underline{e} = (e_1, \ldots, e_s)$ as in equation (15.2) in a matrix
7: **end if**
8: **until** there are $s + 1$ rows in the matrix
9: Perform linear algebra over $\mathbb{F}_2$ to find a non-trivial linear dependence among the vectors $\underline{e}_j$ modulo 2
10: Define X and Y as in equation (15.4)
11: **return** $\gcd(X - Y, N)$

We emphasise that the random squares algorithm has two distinct stages. The first stage is to generate enough relations. The second stage is to perform linear algebra. The first stage can easily be distributed or parallelised, while the second stage is hard to parallelise.

Example 15.2.2. Let $N = 19 \cdot 29 = 551$ and let $\mathcal{B} = \{2, 3, 5\}$. One finds the following congruences (in general 4 relations would be required, but we are lucky in this case)

$$\begin{aligned} 34^2 &\equiv 2 \cdot 3^3 \pmod N \\ 52^2 &\equiv 2^2 \cdot 5^3 \pmod N \\ 55^2 &\equiv 2 \cdot 3^3 \cdot 5 \pmod N. \end{aligned}$$

These relations are stored as the matrix

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix}.$$

The sum of the three rows is the vector

$$(4,\ 6,\ 4)\,.$$

Let

$$X = 264 \equiv 34 \cdot 52 \cdot 55 \pmod{551} \text{ and } Y = 496 \equiv 2^2 \cdot 3^3 \cdot 5^2 \pmod{551}.$$

It follows that

$$X^2 \equiv Y^2 \pmod{N}$$

and $\gcd(X - Y, N) = 29$ splits N.

Exercise 15.2.3. Factor $N = 3869$ using the above method and factor base $\{2, 3, 5, 7\}$.

15.2.1 Complexity of the Random Squares Algorithm

There are a number of issues to deal with when analysing this algorithm. The main problem is to decide how many primes to include in the factor base. The prime number theorem implies that $s = \#\mathcal{B} \approx B/\log(B)$. If we make B larger then the chances of finding a B-smooth number increase, but on the other hand, we need more relations and the linear algebra takes longer. We will determine an optimal value for B later. First we must write down an estimate for the running time of the algorithm, as a function of s. Already this leads to various issues:

- What is the probability that a random value $x^2 \pmod{N}$ factors over the factor base $\mathcal{B}$?
- How many relations do we require until we can be sure there is a non-trivial vector $\underline{e}$?
- What are the chances that computing $\gcd(X - Y, N)$ splits N?

We deal with the latter two points first. It is immediate that $s+1$ relations are sufficient for line 9 of Algorithm 22 to succeed. The question is whether $1 < \gcd(X - Y, N) < N$ for the corresponding integers X and Y. There are several ways the algorithm can fail to split N. For example, it is possible that a relation in equation (15.2) is such that all e_i are even and $x \equiv \pm \prod_i p_i^{e_i/2} \pmod{N}$. One way that such relations could arise is from $1 \leq x < \sqrt{N}$ or $N - \sqrt{N} < x < N$; this situation occurs with negligible probability. If $\sqrt{N} < x < N - \sqrt{N}$ and $a = Y^2$ is a square in $\mathbb{N}$ then $1 \leq Y < \sqrt{N}$ and so $x \not\equiv \pm Y \pmod{N}$ and the relation is useful. The following result shows that all these (and other) bad cases occur with probability at most $1/2$.

Lemma 15.2.4. *The probability to split N using X and Y is at least $\frac{1}{2}$.*

Proof: Let X and Y be the integers computed in line 10 of Algorithm 22. We treat Y as fixed, and consider the probability distribution for X. By Exercise 15.2.1, the number of solutions Z to $Z^2 \equiv Y^2 \pmod{N}$ is 2^m where $m \geq 2$ is the number of distinct primes dividing N. The two solutions $Z = \pm Y$ are useless but the other $2^m - 2$ solutions will all split N.

Since the values for x are chosen uniformly at random it follows that X is a randomly chosen solution to the equation $X^2 \equiv Y^2 \pmod{N}$. It follows that the probability to split N is $(2^m - 2)/2^m \geq 1/2$. □

Exercise 15.2.5. Show that if one takes $s+l$ relations where $l \geq 2$ then the probability of splitting N is at least $1 - 1/2^l$.

We now consider the probability of smoothness. We first assume the probability that $x^2 \pmod N$ is smooth is the same as the probability that a random integer modulo N is smooth.[3]

Lemma 15.2.6. *Let the notation be as above. Let T_B be the expected number of trials until a randomly chosen integer modulo N is B-smooth. Assuming that squares modulo N are as likely to be smooth as random integers of the same size, Algorithm 22 has expected running time at most*

$$c_1 \#\mathcal{B}^2 T_B M(\log(N)) + c_2 (\#\mathcal{B})^3$$

bit operations for some constants c_1, c_2 (where $M(n)$ is the cost of multiplying two n-bit integers).

Proof: Suppose we compute the factorisation of $x^2 \pmod N$ over $\mathcal{B}$ by trial division. This requires $O(\#\mathcal{B} M(\log(N)))$ bit operations for each value of x. We need $(\#\mathcal{B}+1)$ relations to have a soluble linear algebra problem. As said above, the expected number of trials of x to get a B-smooth value of $x^2 \pmod N$ is T_B. Hence the cost of finding the relations is $O((\#\mathcal{B}+1) T_B (\#\mathcal{B}) M(\log(N)))$, which gives the first term.

The linear algebra problem can be solved using Gaussian elimination (we are ignoring that the matrix is sparse) over $\mathbb{F}_2$, which takes $O((\#\mathcal{B})^3)$ bit operations. This gives the second term. □

It remains to choose B as a function of N to minimise the running time. By the discussion in Section 15.1, it is natural to approximate T_B by u^u where $u = \log(N)/\log(B)$. We now explain how subexponential functions naturally arise in such algorithms. Since increasing B makes the linear algebra slower, but makes relations more likely (i.e., lowers T_B), a natural approach to selecting B is to try to equate both terms of the running time in Lemma 15.2.6. This leads to $u^u = \#\mathcal{B}$. Putting $u = \log(N)/\log(B)$, $\#\mathcal{B} = B/\log(B)$, taking logs, and ignoring $\log(\log(B))$ terms, gives

$$\log(N)\log(\log(N))/\log(B) \approx \log(B).$$

This implies $\log(B)^2 \approx \log(N)\log(\log(N))$ and so $B \approx L_N(1/2, 1)$. The overall complexity for this choice of B would be $L_N(1/2, 3+o(1))$ bit operations.

A more careful argument is to set $B = L_N(1/2, c)$ and use Corollary 15.1.3. It follows that $T_B = L_N(1/2, 1/(2c) + o(1))$ as $N \to \infty$. Putting this into the equation of Lemma 15.2.6 gives complexity $L_N(1/2, 2c + 1/(2c) + o(1)) + L_N(1/2, 3c)$ bit operations. The function $x + 1/x$ is minimised at $x = 1$, hence we should take $c = 1/2$.

Theorem 15.2.7. *Let the notation be as above. Under the same assumptions as Lemma 15.2.6 then Algorithm 22 has complexity*

$$L_N(1/2, 2 + o(1))$$

bit operations as $N \to \infty$.

[3] Section 16.3 of Shoup [556] gives a modification of the random squares algorithm for which one can avoid this assumption. The trick is to note that at least one of the cosets of $(\mathbb{Z}/N\mathbb{Z})^*/((\mathbb{Z}/N\mathbb{Z})^*)^2$ has at least as great a proportion of smooth numbers as random integers up to N (Shoup credits Rackoff for this trick). The idea is to work in one of these cosets by choosing at random some $1 < \delta < N$ and considering relations coming from smooth values of $\delta x^2 \pmod N$.

Proof: Put $B = L_N(1/2, 1/2)$ into Lemma 15.2.6. □

We remark that, unlike the Pollard rho or Pollard $p-1$ methods, this factoring algorithm has essentially no dependence on the factors of N. In other words, its running time is essentially the same for all integers of a given size. This makes it particularly suitable for factoring $N = pq$ where p and q are primes of the same size.

15.2.2 The Quadratic Sieve

To improve the result of the previous section it is necessary to reduce the cost of the linear algebra and to reduce the cost of decomposing smooth elements as products of primes. We sketch the **quadratic sieve** algorithm of Pomerance. We do not have space to present all the details of this algorithm (interested readers should see Section 6.1 of [162] or Section 16.4.2 of [556]).

A crucial idea, which seems to have first appeared in the work of Schroeppel[4], is **sieving**. The point is to consider a range of values of x and simultaneously determine the decompositions of $x^2 \pmod N$ over the factor base. It is possible to do this so that the cost of each individual decomposition is only $O(\log(B))$ bit operations.

Another crucial observation is that the relation matrix is sparse, in other words, rows of the matrix have rather few non-zero entries. In such a case, the cost of linear algebra can be reduced from $O((\#\mathcal{B})^3)$ bit operations to $O((\#\mathcal{B})^{2+o(1)})$ bit operations (as $\#\mathcal{B} \to \infty$). The best methods are due to Lanczos or Wiedemann; see Section 6.1.3 of Crandall and Pomerance [162] or Section 3.4 of Joux [317] for references and discussion.

A further trick is to choose $x = \lfloor \sqrt{N} \rfloor + i$ where $i = 0, 1, -1, 2, -2, \ldots$. The idea is that if $x = \sqrt{N} + \epsilon$ then either $x^2 - N$ or $N - x^2$ is a positive integer of size $2\sqrt{N}|\epsilon|$. Since these integers are much smaller than N they have a much better chance of being smooth than the integers $x^2 \pmod N$ in the random squares algorithm. To allow for the case of $\epsilon < 0$ we need to add -1 to our factor base and use the fact that a factorisation $N - x^2 = \prod_{i=1}^{s} p_i^{e_i}$ corresponds to a relation $x^2 \equiv (-1)\prod_{i=1}^{s} p_i^{e_i} \pmod N$.

Since we are now only considering values x of the form $\sqrt{N} + \epsilon$ where $|\epsilon|$ is small it is necessary to assume the probability that $x^2 - N$ or $N - x^2$ (as appropriate) is B-smooth is that same as the probability that a randomly chosen integer of that size is B-smooth. This is a rather strong assumption (though it is supported by numerical evidence) and so the running time estimates of the quadratic sieve are only heuristic.

The heuristic complexity of the quadratic sieve is determined in Exercise 15.2.8. Note that, since we will need to test $L_N(1/2, 1 + o(1))$ values (here $o(1)$ is as $N \to \infty$) for smoothness, we have $|\epsilon| = L_N(1/2, 1 + o(1))$. It follows that the integers being tested for smoothness have size $\sqrt{N}L_N(1/2, 1 + o(1)) = N^{1/2+o(1)}$.

Exercise 15.2.8. ★ Let T_B be the expected number of trials until an integer of size $2\sqrt{N}L_N(1/2, 1)$ is B-smooth. Show that the running time of the quadratic sieve is at most

$$c_1 \#\mathcal{B} T_B \log(B) M(\log(N)) + c_2 \#\mathcal{B}^{2+o(1)}$$

bit operations for some constants c_1, c_2 as $N \to \infty$.

Let $B = L_N(1/2, 1/2)$. Show that the natural heuristic assumption (based on Corollary 15.1.8) is that $T_B = L_N(1/2, 1/2 + o(1))$. Hence, show that the heuristic complexity of the quadratic sieve is $L_N(1/2, 1 + o(1))$ bit operations as $N \to \infty$.

Example 15.2.9. Let $N = 2041$ so that $\lfloor \sqrt{N} \rfloor = 45$.

Let $\mathcal{B} = \{-1, 2, 3, 5\}$. Taking $x = 43, 44, 45, 46$ one finds the following factorisations of $x^2 - N$:

[4] See [371, 489] for some remarks on the history of integer factoring algorithms.

x	$x^2 \pmod N$	$\underline{e}$
43	$-2^6 \cdot 3$	(1, 6, 1, 0)
44	Not 5-smooth	
45	-2^4	(1, 4, 0, 0)
46	$3 \cdot 5^2$	(0, 0, 1, 2)

Taking $\underline{e} = \underline{e}_1 + \underline{e}_2 + \underline{e}_3 = (2, 10, 2, 2)$ gives all coefficients even. Putting everything together, we set $X = 43 \cdot 45 \cdot 46 \equiv 1247 \pmod N$ and $Y = -1 \cdot 2^5 \cdot 3 \cdot 5 \equiv 1561 \pmod N$. One can check that $X^2 \equiv Y^2 \pmod N$ and that $\gcd(X - Y, N) = 157$.

Exercise 15.2.10. Show that in the quadratic sieve one can also use values $x = \lfloor \sqrt{kN} \rfloor + i$ where $k \in \mathbb{N}$ is very small and $i = 0, 1, -1, 2, -2, \ldots$.

Exercise 15.2.11. Show that using sieving and fast linear algebra, but not restricting to values $\pm x^2 \pmod N$ of size $N^{1/2+o(1)}$ gives an algorithm with heuristic expected running time of $L_N(1/2, \sqrt{2} + o(1))$ bit operations as $N \to \infty$.

Exercise 15.2.12. A subexponential algorithm is asymptotically much faster than a $\tilde{O}(N^{1/4})$ algorithm. Verify that if $N = 2^{1024}$ then $N^{1/4} = 2^{256}$ while $L_N(1/2, 2) \approx 2^{197}$ and $L_N(1/2, 1) \approx 2^{98.5}$.

The best proven asymptotic complexity for factoring integers N is $L_N(1/2, 1 + o(1))$ bit operations. This result is due to Pomerance and Lenstra [381].

15.2.3 Summary

We briefly highlight the key ideas in the algorithms of this section. The crucial concept of smooth elements of the group $(\mathbb{Z}/N\mathbb{Z})^*$ arises from considering an integer modulo N as an element of $\mathbb{Z}$. The three essential properties of smooth numbers that were used in the algorithm are:

1. One can efficiently decompose an element of the group as a product of smooth elements, or determine that the element is not smooth.
2. The probability that a random element is smooth is sufficiently high.
3. There is a way to apply linear algebra to the relations obtained from smooth elements to solve the computational problem.

We will see analogues of these properties in the algorithms below.

There are other general techniques that can be applied in most algorithms of this type. For example, the linear algebra problems are usually sparse and so the matrices and algorithms should be customised for this. Another general concept is "large prime variation" which, in a nutshell, is to also store "nearly smooth" relations (i.e., elements that are the product of a smooth element with one or two prime elements that are not too large) and perform some elimination of these "large primes" before doing the main linear algebra stage (this is similar to, but more efficient than, taking a larger factor base). Finally we remark that the first stage of these algorithms (i.e., collecting relations) can always be distributed or parallelised.

15.3 Elliptic Curve Method Revisited

We assume throughout this section that $N \in \mathbb{N}$ is an integer to be factored and that N is odd, composite, and not a perfect power. We denote by p the smallest prime factor of N.

The elliptic curve method (ECM) works well in practice but, as with the Pollard $p-1$ method, its complexity depends on the size of the smallest prime dividing N. It is not a polynomial-time algorithm because, for any constant $c > 0$ and over all N and $p \mid N$, a randomly chosen elliptic curve over $\mathbb{F}_p$ is not likely to have $O(\log(N)^c)$-smooth order. As we have seen, the theorem of Canfield, Erdös and Pomerance [117] says it is more reasonable to hope that integers have a subexponential probability of being subexponentially smooth. Hence, one might hope that the elliptic curve method has subexponential complexity. Indeed, Lenstra [377] makes the following conjecture (which is essentially that the Canfield-Erdös-Pomerance result holds in small intervals).

Conjecture 15.3.1. *(Lenstra [377], page 670) The probability that an integer, chosen uniformly at random in the range $(X - \sqrt{X}, X + \sqrt{X})$, is $L_X(1/2, c)$-smooth is $L_X(1/2, -1/(2c) + o(1))$ as X tends to infinity.*[5]

One can phrase Conjecture 15.3.1 as saying that, if p_s is the probability that a random integer between 1 and X is Y-smooth, then $\Psi(X + 2\sqrt{X}, Y) - \Psi(X, Y) \approx 2\sqrt{X}p_s$. More generally, one would like to know that, for sufficiently large[6] X, Y and Z,

$$\Psi(X + Z, Y) - \Psi(X, Y) \sim Z\Psi(X, Y)/X \tag{15.5}$$

or, in other words, that integers in a short interval at X are about as likely to be Y-smooth as integers in a large interval at X.

We now briefly summarise some results in this area; see Granville [267] for details and references. Harman (improved by Lenstra, Pila and Pomerance [380]) showed, for any fixed $\beta > 1/2$ and $X \geq Y \geq \exp(\log(X)^{2/3+o(1)})$, where the $o(1)$ is as $X \to \infty$, that

$$\Psi(X + X^\beta, Y) - \Psi(X, Y) > 0.$$

Obtaining results for the required value $\beta = 1/2$ seems to be hard and the experts refer to the "$\sqrt{X}$ barrier" for smooth integers in short intervals. It is known that this barrier can be broken most of the time: Hildebrand and Tenenbaum showed that, for any $\epsilon > 0$, equation (15.5) holds when $X \geq Y \geq \exp(\log(X)^{5/6+\epsilon})$ and $Y \exp(\log(X)^{1/6}) \leq Z \leq X$ for all but at most $M/\exp(\log(M)^{1/6-\epsilon})$ integers $1 \leq X \leq M$. As a special case, this result shows that, for almost all primes p, the interval $[p-\sqrt{p}, p+\sqrt{p}]$ contains a Y-smooth integer where $Y = \exp(\log(X)^{5/6+\epsilon})$ (i.e., subexponential smoothness).

Using Conjecture 15.3.1 one obtains the following complexity for the elliptic curve method (we stress that the complexity is in terms of the smallest prime factor p of N, rather than N itself).

Theorem 15.3.2. *(Conjecture 2.10 of [377]) Assume Conjecture 15.3.1. One can find the smallest factor p of an integer N in $L_p(1/2, \sqrt{2} + o(1))M(\log(N))$ bit operations as $p \to \infty$.*

Proof: Guess the size of p and choose $B = L_p(1/2, 1/\sqrt{2})$ (since the size of p is not known one actually runs the algorithm repeatedly for slowly increasing values of B). Then each run of Algorithm 12 requires $O(B \log(B)M(\log(N))) = L_p(1/2, 1/\sqrt{2} + o(1))M(\log(N))$ bit operations. By Conjecture 15.3.1 one needs to repeat the process $L_p(1/2, 1/\sqrt{2}+o(1))$ times. The result follows. □

[5] Lenstra considers the sub-interval $(X-\sqrt{X}, X+\sqrt{X})$ of the Hasse interval $[X+1-2\sqrt{X}, X+1+2\sqrt{X}]$ because the distribution of isomorphism classes of randomly chosen elliptic curves is relatively close to uniform when restricted to those whose group order lies in this sub-interval. In contrast, elliptic curves whose group orders are near the edge of the Hasse interval arise with lower probability.

[6] The notation $\sim$ means taking a limit as $X \to \infty$, so it is necessary that Y and Z grow in a controlled way as X does.

Exercise 15.3.3. Let $N = pq$ where p is prime and $p < \sqrt{N} < 2p$. Show that $L_p(1/2, \sqrt{2} + o(1)) = L_N(1/2, 1 + o(1))$. Hence, in the worst case, the complexity of ECM is the same as the complexity of the quadratic sieve.

For further details on the elliptic curve method we refer to Section 7.4 of [162]. We remark that Lenstra, Pila and Pomerance [380] have considered a variant of the elliptic curve method using divisor class groups of hyperelliptic curves of genus 2. The Hasse-Weil interval for such curves contains an interval of the form $(X, X + X^{3/4})$ and Theorem 1.3 of [380] proves that such intervals contain $L_X(2/3, c_1)$-smooth integers (for some constant c_1) with probability $1/L_X(1/3, 1)$. It follows that there is a rigorous factoring algorithm with complexity $L_p(2/3, c)$ bit operations for some constant c_2. This algorithm is not used in practice, as the elliptic curve method works fine already.

Exercise 15.3.4. Suppose a sequence of values $1 < x < N$ are chosen uniformly at random. Show that one can find such a value that is $L_N(2/3, c)$-smooth, together with its factorisation, in expected $L_N(1/3, c' + o(1))$ bit operations for some constant c'.

Remark 15.3.5. It is tempting to conjecture that the Hasse interval contains a polynomially-smooth integer (indeed, this has been done by Maurer and Wolf [407]; see equation (21.9)). This is not relevant for the elliptic curve factoring method, since such integers would be very rare. Suppose the probability that an integer of size X is Y-smooth is exactly $1/u^u$, where $u = \log(X)/\log(Y)$ (by Theorem 15.1.2, this is reasonable as long as $Y^{1-\epsilon} \geq \log(X)$). It is natural to suppose that the interval $[X - 2\sqrt{X}, X + 2\sqrt{X}]$ is likely to contain a Y-smooth integer if $4\sqrt{X} > u^u$. Let $Y = \log(X)^c$. Taking logs of both sides of the inequality gives the condition

$$\log(4) + \tfrac{1}{2}\log(X) > \frac{\log(X)}{c\log(\log(X))}(\log(\log(X)) - \log(c\log(\log(X)))).$$

It is therefore natural to conclude that when $c \geq 2$ there is a good chance that the Hasse interval of an elliptic curve over $\mathbb{F}_p$ contains a $\log(p)^c$-smooth integer. Proving such a claim seems to be far beyond the reach of current techniques.

15.4 The Number Field Sieve

The most important integer factorisation algorithm for large integers is the **number field sieve** (NFS). A special case of this method was invented by Pollard.[7] The algorithm requires algebraic number theory and a complete discussion of it is beyond the scope of this book. Instead, we just sketch some of the basic ideas. For full details we refer to Lenstra and Lenstra [372], Section 6.2 of Crandall and Pomerance [162], Section 10.5 of Cohen [136] or Stevenhagen [584].

As we have seen from the quadratic sieve, reducing the size of the values being tested for smoothness yields a better algorithm. Indeed, in the quadratic sieve the numbers were reduced from size $O(N)$ to $O(N^{1/2+o(1)})$ and, as shown by Exercise 15.2.11, this trick alone lowers the complexity from $O(L_N(1/2, \sqrt{2} + o(1)))$ to $O(L_N(1/2, 1 + o(1)))$. To break the "$O(L_N(1/2, c))$ barrier" one must make the numbers being tested for smoothness dramatically smaller. A key observation is that if the numbers are of size $O(L_N(2/3, c'))$ then they are $O(L_N(1/3, c''))$ smooth, for some constants c' and c'', with probability approximately $1/u^u = 1/L_N(1/3, c'/(3c'') + o(1))$. Hence, one can expect an algorithm

[7] The goal of Pollard's method was to factor integers of the form $n^3 + k$ where k is small. The the algorithm in the case of numbers of a special form is known as the **special number field sieve**.

with running time $O(L_N(1/3, c+o(1)))$ bit operations, for some constant c, by considering smaller values for smoothness.

It seems to be impossible to directly choose values x such that $x^2 \pmod N$ is of size $L_N(2/3, c + o(1))$ for some constant c. Hence, the number field sieve relies on two factor bases $\mathcal{B}_1$ and $\mathcal{B}_2$. Using smooth elements over $\mathcal{B}_1$ (respectively, $\mathcal{B}_2$) and linear algebra one finds an integer square u^2 and an algebraic integer square v^2. The construction allows us to associate an integer w modulo N to v such that $u^2 \equiv w^2 \pmod N$ and hence one can try to split N.

We briefly outline the ideas behind the algorithm. First, choose a monic irreducible polynomial $P(x) \in \mathbb{Z}[x]$ of degree d (where d grows like $\lfloor (3\log(N)/\log(\log(N)))^{1/3} \rfloor$) with a root $m = \lfloor N^{1/d} \rfloor$ modulo N (i.e., $P(m) \equiv 0 \pmod N$). Factor base $\mathcal{B}_1$ is primes up to $B = L_N(1/3, c)$ and factor base $\mathcal{B}_2$ is small prime ideals in the ring $\mathbb{Z}[\theta]$ in the number field $K = \mathbb{Q}(\theta) = \mathbb{Q}[x]/(P(x))$ (i.e., θ is a generic root of $P(x)$). The algorithm exploits, in the final step, the ring homomorphism $\phi : \mathbb{Z}[x]/(P(x)) \rightarrow \mathbb{Z}/N\mathbb{Z}$ given by $\phi(\theta) = m \pmod N$. Suppose the ideal $(a - b\theta)$ is a product of prime ideals in $\mathcal{B}_2$ (one factors the ideal $(a - b\theta)$ by factoring its norm in $\mathbb{Z}$), say

$$(a - b\theta) = \prod_{i=1}^{r} \wp_i^{e_i}.$$

Suppose also that $a - bm$ is a smooth integer in $\mathcal{B}_1$, say

$$a - bm = \prod_{j=1}^{s} p_j^{f_j}.$$

If these equations hold then we call $(a - b\theta)$ and $a - bm$ smooth and store a, b and the sequences of e_i and f_j. We do not call this a "relation" as there is no direct relationship between the prime ideals $\wp_i$ and the primes p_j. Indeed, the $\wp_j$ are typically non-principal ideals and do not necessarily contain an element of small norm. Hence, the two products are modelled as being "independent".

It is important to estimate the probability that both the ideal $(a-b\theta)$ and the integer $a-bm$ are smooth. One shows that taking integers $|a|, |b| \leq L_N(1/3, c'+o(1))$ for a suitable constant c' gives $(a-b\theta)$ of norm $L_N(2/3, c''+o(1))$ and $a-bm$ of size $L_N(2/3, c'''+o(1))$ for certain constants c'' and c'''. To obtain a fast algorithm one uses sieving to determine within a range of values for a and b the pairs (a, b) such that both $a - bm$ and $(a - b\theta)$ factor over the appropriate factor base.

Performing linear algebra on both sides gives a set S of pairs (a, b) such that (ignoring issues with units and non-principal ideals)

$$\begin{aligned} \prod_{(a,b)\in S} (a - bm) &= u^2 \\ \prod_{(a,b)\in S} (a - b\theta) &= v^2 \end{aligned}$$

for some $u \in \mathbb{Z}$ and $v \in \mathbb{Z}[\theta]$. Finally we can "link" the two factor bases: Applying the ring homomorphism $\phi : \mathbb{Z}[\theta] \rightarrow \mathbb{Z}$ gives $u^2 \equiv \phi(v)^2 \pmod N$ and hence we have a chance to split N. A non-trivial task is computing the actual numbers u and $\phi(v)$ modulo N so that one can compute $\gcd(u - \phi(v), N)$.

Since one is only considering integers $a-bm$ in a certain range (and ideals in a certain range) for smoothness one relies on heuristic assumptions about the smoothness probability. The conjectural complexity of the number field sieve is $O(L_N(1/3, c + o(1)))$

bit operations as $N \to \infty$ where $c = (64/9)^{1/3} \approx 1.923$. Note, comparing with Exercise 15.2.12, that if $N \approx 2^{1024}$ then $L_N(1/3, 1.923) \approx 2^{87}$.

15.5 Index Calculus in Finite Fields

We now explain how similar ideas to the above have been used to find subexponential algorithms for the discrete logarithm problem in finite fields. The original idea is due to Kraitchik [354]. While all subexponential algorithms for the DLP share certain basic concepts, the specific details vary quite widely (in particular, precisely what "linear algebra" is required). We present in this section an algorithm that is very convenient when working in subgroups of prime order r in $\mathbb{F}_q^*$ as it relies only on linear algebra over the field $\mathbb{F}_r$.

Let $g \in \mathbb{F}_q^*$ have prime order r and let $h \in \langle g \rangle$. The starting point is the observation that if one can find integers $0 < Z_1, Z_2 < r$ such that

$$g^{Z_1} h^{Z_2} = 1 \tag{15.6}$$

in $\mathbb{F}_q^*$ then $\log_g(h) = -Z_1 Z_2^{-1} \pmod{r}$. The idea will be to find such a relation using a factor base and linear algebra. Such algorithms go under the general name of **index calculus** algorithms; the reason for this is that **index** is another word for discrete logarithm, and the construction of a solution to equation (15.6) is done by calculations using indices.

15.5.1 Rigorous Subexponential Discrete Logarithms Modulo p

We now sketch a subexponential algorithm for the discrete logarithm problem in $\mathbb{F}_p^*$. It is closely related to the random squares algorithm of Section 15.2. Let $g \in \mathbb{F}_p^*$ have order r (we will assume r is prime, but the general case is not significantly different) and let $h \in \mathbb{F}_p^*$ be such that $h \in \langle g \rangle$. We will also assume, for simplicity, that $r^2 \nmid (p-1)$ (we show in Exercise 15.5.8 that this condition can be avoided).

The natural idea is to choose the factor base $\mathcal{B}$ to be the primes in $\mathbb{Z}$ up to B. We let $s = \#\mathcal{B}$. One can take random powers $g^z \pmod{p}$ and try to factor over $\mathcal{B}$. One issue is that the values g^z only lie in a subgroup of $\mathbb{F}_p^*$ and so a strong smoothness heuristic would be required. To get a rigorous algorithm (under the assumption that $r^2 \nmid (p-1)$) write G' for the subgroup of $\mathbb{F}_p^*$ of order $(p-1)/r$, choose a random $\delta \in G'$ at each iteration and try to factor $g^z \delta \pmod{p}$; this is now a uniformly distributed element of $\mathbb{F}_p^*$ and so Corollary 15.1.8 can be applied. We remark that the primes p_i themselves do not necessarily lie in the subgroup $\langle g \rangle$.

Exercise 15.5.1. Let $r \mid (p-1)$ be a prime such that $r^2 \nmid (p-1)$. Let $g \in \mathbb{F}_p^*$ have order dividing r and denote by $G' \subseteq \mathbb{F}_p^*$ the subgroup of order $(p-1)/r$. Show that $\langle g \rangle \cap G' = \{1\}$.

Exercise 15.5.2. Give two ways to sample randomly from G'. When would each be used?
[Hint: see Section 11.4.]

The algorithm proceeds by choosing random values $1 \leq z < r$ and random $\delta \in G'$ and testing $g^z \delta \pmod{p}$ for smoothness. The i-th relation is

$$g^{z_i} \delta_i \equiv \prod_{j=1}^{s} p_j^{e_{i,j}} \pmod{p}. \tag{15.7}$$

The values z_i are stored in a vector and the values $\underline{e}_i = (e_{i,1}, \ldots, e_{i,s})$ are stored as a row in a matrix. We need s relations of this form. We also need at least one relation involving h (alternatively, we could have used a power of h in every relation in equation (15.7)) so try random values z_{s+1} and $\delta_{s+1} \in G'$ until $g^{z_{s+1}} h \delta_{s+1} \pmod p$ is B-smooth. One performs linear algebra modulo r to find integers $0 \leq \lambda_1, \ldots, \lambda_{s+1} < r$ such that

$$\sum_{i=1}^{s+1} \lambda_i \underline{e}_i = (rf_1, \ldots, rf_s) \equiv (0, \ldots, 0) \pmod r$$

where $f_1, \ldots, f_s \in \mathbb{Z}_{\geq 0}$. In matrix notation, writing $A = (e_{i,j})$, this is $(\lambda_1, \ldots, \lambda_{s+1})A \equiv (0, \ldots, 0) \pmod r$. In other words, the linear algebra problem is finding a non-trivial element in the kernel of the matrix A modulo r. Let $Z_1 = \sum_{i=1}^{s+1} \lambda_i z_i \pmod r$ and $Z_2 = \lambda_{s+1}$. Then

$$g^{Z_1} h^{Z_2} \left(\prod_i \delta_i^{\lambda_i} \right) \equiv \left(\prod_i p_i^{f_i} \right)^r \pmod p. \tag{15.8}$$

Since $g^{Z_1} h^{Z_2} \in \langle g \rangle$ and the other terms are all in G' it follows from Exercise 15.5.1 that $g^{Z_1} h^{Z_2} \equiv 1 \pmod r$ as required. We stress that it is not necessary to compute $\prod_i \delta_i^{\lambda_i}$ or the right hand side of equation (15.8).

The algorithm succeeds as long as $\lambda_{s+1} \not\equiv 0 \pmod r$ (and if $\lambda_{s+1} = 0$ then there is a linear dependence from the earlier relations, which can be removed by deleting one or more rows of the relation matrix).

Exercise 15.5.3. Show that if one replaces equation (15.7) by $g^{z_{1,i}} h^{z_{2,i}} \delta_i$ for random $z_{1,i}, z_{2,i}$ and δ_i then one obtains an algorithm that succeeds with probability $1 - 1/r$.

Example 15.5.4. Let $p = 223$. Then $g = 15$ has prime order $r = 37$. Suppose $h = 68$ is the instance of the DLP we want to solve. Let $\mathcal{B} = \{2, 3, 5, 7\}$. Choose the element $g_1 = 184$ of order $(p-1)/r = 6$. One can check that we have the following relations.

z	i	Factorization of $g^z g_1^i \pmod p$
1	1	$2^2 \cdot 3 \cdot 7$
33	0	$2^3 \cdot 7$
8	1	$3^2 \cdot 5$
7	0	$2^3 \cdot 3 \cdot 5$

One also finds the relation $hg^7 g_1^2 = 2^3 \cdot 3^2$.

We represent the relations as the vector and matrix

$$\underline{z} = \begin{pmatrix} 1 \\ 33 \\ 8 \\ 7 \\ 7 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 1 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 3 & 1 & 1 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix}.$$

Now perform linear algebra modulo 37. One finds the non-trivial kernel vector $\underline{v} = (1, 36, 20, 17, 8)$. Computing $Z_1 = \underline{v} \cdot \underline{z} = 7 \pmod{37}$ and $Z_2 = 8$ we find $g^{Z_1} h^{Z_2} \equiv 1 \pmod{223}$ and so the solution is $-Z_1 Z_2^{-1} \equiv 13 \pmod{37}$.

Exercise 15.5.5. Write the above algorithm in pseudocode (using trial division to determine the smooth relations).

Exercise 15.5.6. Let the notation be as above. Let T_B be the expected number of trials of random integers modulo p until one is B-smooth. Show that the expected running time of this algorithm (using naive trial division for the relations and using the Lanczos or Wiedemann methods for the linear algebra) is

$$O((\#\mathcal{B})^2 T_B M(\log(p)) + (\#\mathcal{B})^{2+o(1)} M(\log(r)))$$

bit operations as $p \to \infty$

Exercise 15.5.7. Show that taking $B = L_p(1/2, 1/2)$ is the optimal value to minimise the complexity of the above algorithm, giving a complexity of $O(L_p(1/2, 2 + o(1)))$ bit operations for the discrete logarithm problem in $\mathbb{F}_p^*$ as $p \to \infty$. (Note that, unlike many of the results in this chapter, this result does not rely on any heuristics.)

We remark that, in practice, rather than computing a full exponentiation g^z one might use a pseudorandom walk as done in Pollard rho. For further implementation tricks see Sections 5.1 to 5.5 of Odlyzko [469].

If g does not have prime order (e.g., suppose g is a generator of $\mathbb{F}_p^*$ and has order $p-1$) then there are several options: One can apply Pohlig-Hellman and reduce to subgroups of prime order and apply index calculus in each subgroup (or at least the ones of large order). Alternatively, one can apply the algorithm as above and perform the linear algebra modulo the order of g. There will usually be difficulties with non-invertible elements in the linear algebra, and there are several solutions, such as computing the Hermite normal form of the relation matrix or using the Chinese remainder theorem, we refer to Section 5.5.2 of Cohen [136] and Section 15.2.1 of Joux [317] for details.

Exercise 15.5.8. Give an algorithm similar to the above that works when $r^2 \mid (p-1)$.

Exercise 15.5.9. This exercise is about solving many different discrete logarithm instances $h_i = g^{a_i} \pmod p$, for $1 \leq i \leq n$, to the same base g. Once sufficiently many relations are found, determine the cost of solving each individual instance of the DLP. Hence show that one can solve any constant number of instances of the DLP to a given base $g \in \mathbb{F}_p^*$ in $O(L_p(1/2, 2 + o(1)))$ bit operations as $p \to \infty$.

15.5.2 Heuristic Algorithms for Discrete Logarithms Modulo p

To get a faster algorithm it is necessary to improve the time to find smooth relations. It is natural to seek methods to sieve rather than factoring each value by trial division, but it is not known how to do this for relations of the form in equation (15.7). It would also be natural to find an analogue to Pomerance's method of considering residues of size about the square-root of random; Exercise 15.5.10 gives an approach to this, but it does not lower the complexity.

Exercise 15.5.10. (Blake, Fuji-Hara, Mullin and Vanstone [61]) Once one has computed $w = g^z \delta \pmod p$ one can apply the Euclidean algorithm to find integers w_1, w_2 such that $w_1 w \equiv w_2 \pmod p$ and $w_1, w_2 \approx \sqrt{p}$. Since w_1 and w_2 are smaller one would hope that they are much more likely to both be smooth (however, note that both must be smooth). We now make the heuristic assumption that the probability each w_i is B-smooth is independent and the same as the probability that any integer of size $\sqrt{p}$ is B-smooth. Show that the heuristic running time of the algorithm has u^u replaced by $(u/2)^u$ (where $u = \log(p)/\log(B)$) and so the asymptotic running time remains the same.

Coppersmith, Odlyzko and Schroeppel [145] proposed an algorithm for the DLP in $\mathbb{F}_p^*$ that uses sieving. Their idea is to let $H = \lceil \sqrt{p} \rceil$ and define the factor base to be

$$\mathcal{B} = \{q : q \text{ prime}, q < L_p(1/2, 1/2)\} \cup \{H + c : 1 \leq c \leq L_p(1/2, 1/2 + \epsilon)\}.$$

Since $H^2 \pmod p$ is of size $\approx p^{1/2}$ it follows that if $(H + c_1), (H + c_2) \in \mathcal{B}$ then $(H + c_1)(H + c_2) \pmod p$ is of size $p^{1/2+o(1)}$. One can therefore generate relations in $\mathcal{B}$. Further, it is shown in Section 4 of [145] how to sieve over the choices for c_1 and c_2. A heuristic analysis of the algorithm gives complexity $L_p(1/2, 1 + o(1))$ bit operations.

The **number field sieve** (NFS) is an algorithm for the DLP in $\mathbb{F}_p^*$ with heuristic complexity $O(L_p(1/3, c + o(1)))$ bit operations. It is closely related to the number field sieve for factoring and requires algebraic number theory. As with the factoring algorithm, there are two factor bases. Introducing the DLP instance requires an extra algorithm (we will see an example of this in Section 15.5.4). We do not have space to give the details and instead refer to Schirokauer, Weber and Denny [519] or Schirokauer [515, 517] for details.

15.5.3 Discrete Logarithms in Small Characteristic

We now consider the discrete logarithm problem in $\mathbb{F}_q^*$ where $q = p^n$, p is relatively small (the case of most interest is $p = 2$) and n is large. We represent such a field with a polynomial basis as $\mathbb{F}_p[x]/(F(x))$ for some irreducible polynomial $F(x)$ of degree n. The natural notion of smoothness of an element $g(x) \in \mathbb{F}_p[x]/(F(x))$ is that it is a product of polynomials of small degree. Since factoring polynomials over finite fields is polynomial-time we expect to more easily get good algorithms in this case. The first work on this topic was due to Hellman and Reyneri but we follow Odlyzko's large paper [469]. First we quote some results on smooth polynomials.

Definition 15.5.11. Let p be prime and $n, b \in \mathbb{N}$. Let $I(n)$ be the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree n. A polynomial $g(x) \in \mathbb{F}_p[x]$ is called **b-smooth** if all its irreducible factors have degree $\leq b$. Let $N(n, b)$ be the number of b-smooth polynomials of degree exactly equal to n. Let $p(n, b)$ be the probability that a uniformly chosen polynomial of degree at most n is b-smooth.

Theorem 15.5.12. *Let p be prime and $n, b \in \mathbb{N}$.*

1. *$I(n) = \frac{1}{n}\sum_{d|n} \mu(d) p^{n/d} = \frac{1}{n}p^n + O(p^{n/2}/n)$ where $\mu(d)$ is the Möbius function.*[8]
2. *If $n^{1/100} \leq b \leq n^{99/100}$ then $N(n, b) = p^n(b/n)^{(1+o(1))n/b}$ as n tends to infinity.*
3. *If $n^{1/100} \leq b \leq n^{99/100}$ then $p(n, b)$ is at least $u^{-u(1+o(1))}$ where $u = n/b$ and n tends to infinity.*
4. *If $n^{1/100} \leq b \leq n^{99/100}$ then the expected number of trials before a randomly chosen element of $\mathbb{F}_p[x]$ of degree n is b-smooth is $u^{u(1+o(1))}$ as $u \to \infty$.*

Proof: Statement 1 follows from an elementary counting argument (see, for example, Theorem 3.25 of Lidl and Niederreiter [388]).

Statement 2 in the case $p = 2$ is Corollary A.2 of Odlyzko [469]. The general result was proved by Soundararajan (see Theorems 2.1 and 2.2 of Lovorn Bender and Pomerance [397]). Also see Section 9.15 of [388].

Statement 3 follows immediately from statement 2 and the fact there are p^n monic polynomials of degree at most n (when considering smoothness it is sufficient to study monic polynomials). Statement 4 follows immediately from statement 3. □

[8] This is the "prime number theorem for polynomials", $I(n) \approx p^n / \log_p(p^n)$.

The algorithm then follows exactly the ideas of the previous section. Suppose g has prime order $r \mid (p^n - 1)$ and $h \in \langle g \rangle$. The factor base is

$$\mathcal{B} = \{P(x) \in \mathbb{F}_p[x] : P(x) \text{ is monic, irreducible and } \deg(P(x)) \leq b\}$$

for some integer b to be determined later. Note that $\#\mathcal{B} = I(1) + I(2) + \cdots + I(b) \approx p^{b+1}/(b(p-1))$ (see Exercise 15.5.14). We compute random powers of g multiplied by a suitable $\delta \in G'$ (where, if $r^2 \nmid (p^n - 1)$, $G' \subseteq \mathbb{F}_{p^n}^*$ is the subgroup of order $(p^n - 1)/r$; when $r^2 \mid (p^n - 1)$ then use the method of Exercise 15.5.8), reduce to polynomials in $\mathbb{F}_p[x]$ of degree at most n, and try to factor them into products of polynomials from $\mathcal{B}$. By Exercise 2.12.11 the cost of factoring the b-smooth part of a polynomial of degree n is $O(bn\log(n)\log(p)M(\log(p^n))) = O(\log(p^n)^3)$ bit operations (in any case, polynomial-time). As previously, we are generating polynomials of degree n uniformly at random and so, by Theorem 15.5.12, the expected number of trials to get a relation is $u^{u(1+o(1))}$ where $u = n/b$ as $u \to \infty$. We need to obtain $\#\mathcal{B}$ relations in general. Then we obtain a single relation of the form $hg^a\delta = \prod_{P \in \mathcal{B}} P^{e_P}$, perform linear algebra, and hence solve the DLP.

Exercise 15.5.13. Write the above algorithm in pseudocode.

Exercise 15.5.14. Show that $\sum_{i=1}^{b} I(b) \leq \frac{1}{b}p^b(1 + 2/(p-1)) + O(bp^{b/2})$. Show that a very rough approximation is $p^{b+1}/(b(p-1))$.

Exercise 15.5.15. Let the notation be as above. Show that the complexity of this algorithm is at most

$$c_1 \#\mathcal{B} u^{u(1+o(1))} \log(q)^3 + c_2 (\#\mathcal{B})^{2+o(1)} M(\log(r))$$

bit operations (for some constants c_1 and c_2) as $n \to \infty$ in $q = p^n$.

For the complexity analysis it is natural to arrange that $\#\mathcal{B} \approx L_{p^n}(1/2, c)$ for a suitable constant c. Recall that $\#\mathcal{B} \approx p^b/b$. To have $p^b/b = L_{p^n}(1/2, c)$ then, taking logs,

$$b\log(p) - \log(b) = c\sqrt{n\log(p)(\log(n) + \log(\log(p)))}.$$

It follows that $b \approx c\sqrt{n\log(n)/\log(p)}$.

Exercise 15.5.16. Show that one can compute discrete logarithms in $\mathbb{F}_{p^n}^*$ in expected $O(L_{p^n}(1/2, \sqrt{2} + o(1)))$ bit operations for fixed p and as $n \to \infty$. (Note that this result does not rely on any heuristic assumptions.)

Exercise 15.5.17. Adapt the trick of exercise 15.5.10 to this algorithm. Explain that the complexity of the algorithm remains the same, but is now heuristic.

Lovorn Bender and Pomerance [397] give rigorous complexity $L_{p^n}(1/2, \sqrt{2} + o(1))$ bit operations as $p^n \to \infty$ and $p \leq n^{o(n)}$ (i.e., p is not fixed).

15.5.4 Coppersmith's Algorithm for the DLP in $\mathbb{F}_{2^n}^*$

This algorithm (inspired by the "systematic equations" of Blake, Fuji-Hara, Mullin and Vanstone [61]) was the first algorithm in computational number theory to have heuristic subexponential complexity of the form $L_q(1/3, c + o(1))$.

The method uses a polynomial basis for $\mathbb{F}_{2^n}$ of the form $\mathbb{F}_2[x]/(F(x))$ for $F(x) = x^n + F_1(x)$ where $F_1(x)$ has very small degree. For example, $\mathbb{F}_{2^{127}} = \mathbb{F}_2[x]/(x^{127} + x + 1)$.

The "systematic equations" of Blake et al are relations among elements of the factor base that come almost for free. For example, in $\mathbb{F}_{2^{127}}$, if $A(x) \in \mathbb{F}_2[x]$ is an irreducible polynomial in the factor base then $A(x)^{128} = A(x^{128}) \equiv A(x^2+x) \pmod{F(x)}$ and $A(x^2+x)$ is either irreducible or is a product $P(x)P(x+1)$ of irreducible polynomials of the same degree (Exercise 15.5.18). Hence, for many polynomials $A(x)$ in the factor base one gets a non-trivial relation.

Exercise 15.5.18. Let $A(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial. Show that $A(x^2+x)$ is either irreducible or a product of two polynomials of the same degree.

Coppersmith [140] extended the idea as follows: Let $b \in \mathbb{N}$ be such that $b = cn^{1/3}\log(n)^{2/3}$ for a suitable constant c (later we take $c = (2/(3\log(2)))^{2/3}$), let $k \in \mathbb{N}$ be such that $2^k \approx \sqrt{n/b} \approx \frac{1}{\sqrt{c}}(n/\log(n))^{1/3}$, and let $l = \lceil n/2^k \rceil \approx \sqrt{nb} \approx \sqrt{c}n^{2/3}\log(n)^{1/3}$. Let $\mathcal{B} = \{A(x) \in \mathbb{F}_2[x] : \deg(A(x)) \leq b, A(x) \text{ irreducible}\}$. Note that $\#\mathcal{B} \approx 2^b/b$ by Exercise 15.5.14. Suppose $A(x), B(x) \in \mathbb{F}_2[x]$ are such that $\deg(A(x)) = d_A \approx b$ and $\deg(B(x)) = d_B \approx b$ and define $C(x) = A(x)x^l + B(x)$. In practice one restricts to pairs $(A(x), B(x))$ such that $\gcd(A(x), B(x)) = 1$. The crucial observation is that

$$C(x)^{2^k} = A(x^{2^k}) \cdot (x^{2^k})^l + B(x^{2^k}) \equiv A(x^{2^k})x^{2^k l - n}F_1(x) + B(x^{2^k}) \pmod{F(x)}. \quad (15.9)$$

Write $D(x)$ for the right hand side of equation (15.9). We have $\deg(C(x)) \leq \max\{d_A + l, d_B\} \approx l \approx n^{2/3}\log(n)^{1/3}$ and $\deg(D(x)) \leq \max\{2^k d_A + (2^k l - n) + \deg(F_1(x)), 2^k d_B\} \approx 2^k b \approx n^{2/3}\log(n)^{1/3}$.

Example 15.5.19. (Thomé [608]) Let $n = 607$ and $F_1(x) = x^9 + x^7 + x^6 + x^3 + x + 1$. Let $b = 23$, $d_A = 21, d_B = 28$, $2^k = 4$, $l = 152$. The degrees of $C(x)$ and $D(x)$ are 173 and 112 respectively.

We have two polynomials $C(x), D(x)$ of degree $\approx n^{2/3}$ that we wish to be b-smooth where $b \approx n^{1/3}\log(n)^{2/3}$. We will sketch the complexity later under the heuristic assumption that, from the point of view of smoothness, these polynomials are independent. We will also assume that the resulting relations are essentially random (and so with high probability there is a non-trivial linear dependence once $\#\mathcal{B}+1$ relations have been collected).

Having generated enough relations among elements of the factor base, it is necessary to find some relations involving the elements g and h of the DLP instance. This is not trivial. All DLP algorithms having complexity $L_q(1/3, c+o(1))$ feature a process called **special q-descent** that achieves this. The first step is to express g (respectively, h) as a product $\prod_i G_i(x)$ of polynomials of degree at most $b_1 = n^{2/3}\log(n)^{1/3}$; this can be done by multiplying g (resp. h) by random combinations of elements of $\mathcal{B}$ and factoring (one can also apply the Blake et al trick as in Exercise 15.5.10). We now have a list of around $2n^{1/3} < n$ polynomials $G_i(x)$ of degree $\approx n^{2/3}$ that need to be "smoothed" further. Section VII of [140] gives a method to do this: essentially one performs the same sieving as earlier except that $A(x)$ and $B(x)$ are chosen so that $G_i(x) \mid C(x) = A(x)x^l + B(x)$ (not necessarily with the same value of l or the same degrees for $A(x)$ and $B(x)$). Defining $D(x) = C(x)^{2^k} \pmod{F(x)}$ (not necessarily the same value of k as before) one hopes that $C(x)/G(x)$ and $D(x)$ are b-smooth. After sufficiently many trials one has a relation that expresses $G_i(x)$ in terms of elements of $\mathcal{B}$. Repeating for the polynomially many values $G_i(x)$ one eventually has the values g and h expressed in terms of elements of $\mathcal{B}$. One can then do linear algebra modulo the order of g to find integers Z_1, Z_2 such that $g^{Z_1}h^{Z_2} = 1$ and the DLP is solved.

Example 15.5.20. We give an example of Coppersmith's method for $\mathbb{F}_{2^{15}} = \mathbb{F}_2[x]/(F(x))$ where $F(x) = x^{15} + x + 1$. We consider the subgroup of $\mathbb{F}_{2^{15}}^*$ of order $r = 151$ (note that $(2^{15} - 1)/r = 7 \cdot 31 = 217$). Let $g = x^{11} + x^7 + x^5 + x^2 + 1$ and $h = x^{14} + x^{11} + x^{10} + x^9 + 1$ be the DLP instance.

First note that $n^{1/3} \approx 2.5$ and $n^{2/3} \approx 6.1$. We choose $b = 3$ and so $\mathcal{B} = \{x, x+1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1\}$. We hope to be testing polynomials of degree around 6 to 8 for smoothness.

First, we find some "systematic equations". We obviously have the relation $x^{15} = x+1$. We also have $(x + 1)^{16} = x^2 + x + 1$ and $(x^3 + x + 1)^{16} = (x^3 + x + 1)(x^3 + x^2 + 1)$.

Now, we do Coppersmith's method. We must choose $2^k \approx \sqrt{n/b} = \sqrt{5} \approx 2.2$ so take $2^k = 2$. Let $l = \lceil n/2^k \rceil = 8$, choose $A(x)$ and $B(x)$ of degree at most 2, set $C(x) = A(x)x^8 + B(x)$ and $D(x) = C(x)^2 \pmod{F(x)}$, and test $C(x)$ and $D(x)$ for smoothness over $\mathcal{B}$. We find the following pairs $(A(x), B(x))$ such that both $C(x)$ and $D(x)$ factor over $\mathcal{B}$.

$A(x)$	$B(x)$	$C(x)$	$D(x)$
1	1	$(x+1)^8$	$x^2 + x + 1$
1	x	$x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$	x
1	x^2	$x^2(x+1)^2(x^2 + x + 1)^2$	$x(x^3 + x + 1)$

The first relation in the table is a restatement of $(x + 1)^{16} = x^2 + x + 1$. All together, we have the relation matrix

$$\begin{pmatrix} 15 & -1 & 0 & 0 & 0 \\ 0 & 16 & -1 & 0 & 0 \\ 0 & 0 & 0 & 15 & -1 \\ 1 & 2 & 0 & 2 & 2 \\ 3 & 4 & 4 & -1 & 0 \end{pmatrix}. \tag{15.10}$$

To solve the DLP one can now try to express g and h over the factor base. One has

$$g^{22} = x(x + 1)(x^2 + x + 1)^2(x^3 + x^2 + 1).$$

For h we find

$$hg^{30} = x^6(x + 1)^4 G(x)$$

where $G(x) = x^4 + x + 1$ is a "large prime". To "smooth" $G(x)$ we choose $A(x) = 1$, $B(x) = A(x)x^8 \pmod{G(x)} = x^2 + 1$, $C(x) = A(x)x^8 + B(x)$ and $D(x) = C(x)^2 \pmod{F(x)}$. One finds $C(x) = G(x)^2$ and $D(x) = (x + 1)(x^3 + x^2 + 1)$. In other words, $G(x)^4 = (x + 1)(x^3 + x^2 + 1)$.

There are now two ways to proceed. Following the algorithm description above we add to the matrix the two rows $(1, 1, 2, 0, 1)$ and $4(6, 4, 0, 0, 0) + (0, 1, 0, 0, 0, 1) = (24, 17, 0, 0, 1)$ corresponding to g^{22} and $h^4 g^{120}$. Finding a non-trivial kernel vector modulo 151, such as $(1, 114, 0, 132, 113, 133, 56)$ gives the relation

$$1 = (g^{22})^{133}(h^4 g^{120})^{56} = g^{133} h^{73}$$

from which we deduce $h = g^{23}$.

An alternative approach to the linear algebra is to diagonalise the system in equation (15.10) using linear algebra over $\mathbb{Z}$ (or at least modulo $2^{15} - 1$) to get $x + 1 = x^{15}, x^2 + x + 1 = x^{240}, x^3 + x + 1 = x^{1023}$ and $x^3 + x^2 + 1 = x^{15345}$. One then gets

$$g^{22} = x(x + 1)(x^2 + x + 1)^2(x^3 + x^2 + 1) = x^{1+15+2\cdot 240+15345} = x^{15841}$$

and so

$$g = x^{15841 \cdot 22^{-1} \pmod{(2^{15}-1)}} = x^{26040} = (x^{217})^{120}.$$

Similarly, $G(x)^4 = (x+1)(x^3+x^2+1) = x^{15+15345} = x^{15360}$ and so $G(x) = x^{3840}$. Finally,

$$h = g^{-30}x^6(x+1)^4G(x) = x^{-30 \cdot 26040+6+4 \cdot 15+3840} = x^{9114} = (x^{217})^{42}$$

and so $h = g^{42 \cdot 120^{-1} \pmod{151}} = g^{23}$.

Conjecture 15.5.21. *Coppersmith's algorithm solves the DLP in $\mathbb{F}_q^*$ where $q = 2^n$ in $L_q(1/3, (32/9)^{1/3} + o(1))$ bit operations as $n \to \infty$.*

Note that, to compare with Exercise 15.2.12, if $q = 2^{1024}$ then $L_q(1/3, (32/9)^{1/3}) \approx 2^{67}$.

This conjecture would hold if the probability that the polynomials $C(x)$ and $D(x)$ are smooth was the same as for independently random polynomials of the same degree. We now give a justification for the constant. Let $b = cn^{1/3}\log(n)^{2/3}$. Note that $2^k \approx \sqrt{n/b} \approx (n/\log(n))^{1/3}/\sqrt{c}$ and $l \approx \sqrt{nb}$. We need around $2^b/b$ relations, and note that $\log(2^b/b) \approx b\log(2) = c\log(2)n^{1/3}\log(n)^{2/3}$. We have $\deg(C(x)) \approx d_A + l$ and $\deg(D(x)) \approx 2^k d_A$. The number of trials until $C(x)$ is b-smooth is u^u where $u = (d_A + l)/b \approx h/b \approx \sqrt{n/b} = \frac{1}{\sqrt{c}}(n/\log(n))^{1/3}$. Hence, $\log(u^u) = u\log(u) \approx \frac{1}{3\sqrt{c}}n^{1/3}\log(n)^{2/3}$. Similarly, the number of trials until $D(x)$ is b-smooth is approximately u^u where $u = (2^k d_A)/b \approx 2^k \approx \sqrt{n/b}$ and the same argument applies. Since both events must occur the expected number of trials to get a relation is $\exp(\frac{2}{3\sqrt{c}}(n\log(n)^2)^{1/3})$. Hence, total expected time to generate enough relations is

$$\exp\left((c\log(2) + \tfrac{2}{3\sqrt{c}})n^{1/3}\log(n)^{2/3}\right).$$

This is optimised when $c^{3/2}\log(2) = 2/3$, which leads to the stated complexity for the first stage of the algorithm. (In practice one chooses c so that there are enough smooth pairs $(C(x), D(x))$ to generate the required number of relations.) The linear algebra is $O((2^b/b)^{2+o(1)}M(\log(r)))$ bit operations, which is the same complexity, and the final stage of solving the DLP has lower complexity (it is roughly the same as the cost of finding polynomially many smooth relations, rather than finding $2^b/b$ of them). For more details about the complexity of Coppersmith's method we refer to Section 2.4 of Thomé [608].

Since one can detect smoothness of polynomials in polynomial-time it is not necessary, from a complexity theory point of view, to sieve. However, in practice sieving can be worthwhile and a method to do this was given by Gordon and McCurley [263].

Coppersmith's idea is a special case of a more general approach to index calculus algorithms known as the **function field sieve**. Note that Coppersmith's algorithm only has one factor base, whereas the function field sieve works using two factor bases.

15.5.5 The Joux-Lercier Algorithm

The function field sieve of Adleman is a general algorithm for discrete logarithms in $\mathbb{F}_{p^n}$ where p is relatively small compared with n. Joux and Lercier gave a much simpler and better algorithm. We will sketch this algorithm, but refer to Joux and Lercier [318] and Section 15.2 of [317] for full details. We also refer to [517] for a survey of the function field sieve.

Let p be prime and $n \in \mathbb{N}$. Let $d = \lceil \sqrt{n} \rceil$. Suppose one has monic polynomials $F_1(t), F_2(t) \in \mathbb{F}_p[t]$ such that $\deg(F_1(t)) = \deg(F_2(t)) = d$ and $F_2(F_1(t)) - t$ has an irreducible factor $F(t)$ of degree n. We represent $\mathbb{F}_{p^n}$ with the polynomial basis $\mathbb{F}_p[t]/(F(t))$.

Given a prime p and an integer n one can find such polynomials $F_1(t)$ and $F_2(t)$ in very little time (e.g., by choosing polynomials of the right degree uniformly at random and testing the condition using polynomial factorisation).

Exercise 15.5.22. Let $n = 15$. Find polynomials $F_1(t), F_2(t) \in \mathbb{F}_2[t]$ of degree 4 such that $F_2(F_1(t)) - t$ has an irreducible factor of degree 15.

Now consider the polynomial ring $A = \mathbb{F}_p[x, y]$ and two ring homomorphisms $\psi_1 : A \to A_1 = \mathbb{F}_p[x]$ by $\psi_1(y) = F_1(x)$ and $\psi_2 : A \to A_2 = \mathbb{F}_p[y]$ by $\psi_2(x) = F_2(y)$. Define $\phi_1 : A_1 \to \mathbb{F}_{p^n}$ by $\phi_1(x) = t \pmod{F(t)}$ and $\phi_2 : A_2 \to \mathbb{F}_{p^n}$ by $\phi_2(y) = F_1(t) \pmod{F(t)}$.

Exercise 15.5.23. Let the notation be as above and $G(x, y) \in \mathbb{F}_p[x, y]$. Show that $\phi_1(\psi_1(G(x, y))) = \phi_2(\psi_2(G(x, y)))$ in $\mathbb{F}_{p^n}$.

Let $\mathcal{B}_1 \subseteq A_1 = \mathbb{F}_p[x]$ and $\mathcal{B}_2 \subseteq \mathbb{F}_p[y]$ be the sets of linear polynomials. The idea of the algorithm is simply to consider polynomials in $\mathbb{F}_p[x, y]$ of the form $G(x, y) = xy + ax + by + c$. If $\psi_1(G(x, y)) = (x + b)F_1(x) + (ax + c)$ factors over $\mathcal{B}_1$ as $\prod_{i=1}^{d+1}(x - u_i)$ and if $\psi_2(G(x, y)) = (y + a)F_2(y) + (by + c)$ factors over $\mathcal{B}_2$ as $\prod_{j=1}^{d+1}(y - v_j)$ then we have a relation. The point is that such a relation corresponds to

$$\prod_{i=1}^{d+1}(t - u_i) = \prod_{j=1}^{d+1}(F_1(t) - v_j)$$

in $\mathbb{F}_{p^n}$.

One also needs to introduce the DLP instance by using a special q-descent: given an irreducible polynomial $q(x)$ one constructs polynomials $a(x), b(x)$ such that $q(x) \mid (a(x)F_1(x) + b(x))$ and one hopes that $(a(x)F_1(x) + b(x))/q(x)$ has small factors and that $a(F_2(y))y + b(F_2(y))$ has small factors, and hence iterate the process. When enough relations are collected (including at least one "systematic equation" to remove the parasitic solution explained on page 442 of Joux/indexAJoux, A. [317]) one can perform linear algebra to solve the DLP. The heuristic complexity of this algorithm is shown in [318] and Section 15.2.1.2 of [317] to be between $L_{p^n}(1/3, 3^{1/3} + o(1))$ and $L_{p^n}(1/3, (32/9)^{1/3} + o(1))$ for $p \leq L_{p^n}(1/3, (4/9)^{1/3} + o(1))$.

15.5.6 Number Field Sieve for the DLP

Concepts from the number field sieve for factoring have been applied in the setting of the DLP. Again, one uses two factor bases, corresponding to ideals in the ring of integers of some number field (one of the number fields may be $\mathbb{Q}$). As with Coppersmith's method, once sufficiently many relations have been found among elements of the factor bases, special q-descent is needed to solve a general instance of the DLP. We refer to Schirokauer [517] for details of the NFS algorithm for the DLP, and also for the heuristic arguments that one can solve the DLP in $\mathbb{F}_p^*$ in $L_p(1/3, (64/9)^{1/3} + o(1))$ bit operations. When p has a special form (e.g., $p = 2^n \pm 1$) then the **special number field sieve** (SNFS) can be used to solve the DLP in (heuristic) $L_p(1/3, (32/9)^{1/3} + o(1))$ bit operations, see [518].

We should also mention the **special function field sieve** (SFFS) for solving the DLP in $\mathbb{F}_{p^n}^*$, which has heuristic complexity $L_{p^n}(1/3, (32/9)^{1/3} + o(1))$ bit operations as $p^n \to \infty$ as long as $p \leq n^{o(\sqrt{n})}$, see Schirokauer [516, 517].

15.5.7 Discrete Logarithms for all Finite Fields

We have sketched algorithms for the DLP in $\mathbb{F}_p^*$ when p is large or $\mathbb{F}_{p^n}^*$ when p is relatively small. We have not considered cases $\mathbb{F}_q^*$ where $q = p^n$ with p large and $n > 1$. The basic concepts can be extended to cover all cases, but ensuring that subexponential complexity is achieved for all combinations of p and n is non-trivial. Adleman and Demarrais [2] were the first to give a heuristic subexponential algorithm for all finite fields. They split the problem space into $p > n$ and $p \leq n$; in the latter case they have complexity $L_q(1/2, 3 + o(1))$ bit operations as $q \to \infty$ and in the former case heuristic complexity $L_q(1/2, c + o(1))$ for a non-explicit constant c.

Heuristic algorithms with complexity $L_q(1/3, c + o(1))$ for all finite fields are given by Joux and Lercier [318] and Joux, Lercier, Smart and Vercauteren [319].

15.6 Discrete Logarithms on Hyperelliptic Curves

Some index calculus algorithms for the discrete logarithm problem in finite fields generalise naturally to solving the DLP in the divisor class group of a curve. Indeed, some of these algorithms also apply to the ideal class group of a number field, but we do not explore that situation in this book. An excellent survey of discrete logarithm algorithms for divisor class groups is Chapter VII of [65].

We consider hyperelliptic curves $C : y^2 + H(x)y = F(x)$ over $\mathbb{F}_q$ of genus g, so $\deg(H(x)) \leq g + 1$ and $\deg(F(x)) \leq 2g + 2$. Recall that elements of the divisor class group have a Mumford representation $(u(x), y - v(x))$ (for curves with a split model there is also an integer $0 \leq n \leq g - \deg(u(x))$ to take into account the behaviour at infinity). Let D_1 and D_2 be reduced divisors representing divisor classes of order r (where r is a prime such that $r^2 \nmid \#\mathrm{Pic}^0_{\mathbb{F}_q}(C)$). The goal is to compute $a \in \mathbb{Z}/r\mathbb{Z}$ such that $D_2 \equiv [a]D_1$.

Recall from Exercise 10.3.12 that a reduced divisor with Mumford representation $(u(x), v(x))$ is said to be a **prime divisor** if the polynomial $u(x)$ is irreducible over $\mathbb{F}_q$. The **degree** of the effective affine divisor is $\deg(u(x))$. Any effective affine divisor D can be written as a sum of prime effective affine divisors by factoring the $u(x)$ polynomial of its Mumford representation. Hence, it is natural to define D to be b-smooth if it is a sum of prime effective divisors of degree at most b. This suggests selecting the factor base $\mathcal{B}$ to consist of all prime effective affine divisors of degree at most b for some smoothness bound $1 \leq b \leq g$.

We assume that $\mathcal{B}$ generates the group $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$; this is immediate when the group has prime order and $\mathcal{B}$ contains a non-trivial element. Voloch [624] has proved that degree 1 primes generate $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ whenever $q > (8g(C) - 2)^2$, where $g(C)$ is the genus of C.

One can obtain an algorithm for the DLP of a familiar form, by generating reduced divisors and testing whether they are smooth. One issue is that our smoothness results for polynomials apply when polynomials are sampled uniformly from the set of all polynomials of degree n in $\mathbb{F}_q[x]$, whereas we now need to apply the results to the set of polynomials $u(x) \in \mathbb{F}_q[x]$ of degree g that arise in Mumford's representation. This issue is handled using Theorem 15.6.1.

There are two rather different ways to generate reduced divisors, both of which are useful for the algorithm.

1. One can take random group elements of the form $[n]D_1$ or $[n_1]D_1 + [n_2]D_2$ and compute the Mumford representation of the corresponding reduced effective affine divisor. This is the same approach as used in Section 15.5.1 and, in the context of ideal/divisor class groups, is sometimes called the **Hafner-McCurley algorithm**.

If the divisor is $\mathcal{B}$-smooth then we obtain a relation between elements of $\mathcal{B}$ and D_1 and D_2.

2. One can consider the effective affine divisor of the function $a(x) + yb(x)$ for random polynomials $a(x), b(x)$. This idea is due to Adleman, DeMarrais and Huang [4]. Since a principal divisor is equivalent to zero in the ideal class group, if the divisor is $\mathcal{B}$-smooth then we get a relation in $\mathcal{B}$.

To introduce the instance of the DLP into the system it is necessary to have some relations involving D_1 and D_2. This can either be done using the first method, or by choosing $a(x)$ and $b(x)$ so that points in the support of either D_1 or D_2 lie in the support of $\mathrm{div}(a(x)+yb(x))$ (we have seen this kind of idea already, e.g., in Coppersmith's algorithm).

It is convenient to add to $\mathcal{B}$ all points at infinity and all points $P \in C(\overline{\mathbb{F}}_q)$ such that $P = \iota(P)$ (equivalently all $\mathbb{F}_q$-rational prime divisors with this property). Since the latter divisors all have order 2 one automatically obtains relations that can be used to eliminate them during the linear algebra stage of the algorithm. Hence, we say that a reduced divisor $D = \mathrm{div}(u(x), y - v(x))$ in Mumford representation is b-**smooth** if $u(x)$ is b-smooth after any factors corresponding to points of order 2 have been removed.

Let C be a hyperelliptic curve over $\mathbb{F}_q$ of genus g and $1 \leq b < g$. Prime effective affine divisors on C of degree b correspond to irreducible polynomials $u(x)$ of degree b (and for roughly half of all such polynomials $u(x)$ there are two solutions $v(x)$ to $v(x)^2 + v(x)H(x) - F(x) \equiv 0 \pmod{u(x)}$). Hence, it is natural to expect that there are approximately q^b/b such divisors. It follows that $\#\mathcal{B}$ should be around $\sum_{i=1}^{b} q^i/i \approx \frac{1}{b}p^b(1 + 2/(p-1))$ by the same argument as Exercise 15.5.14.

For the analysis, one needs to estimate the probability that a randomly chosen reduced divisor is smooth.

Theorem 15.6.1. *(Theorem 6 of Enge and Stein [198]) Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$. Let $c > 1$ and let $b = \lceil \log_q(L_{q^g}(1/2, c)) \rceil$. Then the number of b-smooth reduced divisors of degree g is at least*

$$\frac{q^g}{L_{q^g}(1/2, 1/(2c) + o(1))}$$

for fixed q and $g \to \infty$.

Note that the smoothness bound in the above result is the ceiling of a real number. Hence one cannot deduce subexponential running time unless the genus is sufficiently large compared with the field size.

15.6.1 Index Calculus on Hyperelliptic Curves

Suppose that $r \mid N = \#\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ and $r^2 \nmid N$. Suppose $\overline{D}_1, \overline{D}_2$ are two divisor classes on C over $\mathbb{F}_q$ of order r represented by reduced divisors D_1 and D_2. The algorithm of Section 15.5.1 immediately applies to solve the DLP: choose the factor base as above; generate random reduced divisors by computing $[n_1]D_1 + [n_2]D_2 + \delta$ (where δ is uniformly chosen[9] from the subgroup $G' \subseteq \mathrm{Pic}^0_{\mathbb{F}_q}(C)$ of order N/r); store the resulting smooth relations; perform linear algebra modulo r to find integers a, b such that $[a]D_1 + [b]D_2 \equiv 0$ (extra care is needed when there are two points at infinity to be sure the relation is correct).

[9] We assume that generators for this group are known so that it is easy to sample uniformly from this group.

Exercise 15.6.2. Show that the expected running time of this algorithm is (rigorously!) $L_{q^g}(1/2, \sqrt{2} + o(1))$ bit operations as $g \to \infty$.

We refer to Section VII.5 of [65] for practical details of the algorithm. Note that the performance can be improved using the sieving method of Flassenberg and Paulus [206].

15.6.2 The Algorithm of Adleman, De Marrais and Huang

This algorithm, from [4], uses the same factor base as the method of the previous section. The main difference is to generate relations by decomposing principal divisors $A(x) + yB(x)$. An advantage of this approach is that group operations are not required.

By Exercise 10.1.26 it is easy to compute $v_P(A(x) + yB(x))$ by computing the norm $A(x)^2 - H(x)A(x)B(x) - F(x)B(x)^2$ and factoring it as a polynomial. If $\deg(A(x)) = d_A < g$ and $\deg(B(x)) = d_B < g$ then the norm has degree at most $\max\{2d_A, (g+1) + d_A + d_B, 2g + 2 + 2d_B\}$, which is much larger in general than the degree g polynomial in a reduced Mumford representation, but still $O(g)$ in practice.

We need to make the heuristic assumption that the probability the norm is b-smooth is the same as the probability that a random polynomial of the same degree is b-smooth. We therefore assume the expected number of trials to get an $L_{q^g}(1/2, c)$-smooth polynomial is $L_{q^g}(1/2, 1/(2c) + o(1))$ as g tends to infinity.

We also need some relations involving D_1 and D_2. Adleman et al do this by first decomposing D_1 and D_2 as a sum of prime divisors. Then they "smooth" each prime divisor $\mathrm{div}(u(x), y - v(x))$ by choosing polynomials $B(x), W(x) \in \mathbb{F}_q[x]$, setting $A'(x) = B(x)(v(x) + H(x)) \pmod{u(x)}$ and then $A(x) = A'(x) + u(x)W(x)$. One computes $N(x) = (A(x)^2 - H(x)A(x)B(x) - F(x)B(x)^2)$. By construction, $u(x) \mid N(x)$ and one continues randomly choosing A and W until $N(x)/u(x)$ is b-smooth.

The details of the algorithm are then the same as the algorithm in Section 15.5.1: one uses linear algebra modulo r to get a relation $[a]D_1 + [b]D_2 \equiv 0$ (again, care is needed when there are two points at infinity). We leave the details as an exercise.

Exercise 15.6.3. Write pseudocode for the Adleman, DeMarrais, Huang algorithm.

The heuristic complexity of the algorithm is of the same form as the earlier algorithm (the cost of smoothing the divisors D_1 and D_2 is heuristically the same as finding less than $2g$ relations so is negligible. One obtains heuristic asymptotic complexity of $L_{q^g}(1/2, \sqrt{2} + o(1))$ bit operations as g tends to infinity. This is much better than the complexity claimed in [4] since that paper also gives an algorithm to compute the group structure (and so the linear algebra requires computing the Hermite normal form).

These ideas will be used again in Section 15.9.1.

15.6.3 Gaudry's Algorithm

Gaudry [242] considered the algorithm of Section 15.6.1 for fixed genus, rather than asympotically as $g \to \infty$. In particular he chose the smoothness bound $b = 1$ (so the factor base $\mathcal{B}$ only consists of degree one prime divisors, i.e., points). Good surveys of Gaudry's algorithm are given in Chapter VII of [65] and Section 21.2 of [16].

Exercise 15.6.4. Let C be a hyperelliptic curve of genus g over a finite field $\mathbb{F}_q$. Show that the number of prime divisors on C of degree 1 is $\#C(\mathbb{F}_q) = q(1 + o(1))$ for fixed g as $q \to \infty$. Hence, show that the probability that a randomly chosen reduced divisor is 1-smooth is $\frac{1}{g!}(1 + o(1))$ as $q \to \infty$.

Exercise 15.6.5. Following Exercise 15.6.4, it is natural to conjecture that one needs to choose $O(g!q(1+o(1)))$ divisors (again, this is for fixed g as $q \to \infty$, in which case it is more common to write it as $O(q(1+o(1)))$) to find enough relations to have a non-trivial linear dependence in $\mathcal{B}$. Under this assumption, show that the heuristic expected running time of Gaudry's algorithm is at most

$$c_1 g^2 g! q(1+o(1))M(\log(q)) + c_2 g^3 q^2 M(\log(q))) = O(q^2 M(\log(q))(1+o(1))) \quad (15.11)$$

bit operations (for some constants c_1 and c_2) for fixed g as $q \to \infty$.

The first term in equation (15.11) is the running time for relation generation. If g is fixed then asymptotically this is dominated by the second term, which is the running time for the linear algebra stage. If g is fixed, then the running time is $\tilde{O}(q^2)$ bit operations. Hence Gaudry's algorithm is asymptotically faster than Pollard's rho method for hyperelliptic curves of a fixed genus $g \geq 5$. However, the hidden constant in the expression $\tilde{O}(q^2)$ depends very badly on g. In practice, Gaudry's method seems to be superior to rho for small g (e.g., $g = 5, 6, 7$).

Harley and Thériault (see [607]) suggested reducing the factor base size in Gaudry's algorithm in order to balance the running times of the relation generation and linear algebra stages. Thériault [607] also proposed a "large prime" variant of Gaudry's algorithm. Gaudry, Thériault, Thomé and Diem [250] proposed a "double large prime" variant of Gaudry's algorithm that is based on the double large prime strategy that was successful in accelerating integer factorization algorithms. The factor base $\mathcal{B}$ is now chosen to be a subset of the degree one divisors and degree one divisors that are not in $\mathcal{B}$ are called *large primes*. A divisor is defined to be smooth if it can be written as a sum of prime divisors and at most two large primes. Relations are collected as before, and then combined to eliminate the large primes (we refer to Section 21.3 of [16] for further discussion of large primes and graph methods for eliminating them). It is shown in [250] that, for fixed g, the expected running time of the algorithm is $\tilde{O}(q^{2-\frac{2}{g}})$ bit operations. This is faster than Pollard rho for $g \geq 3$ when q is sufficiently large. Gaudry's approach was generalised to all curves of fixed genus by Diem [176].

15.7 Weil Descent

As we have seen, there are subexponential algorithms for the DLP in the divisor class group of a hyperelliptic curve of high genus. A natural approach to solve the DLP on elliptic curves is therefore to transform the problem into a DLP on a high genus curve. However, the naive way to do this embeds a small problem into a big one, and does not help to solve the DLP. Frey [212] proposed[10] to use Weil restriction of scalars to transform the DLP on an elliptic curve $E(\mathbb{F}_{q^n})$ for $n > 1$ to the DLP on a curve of genus $g \geq n$ over $\mathbb{F}_q$. Frey called this idea **Weil descent**.

Geometrically the principle is to identify the Weil restriction of an open affine subset of $E(\mathbb{F}_{q^n})$ (see Section 5.7) with an open affine subset of an Abelian variety A over $\mathbb{F}_q$ of dimension n. One can then try to find a curve C on A, so that there is a map from the Jacobian of C to A. Following Gaudry, Hess and Smart [246] it is more convenient to express the situation in terms of function fields and divisor class groups. We only sketch

[10] The standard reference is a lecture given by Frey at the ECC 1998 conference. His talk was mostly about a different (constructive) application of Weil restriction of scalars. However, he did mention the possibility of using this idea for an attack. Galbraith and Smart developed the details further in [229] and many works followed.

the details since an excellent survey is provided by Hess in Chapter VIII of [65] and many important details are explained by Diem in [172].

Let E be an elliptic curve over $\mathbb{K} = \mathbb{F}_{q^n}$ and let $\Bbbk = \mathbb{F}_q$. The function field of E is $\mathbb{K}(E)$. The idea (called in this setting a **covering attack**) is to find a curve C over $\mathbb{K}$ such that $\mathbb{K}(C)$ is a finite extension of $\mathbb{K}(E)$ (so that there is a map $C \to E$ of finite degree) and such that there is an automorphism σ of degree n on $\mathbb{K}(C)$ extending the q-power Frobenius so that the fixed field of $\mathbb{K}(C)$ under $\langle\sigma\rangle$ is $\Bbbk(C^0)$ for some curve C^0. The composition of the conorm map from $E(\mathbb{K})$ to $\mathrm{Pic}^0_C(\mathbb{K})$ and the norm map from $\mathrm{Pic}^0_C(\mathbb{K})$ to $\mathrm{Pic}^0_{C^0}(\Bbbk)$ transfers the DLP from $E(\mathbb{K})$ to $\mathrm{Pic}^0_{C^0}(\Bbbk)$. Hence, as long as the composition of these maps is not trivial, then one has reduced the DLP from $E(\mathbb{K})$ to the divisor class group of a curve C^0 over $\Bbbk$. One can then solve the DLP using an index calculus algorithm, which is feasible if the genus of C^0 is not too large.

A variant of the Weil descent concept that avoids function fields and divisor class groups is to perform index calculus directly on Abelian varieties. This variant is the subject of the following section.

15.8 Discrete Logarithms on Elliptic Curves over Extension Fields

We now discuss some related algorithms, which can be applied to elliptic curves over extension fields. We start by recalling Semaev's idea of summation polynomials.

15.8.1 Semaev's Summation Polynomials

Suppose that E is an elliptic curve defined over a prime field $\mathbb{F}_p$, and that elements of $\mathbb{F}_p$ are represented as integers in the interval $[0, p-1]$. Semaev [539] considered a factor base

$$\mathcal{B} = \{(x, y) \in E(\mathbb{F}_p) \ : \ 0 \leq x \leq p^{1/n}\}$$

for some fixed integer $n \geq 2$. Note that $\#\mathcal{B} \approx p^{1/n}$.

Semaev hoped to perform an index calculus algorithm similar to the one in Section 15.5.1. For random points $R = [a]P + [b]Q$ the task is to write R as a sum of points in $\mathcal{B}$. To accomplish this, Semaev introduced the notion of a summation polynomial.

Definition 15.8.1. Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{F}_q$, where the characteristic of $\mathbb{F}_q$ is neither 2 nor 3 (this condition can be avoided). The **summation polynomials** $\mathrm{Summ}_n \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ for $n \geq 2$ are defined as follows:

- $\mathrm{Summ}_2(x_1, x_2) = x_1 - x_2$.
- $\mathrm{Summ}_3(x_1, x_2, x_3) = (x_1 - x_2)^2x_3^2 - 2((x_1 + x_2)(x_1x_2 + a_4) + 2a_6)x_3 + ((x_1x_2 - a_4)^2 - 4a_6(x_1 + x_2))$.
- $\mathrm{Summ}_n(x_1, x_2, \ldots, x_n) = R_x(\mathrm{Summ}_{n-1}(x_1, \ldots, x_{n-2}, x), \mathrm{Summ}_3(x_{n-1}, x_n, x))$ for $n \geq 4$ where $R_x(F, G)$ is the resultant of the polynomials F and G with respect to the variable x.

For many more details see Section 3 of [177]. The following result is from [539].

Theorem 15.8.2. *Summation polynomials have the following properties:*

- $(x_1, \ldots, x_n) \in \overline{\mathbb{F}}_q^n$ *is a root of* Summ_n *if and only if there exists* $(y_1, \ldots, y_n) \in \overline{\mathbb{F}}_q^n$ *such that* $P_i = (x_i, y_i) \in E(\overline{\mathbb{F}}_q)$ *and* $\sum_{i=1}^n P_i = \infty$.

- Summ_n *is symmetric.*
- *The degree of* Summ_n *in* x_i *is* 2^{n-2}.

Exercise 15.8.3. Prove Theorem 15.8.2.

One way to decompose $R = (x_R, y_R)$ in $\mathcal{B}$ is to find solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ to

$$\text{Summ}_{n+1}(x_1, x_2, \ldots, x_n, x_R) \equiv 0 \pmod{p}, \text{ such that } 0 \leq x_i \leq p^{1/n}. \tag{15.12}$$

If such a solution exists and can be found then one finds the corresponding y-coordinates $\pm y_i$. Suppose that each $y_i \in \mathbb{F}_p$. Then each $P_i = (x_i, y_i)$ is in $\mathcal{B}$ and by Theorem 15.8.2 there exist $s_i \in \{-1, 1\}$ such that $s_1 P_1 + \cdots + s_n P_n = R$. The sign bits s_i can be found by exhaustive search, thereby yielding a relation. Since $\#\{P_1 + P_2 + \cdots + P_n : P_i \in \mathcal{B}\} \approx (p^{1/n})^n / n! = p/n!$ the expected number of points R that have to be selected before a relation is obtained is about $n!$.

Unfortunately, no efficient algorithm is known for solving the polynomial equation (15.12) even for $n = 5$ (in which case the equation has degree 16 in each of its 5 variables). Coppersmith's method (see Section 19.2) seems not to be useful for this task.

In reference to the remarks of Section 15.2.3 we see that all requirements for an index calculus algorithm are met, except that it is not efficient to decompose a smooth element over the factor base.

15.8.2 Gaudry's Variant of Semaev's Method

Gaudry [245] realised that it might be possible to take roots of summation polynomials if one was working with elliptic curves over extension fields. Gaudry's algorithm may be viewed as doing Weil descent without divisor class groups. Indeed, the paper [245] presents a general approach to index calculus on Abelian varieties and so the results apply in greater generality than just Weil descent of elliptic curves.

Suppose that E is an elliptic curve defined over a finite field $\mathbb{F}_{q^n}$ with $n > 1$. Gaudry [245] defines a factor base

$$\mathcal{B} = \{(x, y) \in E(\mathbb{F}_{q^n}) \ : \ x \in \mathbb{F}_q\}$$

so that $\#\mathcal{B} \approx q$. Gaudry considers this as the set of $\mathbb{F}_q$-rational points on the algebraic set F formed by intersecting the Weil restriction of scalars of E with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$ by $n-1$ hyperplanes $V(x_i)$ for $2 \leq i \leq n$, where $x = x_1\theta_1 + \cdots + x_n\theta_n$ (with $\theta_1 = 1$) as in Lemma 5.7.1. If the algebraic set F is irreducible then it is a 1-dimensional variety F.

In the relation generation stage, one attempts to decompose a randomly selected point $R \in E(\mathbb{F}_{q^n})$ as a sum of points in $\mathcal{B}$. Gaudry observed that this can be accomplished by finding solutions

$$(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \quad \text{such that} \quad \text{Summ}_{n+1}(x_1, x_2, \ldots, x_n, x_R) = 0. \tag{15.13}$$

Note that $\text{Summ}_{n+1}(x_1, \ldots, x_n, x_R) \in \mathbb{F}_{q^n}[x_1, \ldots, x_n]$ since E is defined over $\mathbb{F}_{q^n}$ and $x_R \in \mathbb{F}_{q^n}$. The conditions $x_j \in \mathbb{F}_q$ in equation (15.13) can be expressed algebraically as follows. Select a basis $\{\theta_1, \ldots, \theta_n\}$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and write

$$\text{Summ}_{n+1}(x_1, \ldots, x_n, x_R) \ = \ \sum_{i=1}^{n} G_i(x_1, \ldots, x_n)\theta_i \tag{15.14}$$

where $G_i(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$. Note that the degree of G_i in x_j is at most 2^{n-1}. The polynomials G_i of equation (15.14) define an algebraic set in $X \subseteq \mathbb{A}^n$ and we are

interested in the points in $X(\mathbb{F}_q)$ (if there are any). Since $\mathbb{F}_q$ is finite there are only finitely many $\mathbb{F}_q$-rational solutions $(x_1, \ldots, x_n)$ to the system.

Gaudry assumes that X is generically a zero-dimensional algebraic set (Gaudry justifies this assumption by noting that if F is a variety then the variety F^n is n-dimensional, and so the map from F^n to the Weil restriction of E, given by adding together n points in F, is a morphism between varieties of the same dimension, and so generically has finite degree). The $\mathbb{F}_q$-rational solutions can therefore be found by finding a Gröbner basis for the ideal generated by the G_i and then taking roots in $\mathbb{F}_q$ of a sequence of univariate polynomials each of which has degree at most $2^{n(n-1)}$. This is predicted to take $O(2^{cn(n-1)}M(\log(q)))$ bit operations for some constant c. Alternatively one could add some field equations $x_j^q - x_j$ to the ideal, to ensure it is zero-dimensional, but this could have an adverse effect on the complexity. Gaudry makes a further heuristic assumption, namely that the smoothness probability behaves as expected when using the large prime variant.

The size of the set $\{P_1 + P_2 + \cdots + P_n : P_i \in \mathcal{B}\}$ is approximately $q^n/n!$ and so the expected number of points R that have to be selected before a relation is obtained is about $n!$. One needs approximately $\#\mathcal{B} \approx q$ relations to be able to find a non-trivial element in the kernel of the relation matrix and hence integers a and b such that $[a]D_1 + [b]D_2 \equiv 0$. It follows that the heuristic expected running time of Gaudry's algorithm is

$$\tilde{O}(2^{cn(n-1)}n!qM(\log(q)) + q^{2+o(1)}) \tag{15.15}$$

bit operations as $q \to \infty$. This is exponential in terms of n and $\log(q)$. However, for fixed n, the running time can be expressed as $\tilde{O}(q^2)$ bit operations.

Gaudry's focus was on n fixed and relatively small. For any fixed $n \geq 5$, Gaudry's heuristic algorithm for solving the ECDLP over $\mathbb{F}_{q^n}$ is asymptotically faster than Pollard's rho method. The double large prime variant (mentioned in Section 15.6.3) can also be used in this setting. The complexity therefore becomes (heuristic) $\tilde{O}(q^{2-\frac{2}{n}})$ bit operations. Hence Gaudry's algorithm is asymptotically faster than Pollard rho even for $n = 3$ and $n = 4$, namely $\tilde{O}(q^{4/3})$ rather than $\tilde{O}(q^{3/2})$ for $n = 3$ and $\tilde{O}(q^{3/2})$ rather than $\tilde{O}(q^2)$ for $n = 4$.

15.8.3 Diem's Algorithm for the ECDLP

Gaudry's focus was on the DLP in $E(\mathbb{F}_{q^n})$ when n is fixed. This yields an exponential-time algorithm. Diem [173, 177] considered the case where n is allowed to grow, and obtained a subexponential-time algorithm.

The crux of Diem's method is remarkably simple: he assumes $n \approx \sqrt{\log(q)}$ and obtains an algorithm for the DLP in $E(\mathbb{F}_{q^n})$ with complexity $O(q^c)$ for some constant c (note that even some exponential-time computations in n are polynomial in q as $e^{n^2} \approx q$). Now, $q^c = \exp(c\log(q))$ and $\log(q^n) = n\log(q) \approx \log(q)^{3/2}$ so $q^c \approx \exp(c\log(q^n)^{2/3}) < L_{q^n}(2/3, c)$.

Diem's algorithm is very similar to Gaudry's. In Gaudry's algorithm, the factor base consists of points whose x-coordinates lie in $\mathbb{F}_q$. Diem defines a function $\varphi = \alpha \circ x$, where α is an automorphism over $\mathbb{F}_{q^n}$ of $\mathbb{P}^1$ that satisfies a certain condition, and defines the factor base to be $\mathcal{B} = \{P \in E(\mathbb{F}_{q^n}) : \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\}$. The process of generating relations proceeds in the standard way. Some important contributions of [177] are to prove that the algebraic set defined by the summation polynomials has a good chance of having dimension zero, and that when this is the case the points can be found by taking resultants of multihomogeneous polynomials in time polynomial in $e^{n^2}\log(q)$ (which is exponential in n but polynomial in q).

The main result of [177] is the following. We stress that this result does not rely on any heuristics.

Theorem 15.8.4. *(Diem) Let $a, b \in \mathbb{R}$ be such that $0 < a < b$. There is an algorithm such that, if q is a prime power and $n \in \mathbb{N}$ is such that*

$$a\sqrt{\log(q)} \leq n \leq b\sqrt{\log(q)}$$

and E is any elliptic curve over $\mathbb{F}_{q^n}$, then the algorithm solves the DLP in $E(\mathbb{F}_{q^n})$ in an expected $e^{O(\log(q^n)^{2/3})}$ bit operations.

15.9 Further Results

To end the chapter we briefly mention some methods for non-hyperelliptic curves. It is beyond the scope of the book to present these algorithms in detail. We then briefly summarise the argument that there is no subexponential algorithm for the DLP on elliptic curves in general.

15.9.1 Diem's Algorithm for Plane Curves of Low Degree

Diem [175] used the Adleman-DeMarrais-Huang idea of generating relations using principal divisors $a(x) - yb(x)$ for the DLP on plane curves $F(x, y) = 0$ of low degree (the degree of such a curve is the total degree of $F(x, y)$ as a polynomial). Such curves are essentially the opposite case to hyperelliptic curves (which have rather high degree in x relative to their genus). The trick is simply to note that if $F(x, y)$ has relatively low degree compared to its genus then so does $b(x)^d F(x, a(x))$ and so the divisor of the function $a(x) - yb(x)$ has relatively low weight. The main result is an algorithm with heuristic complexity $\tilde{O}(q^{2-2/(d-2)})$ bit operations for a curve of degree d over $\mathbb{F}_q$.

In the case of non-singular plane quartics (genus 3 curves C over $\mathbb{F}_q$) Diem takes the factor base to be a large set of points $\mathcal{B} \subseteq C(\mathbb{F}_q)$. He generates relations by choosing two distinct points $P_1, P_2 \in \mathcal{B}$ and intersecting the line $y = bx + c$ between them with the curve C. There are two other points of intersection, corresponding to the roots of the quadratic polynomial $F(x, bx + c)/((x - x_{P_1})(x - x_{P_2}))$ and so with probability roughly $1/2$ we expect to get a relation in the divisor class group among points in $C(\mathbb{F}_q)$. Diem shows that the algorithm has complexity $\tilde{O}(q)$ bit operations.

Due to lack of space, and since our focus in this book is hyperelliptic curves (though, it is important to note that Smith [573] has given a reduction of the DLP from hyperelliptic curves of genus 3 to plane quartics) we do not present any further details. Interested readers should see [175, 178].

15.9.2 The Algorithm of Enge-Gaudry-Thomé and Diem

The algorithms for the DLP in the divisor class group of a hyperelliptic curve in Sections 15.6.1 and 15.6.2 had complexity $L_{q^g}(1/2, \sqrt{2} + o(1))$ bit operations as $q \to \infty$. A natural problem is to find algorithms with complexity $L_{q^g}(1/3, c + o(1))$, and this is still open in general. However, an algorithm is known for curves of the form $y^n + F(x, y) = 0$ where $\deg_y(F(x, y)) \leq n - 1$ and $\deg_x(F(x, y)) = d$ for $n \approx g^{1/3}$ and $d \approx g^{2/3}$. We do not have space to give the details, so simply quote the results and refer to Enge and Gaudry [196], Enge, Gaudry and Thomé [197] and Diem [174]. An algorithm to compute the group structure of $\mathrm{Pic}^0_C(\mathbb{F}_q)$ is given with heuristic complexity of $L_{q^g}(1/3, c + o(1))$

bit operations for some constant c. For the discrete logarithm problem the algorithm has heuristic complexity $L_{q^g}(1/3, c' + o(1))$ bit operations where c' is a constant.

Unlike the $L_N(1/3, c + o(1))$ algorithms for factoring or DLP in finite fields, the algorithm does not use two different factor bases. Instead, the algorithm is basically the same idea as Sections 15.6.2 and 15.9.1 with a complexity analysis tailored for curves of a certain form.

15.9.3 Index Calculus for General Elliptic Curves

In this section we briefly discuss why there does not seem to be a subexponential algorithm for the DLP on general elliptic curves.

An approach to an index calculus algorithm for elliptic curves was already discussed by Miller [428] in the paper that first proposed elliptic curves for cryptography. In particular he considered "lifting" an elliptic curve E over $\mathbb{F}_p$ to an elliptic curve $\widetilde{E}$ over $\mathbb{Q}$ (i.e., so that reducing the coefficients of $\widetilde{E}$ modulo p yields E). The factor base $\mathcal{B}$ was defined to be the points of small height (see Section VIII.6 of [564] for details of heights) in $\widetilde{E}(\mathbb{Q})$. The theory of descent (see Chapter VIII of Silverman [564]) essentially gives an algorithm to decompose a point as a sum of points of small height (when this is possible). The idea would therefore be to take random points $[a]P + [b]Q \in E(\mathbb{F}_p)$, lift them to $\widetilde{E}(\mathbb{Q})$ and then decompose them over the factor base. There are several obstructions to this method. First, lifting a random point from $E(\mathbb{F}_p)$ to $\widetilde{E}(\mathbb{Q})$ seems to be hard in general. Indeed, Miller argued (see also [566]) that there are very few points of small height in $\widetilde{E}(\mathbb{Q})$ and so (since we are considering random points $[a]P + [b]Q$ from the exponentially large set $E(\mathbb{F}_p)$) it would be necessary to lift to exponentially large points in $\widetilde{E}(\mathbb{Q})$. Second, the lifting itself seems to be a non-trivial computational task (essentially, solving a non-linear Diophantine equation over $\mathbb{Z}$).

Silverman proposed the **Xedni calculus** attack[11], which was designed to solve the lifting problem. This algorithm was analysed in [322], where it is shown that the probability of finding useful relations is too low.

By now, many people have tried and failed to discover an index calculus algorithm for the DLP on general elliptic curves. However, this does not prove that no such algorithm exists, or that a different paradigm could not lead to faster attacks on the elliptic curve DLP.

[11] "Xedni" is "Index" spelled backwards.

Part IV

Lattices

Chapter 16

Lattices

The word "lattice" has two different meanings in mathematics. One meaning is related to the theory of partial orderings on sets (for example, the lattice of subsets of a set). The other meaning, which is the one relevant to us, is discrete subgroups of $\mathbb{R}^n$.

There are several reasons for presenting lattices in this book. First, there are hard computational problems on lattices that have been used as a building block for public key cryptosystems (e.g., the Goldreich-Goldwasser-Halevi (GGH) cryptosystem, the NTRU cryptosystem, the Ajtai-Dwork cryptosystem, and the LWE cryptosystem); however, we do not present these applications in this book. Second, lattices are used as a fundamental tool for cryptanalysis of public key cryptosystems (e.g., lattice attacks on knapsack cryptosystems, Coppersmith's method for finding small solutions to polynomial equations, attacks on signatures, and attacks on variants of RSA). Third, there are applications of lattices to efficient implementation of discrete logarithm systems (such as the GLV method; see Section 11.3.3). Finally, lattices are used as a theoretical tool for security analysis of cryptosystems, for example the bit security of Diffie-Hellman key exchange using the hidden number problem (see Section 21.7) and the security proofs for RSA-OAEP.

Some good references for lattices, applications of lattices and/or lattice reduction algorithms are: Cassels [122], Siegel [563], Cohen [136], von zur Gathen and Gerhard [238], Grötschel, Lovász and Schrijver [269], Nguyen and Stern [462, 463], Micciancio and Goldwasser [422], Hoffstein, Pipher and Silverman [289], Lenstra's chapter in [113], Micciancio and Regev's chapter in [50] and the proceedings of the conference LLL+25.

Notation used in this part

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$	Integers, rational, real numbers
$\underline{b}, \underline{v}, \underline{w}$	Row vectors (usually in $\mathbb{R}^m$)
$\underline{0}$	Zero vector in $\mathbb{R}^m$
$\underline{e}_i$	i-th unit vector in $\mathbb{R}^m$
I_n	$n \times n$ identity matrix
$\langle \underline{x}, \underline{x} \rangle$	Inner product
$\|\underline{x}\|$	Euclidean length (ℓ_2 norm)
$\|\cdot\|_a$	ℓ_a-norm for $a \in \mathbb{N}$
$\text{span}\{\underline{v}_1, \ldots, \underline{v}_n\}$	Span of a set of vectors over $\mathbb{R}$
$\text{rank}(A)$	Rank of a matrix A
$\lfloor x \rceil$	Closest integer to x, $\lfloor 1/2 \rceil = 1$
B	Basis matrix for a lattice
L	Lattice
$\underline{b}_i^*$	Gram-Schmidt vector arising from ordered basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$
$\mu_{i,j}$	Gram-Schmidt coefficient $\langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$
B_i	$\|\underline{b}_i^*\|^2$
λ_i	Successive minima of a lattice
$\det(L)$	Determinant of a lattice
γ_n	Hermite's constant
X	Bound on the size of the entries in the basis matrix L
$B_{(i)}$	$i \times m$ matrix formed by the first i rows of B
d_i	Determinant of matrix of $\langle \underline{b}_j, \underline{b}_k \rangle$ for $1 \leq j, k \leq i$
D	Product of d_i
$\mathcal{P}_{1/2}(B)$	Fundamental domain (parallelepiped) for lattice basis B
$F(x)$, $F(x, y)$	Polynomial with "small" root
$G(x), G(x, y)$	Polynomial with "small" root in common with $F(x)$ (resp., $F(x, y)$)
X, Y	Bounds on size of root in Coppersmith's method
b_F	Coefficient vector of polynomial F
$R(F, G), R_x(F(x), G(x))$	Resultant of polynomials
W	Bound in Coppersmith's method
P, R	Constants in noisy Chinese remaindering
$\text{amp}(x)$	The amplitude $\gcd(P, x - R)$ in noisy Chinese remaindering
B, B'	Basis matrices for GGH encryption
I_n	$n \times n$ identity matrix
U	Invertible matrix disguising the private key in GGH
$\underline{m}$	Message in McEliece or GGH
$\underline{e}$	Error vector in McEliece or GGH
$\underline{c}$	Ciphertext in McEliece or GGH
σ	Entry in error vector in GGH
M	Size of coefficients in message in GGH
$\underline{s}$	GGH signature
$a_1, \ldots, a_n$	Subset sum weights
$b_1, \ldots, b_n$	Superincreasing sequence
$s = \sum_{i=1}^n x_i a_i$	The sum in a subset sum instance, with $x_i \in \{0, 1\}$
d	Density of a subset sum instance
π	Permutation of $\{1, \ldots, n\}$ used in the Merkle-Hellman cryptosystem
$\underline{\sigma}$	Vector in Nguyen attack
M	Modulus in Merkle-Hellman knapsack
W	Multiplier in Merkle-Hellman knapsack
U	$W^{-1} \pmod M$ in Merkle-Hellman
t	Number of iterations in iterated Merkle-Hellman knapsack

16.1 Basic Notions on Lattices

A lattice is a subset of the vector space $\mathbb{R}^m$. We write all vectors as **rows**; be warned that many books and papers write lattice vectors as columns. We denote by $\|\underline{v}\|$ the Euclidean norm of a vector $\underline{v} \in \mathbb{R}^m$; though some statements also hold for other norms.

Definition 16.1.1. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a linearly independent set of (row) vectors in $\mathbb{R}^m$ ($m \geq n$). The **lattice** generated by $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is the set

$$L = \left\{ \sum_{i=1}^{n} l_i \underline{b}_i \ : \ l_i \in \mathbb{Z} \right\}$$

of **integer** linear combinations of the $\underline{b}_i$. The vectors $\underline{b}_1, \ldots, \underline{b}_n$ are called a **lattice basis**. The **lattice rank** is n and the **lattice dimension** is m. If $n = m$ then L is said to be a **full rank lattice**.

Let $L \subset \mathbb{R}^m$ be a lattice. A **sublattice** is a subset $L' \subset L$ that is a lattice.

A **basis matrix** B of a lattice L is an $n \times m$ matrix formed by taking the rows to be basis vectors $\underline{b}_i$. Thus $B_{i,j}$ is the j-th entry of the row $\underline{b}_i$ and

$$L = \{\underline{x}B : \underline{x} \in \mathbb{Z}^n\}.$$

By assumption the rows of a basis matrix are always linearly independent.

Example 16.1.2. The lattice in $\mathbb{R}^2$ generated by $\{(1,0),(0,1)\}$ is $L = \mathbb{Z}^2$. The corresponding basis matrix is $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Any 2×2 integer matrix B of determinant ± 1 is also a basis matrix for L.

We will mainly assume that the basis vectors $\underline{b}_i$ for a lattice have integer entries. In cryptographic applications this is usually the case. We interchangeably use the words **points** and **vectors** for elements of lattices. The vectors in a lattice form an Abelian group under addition. When $n \geq 2$ there are infinitely many choices for the basis of a lattice.

An alternative approach to lattices is to define $L = \mathbb{Z}^n$ and to have a general length function $q(\underline{v})$. One finds this approach in books on quadratic forms or optimisation problems, e.g., Cassels [121] and Schrijver [531]. In particular, Section 6.2 of [531] presents the LLL algorithm in the context of reducing the lattice $L = \mathbb{Z}^n$ with respect to a length function corresponding to a positive-definite rational matrix.

We now give an equivalent definition of lattice, which is suitable for some applications. A subset $L \subseteq \mathbb{R}^m$ is called **discrete** if, for any real number $r > 0$, the set $\{\underline{v} \in L : \|\underline{v}\| \leq r\}$ is finite. It is clear that a lattice is a subgroup of $\mathbb{R}^m$ that is discrete. The following result shows the converse.

Lemma 16.1.3. *Every discrete subgroup of $\mathbb{R}^m$ is a lattice.*

Proof: (Sketch) Let $\{\underline{v}_1, \ldots, \underline{v}_n\}$ be a linearly independent subset of L of maximal size. The result is proved by induction. The case $n = 1$ is easy (since L is discrete there is an element of minimal non-zero length). When $n > 1$ consider $V = \text{span}\{\underline{v}_1, \ldots, \underline{v}_{n-1}\}$ and set $L' = L \cap V$. By induction, L' is a lattice and so has a basis $\underline{b}_1, \ldots, \underline{b}_{n-1}$. The set $L \cap \{\sum_{i=1}^{n-1} x_i \underline{b}_i + x_n \underline{v}_n : 0 \leq x_i < 1 \text{ for } 1 \leq i \leq n-1 \text{ and } 0 < x_n \leq 1\}$ is finite and so has an element with smallest x_n, call it $\underline{b}_n$. It can be shown that $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is a basis for L. For full details see Theorem 6.1 of [586]. □

Exercise 16.1.4. Given an $m \times n$ integer matrix A show that $\ker(A) = \{\underline{x} \in \mathbb{Z}^m : \underline{x}A = \underline{0}\}$ is a lattice. Show that the rank of the lattice is $m - \text{rank}(A)$. Given an $m \times n$ integer matrix A and an integer M show that $\{\underline{x} \in \mathbb{Z}^m : \underline{x}A \equiv \underline{0} \pmod{M}\}$ is a lattice of rank m.

In the case $m > n$ it is sometimes convenient to project the lattice L into $\mathbb{R}^n$ using the following construction. The motivation is that a linear map that preserves lengths preserves volumes. Note that if the initial basis for L consists of vectors in $\mathbb{Z}^n$ then the resulting basis does not necessarily have this property.

Lemma 16.1.5. *Let B be an $n \times m$ basis matrix for a lattice L where $m > n$. Then there is a linear map $P : \mathbb{R}^m \to \mathbb{R}^n$ such that $P(L)$ is a rank n lattice and $\|P(\underline{v})\| = \|\underline{v}\|$ for all $\underline{v} \in L$. Furthermore, $\langle \underline{b}_i, \underline{b}_j \rangle = \langle P(\underline{b}_i), P(\underline{b}_j) \rangle$ for all $1 \le i < j \le n$.*

If the linear map is represented by an $m \times n$ matrix P so that $P(\underline{v}) = \underline{v}P$ then a basis matrix for the image of L under the projection P is the $n \times n$ matrix BP, which is invertible.

Proof: Given the $n \times m$ basis matrix B with rows $\underline{b}_i$, define $V = \text{span}\{\underline{b}_1, \ldots, \underline{b}_n\} \subset \mathbb{R}^m$, which has dimension n by assumption. Choose (perhaps by running the Gram-Schmidt algorithm) a basis $\underline{v}_1, \ldots, \underline{v}_n$ for V that is orthonormal with respect to the inner product in $\mathbb{R}^m$. Define the linear map $P : V \to \mathbb{R}^n$ by $P(\underline{v}_i) = \underline{e}_i$ and $P(V^\perp) = \{0\}$. For $\underline{v} = \sum_{i=1}^n x_i \underline{v}_i \in V$ we have $\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle} = \sqrt{\sum_{i=1}^n x_i^2} = \|\underline{v}P\|$. Since the vectors $\underline{b}_i$ form a basis for V, the vectors $P(\underline{b}_i) = \underline{b}_i P$ are linearly independent. Hence, BP is an invertible matrix and $P(L)$ is a lattice of rank n. □

We can now prove the following fundamental result.

Lemma 16.1.6. *Two $n \times m$ matrices B and B' generate the same lattice L if and only if B and B' are related by a **unimodular matrix**, i.e., $B' = UB$ where U is an $n \times n$ matrix with integer entries and determinant ± 1.*

Proof: ($\Rightarrow$) Every row of B' is an integer linear combination

$$\underline{b}'_i = \sum_{j=1}^n u_{i,j} \underline{b}_j$$

of the rows in B. This can be represented as $B' = UB$ for an $n \times n$ integer matrix U.

Similarly, $B = U'B' = U'UB$. Now applying the projection P of Lemma 16.1.5 we have $BP = U'UBP$ and, since BP is invertible, $U'U = I_n$ (the identity matrix). Since U and U' have integer entries it follows that $\det(U), \det(U') \in \mathbb{Z}$. From $\det(U)\det(U') = \det(I_n) = 1$ it follows that $\det(U) = \pm 1$.

($\Leftarrow$) Since U is a permutation of $\mathbb{Z}^n$ we have $\{\underline{x}B' : \underline{x} \in \mathbb{Z}^n\} = \{\underline{x}B : \underline{x} \in \mathbb{Z}^n\}$. □

The Hermite normal form is defined in Section A.11. The following result is a direct consequence of Lemma 16.1.6 and the remarks in Section A.11.

Lemma 16.1.7. *If B is the basis matrix of a lattice L then the Hermite normal form of B is also a basis matrix for L.*

The **determinant** of a lattice L is the volume of the fundamental parallelepiped of any basis B for L. When the lattice has full rank then using Definition A.10.7 and Lemma A.10.8 we have $\det(L) = |\det(B)|$. For the case $n < m$ our definition uses Lemma 16.1.5.

Definition 16.1.8. Let the notation be as above. The **determinant** (or **volume**) of a lattice L with basis matrix B is $|\det(BP)|$, where P is a matrix representing the projection of Lemma 16.1.5.

Lemma 16.1.9. *The determinant of a lattice is independent of the choice of basis matrix B and the choice of projection P.*

Proof: Let P and P' be two projection matrices corresponding to orthogonal bases $\{\underline{v}_1, \ldots, \underline{v}_n\}$ and $\{\underline{v}'_1, \ldots, \underline{v}'_n\}$ for $V = \text{span}\{\underline{b}_1, \ldots, \underline{b}_n\}$. Then, by Lemma A.10.3, $P' = PW$ for some orthogonal matrix W (hence $\det(W) = \pm 1$). It follows that $|\det(BP)|$ does not depend on the choice of P.

Let B and B' be two basis matrices for a lattice L. Then $B' = UB$ where U is an $n \times n$ matrix such that $\det(U) = \pm 1$. Then $\det(L) = |\det(BP)| = |\det(UBP)| = |\det(B'P)|$. □

We have seen that there are many different choices of basis for a given lattice L. A fundamental problem is to compute a "nice" lattice basis for L; specifically one where the vectors are relatively short and close to orthogonal. The following exercise shows that these properties are intertwined.

Exercise 16.1.10. Let L be a rank 2 lattice in $\mathbb{R}^2$ and let $\{\underline{b}_1, \underline{b}_2\}$ be a basis for L.

1. Show that
$$\det(L) = \|\underline{b}_1\| \|\underline{b}_2\| |\sin(\theta)| \tag{16.1}$$
where θ is the angle between $\underline{b}_1$ and $\underline{b}_2$.

2. Hence deduce that the product $\|\underline{b}_1\| \|\underline{b}_2\|$ is minimised over all choices $\{\underline{b}_1, \underline{b}_2\}$ of basis for L when the angle θ is closest to $\pm\pi/2$.

Definition 16.1.11. Let L be a lattice in $\mathbb{R}^m$ of rank n with basis matrix B. The **Gram matrix** of B is BB^T. This is an $n \times n$ matrix whose (i,j)th entry is $\langle \underline{b}_i, \underline{b}_j \rangle$.

Lemma 16.1.12. *Let L be a lattice in $\mathbb{R}^m$ of rank n with basis matrix B. Then* $\det(L) = \sqrt{\det(BB^T)}$.

Proof: Consider first the case where $m = n$. Then $\det(L)^2 = \det(B)\det(B^T) = \det(BB^T) = \det((\langle \underline{b}_i, \underline{b}_j \rangle)_{i,j})$. Hence, when $m > n$ and $B' = BP$, $\det(L) = |\det(B')| = \sqrt{\det(B'(B')^T)}$. Now, the (i,j)th entry of $B'(B')^T = (BP)(BP)^T$ is $\langle \underline{b}_i P, \underline{b}_j P \rangle$, which is equal to the (i,j)th entry of BB^T by Lemma 16.1.5. The result follows. □

Note that an integer lattice of non-full rank may not have integer determinant.

Exercise 16.1.13. Find an example of a lattice of rank 1 in $\mathbb{Z}^2$ whose determinant is not an integer.

Lemma 16.1.14. *Let $\underline{b}_1, \ldots, \underline{b}_n$ be an ordered basis for a lattice L in $\mathbb{R}^m$ and let $\underline{b}^*_1, \ldots, \underline{b}^*_n$ be the Gram-Schmidt orthogonalisation. Then* $\det(L) = \prod_{i=1}^n \|\underline{b}^*_i\|$.

Proof: The case $m = n$ is already proved in Lemma A.10.8. For the general case let $\underline{v}_i = \underline{b}^*_i / \|\underline{b}^*_i\|$ be the orthonormal basis required for the construction of the projection P. Then $P(\underline{b}^*_i) = \|\underline{b}^*_i\| \underline{e}_i$. Write B and B^* for the $n \times m$ matrices formed by the rows $\underline{b}_i$ and $\underline{b}^*_i$ respectively. It follows that B^*P is an $n \times n$ diagonal matrix with diagonal entries $\|\underline{b}^*_i\|$. Finally, by the Gram-Schmidt construction, $B^* = UB$ for some $n \times n$ matrix U such that $\det(U) = 1$. Combining these facts gives[1]

$$\det(L) = |\det(BP)| = |\det(UBP)| = |\det(B^*P)| = \prod_{i=1}^n \|\underline{b}^*_i\|.$$

□

[1]The formula $BP = U^{-1}(B^*P)$ is the QR decomposition of BP.

Exercise 16.1.15. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an ordered lattice basis in $\mathbb{R}^m$ and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation. Show that $\|\underline{b}_i\| \geq \|\underline{b}_i^*\|$ and hence $\det(L) \leq \prod_{i=1}^n \|\underline{b}_i\|$.

Definition 16.1.16. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a basis for a lattice L in $\mathbb{R}^m$. The **orthogonality defect** of the basis is

$$\left(\prod_{i=1}^n \|\underline{b}_i\| \right) / \det(L).$$

Exercise 16.1.17. Show that the orthogonality defect of $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is 1 if and only if the basis is orthogonal.

Definition 16.1.18. Let $L \subset \mathbb{R}^m$ be a lattice of rank n. The **successive minima** of L are $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that, for $1 \leq i \leq n$, λ_i is minimal such that there exist i linearly independent vectors $\underline{v}_1, \ldots, \underline{v}_i \in L$ with $\|\underline{v}_j\| \leq \lambda_i$ for $1 \leq j \leq i$.

It follows that $0 < \lambda_1 \leq \lambda_2 \cdots \leq \lambda_n$. In general there is not a basis consisting of vectors whose lengths are equal to the successive minima, as the following example shows.

Example 16.1.19. Let $L \subset \mathbb{Z}^n$ be the set

$$L = \{(x_1, \ldots, x_n) : x_1 \equiv x_2 \equiv \cdots \equiv x_n \pmod 2\}.$$

It is easy to check that this is a lattice. The vectors $2\underline{e}_i \in L$ for $1 \leq i \leq n$ are linearly independent and have length 2. Every other vector $\underline{x} \in L$ with even entries has length ≥ 2. Every vector $\underline{x} \in L$ with odd entries has all $x_i \neq 0$ and so $\|\underline{x}\| \geq \sqrt{n}$.

If $n = 2$ the successive minima are $\lambda_1 = \lambda_2 = \sqrt{2}$ and if $n = 3$ the successive minima are $\lambda_1 = \lambda_2 = \lambda_3 = \sqrt{3}$. When $n \geq 4$ then $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 2$. For $n \leq 4$ one can construct a basis for the lattice with vectors of lengths equal to the successive minima. When $n > 4$ there is no basis for L consisting of vectors of length 2, since a basis must contain at least one vector having odd entries.

Exercise 16.1.20. For $n = 2, 3, 4$ in Example 16.1.19 write down a basis for the lattice consisting of vectors of lengths equal to the successive minima.

Exercise 16.1.21. For $n > 4$ in Example 16.1.19 show there is a basis for the lattice such that $\|\underline{b}_i\| = \lambda_i$ for $1 \leq i < n$ and $\|\underline{b}_n\| = \sqrt{n}$.

Definition 16.1.22. Let $L \subseteq \mathbb{R}^m$ be a lattice and write $V \subseteq \mathbb{R}^m$ for the $\mathbb{R}$-vector space spanned by the vectors in L. The **dual lattice** of L is $L^* = \{\underline{y} \in V : \langle \underline{x}, \underline{y} \rangle \in \mathbb{Z} \text{ for all } \underline{x} \in L\}$.

Exercise 16.1.23. Show that the dual lattice is a lattice. Let B be a basis matrix of a full rank lattice L. Show that $(B^T)^{-1}$ is a basis matrix for the dual lattice. Hence, show that the determinant of the dual lattice is $\det(L)^{-1}$.

16.2 The Hermite and Minkowski Bounds

We state the following results without rigorously defining the term "volume" and without giving proofs (see Section 1.3 of Micciancio and Goldwasser [422], Chapter 1 of Siegel [563], Chapter 6 of Hoffstein, Pipher and Silverman [289] or Chapter 12 of Cassels [121] for details).

Theorem 16.2.1. *(Blichfeldt) Let L be a lattice in $\mathbb{R}^m$ with basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ and S any measurable set such that $S \subset \text{span}\{\underline{b}_i : 1 \leq i \leq n\}$. If the volume of S exceeds $\det(L)$ then there exist two distinct points $\underline{v}_1, \underline{v}_2 \in S$ such that $(\underline{v}_1 - \underline{v}_2) \in L$.*

Proof: See Theorem 1.3 of [422] or Section III.2.1 of [121]. □

Theorem 16.2.2. *(Minkowski convex body theorem) Let L be a lattice in $\mathbb{R}^m$ with basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ and let S be any convex set such that $S \subset \text{span}\{\underline{b}_i : 1 \leq i \leq n\}$, $\underline{0} \in S$ and if $\underline{v} \in S$ then $-\underline{v} \in S$. If the volume of S is $> 2^n \det(L)$ then there exists a non-zero lattice point $\underline{v} \in S \cap L$.*

Proof: See Section III.2.2 of Cassels [121], Theorem 6.28 of Hoffstein, Pipher and Silverman [289], Theorem 1.4 of Micciancio and Goldwasser [422], or Theorem 6.1 of Stewart and Tall [586]. □

The convex body theorem is used to prove Theorem 16.2.3. The intuition behind this result is that if the shortest non-zero vector in a lattice is large then the volume of the lattice cannot be small.

Theorem 16.2.3. *Let $n \in \mathbb{N}$. There is a constant $0 < \gamma_n \leq n$ such that, for any lattice L of rank n in $\mathbb{R}^n$ having first minimum λ_1 (for the Euclidean norm),*

$$\lambda_1^2 < \gamma_n \det(L)^{2/n}.$$

Proof: See Theorem 1.5 of [422], Theorem 6.25 of [289], or Theorem 12.2.1 of [121]. □

Exercise 16.2.4. Show that the convex body theorem is tight. In other words find a lattice L in $\mathbb{R}^n$ for some n and a symmetric convex subset $S \subseteq \mathbb{R}^n$ such that the volume of S is $2^n \det(L)$ and yet $S \cap L = \{0\}$.

Exercise 16.2.5. Show that, with respect to the ℓ_∞ norm, $\lambda_1 \leq \det(L)^{1/n}$. Show that, with respect to the ℓ_1 norm, $\lambda_1 \leq (n! \det(L))^{1/n} \approx n \det(L)^{1/n}/e$.

Exercise 16.2.6.★ Let $a, b \in \mathbb{N}$. Show that there is a solution $r, s, t \in \mathbb{Z}$ to $r = as + bt$ such that $s^2 + r^2 \leq \sqrt{2}b$.

Definition 16.2.7. Let $n \in \mathbb{N}$. The smallest real number γ_n such that

$$\lambda_1^2 \leq \gamma_n \det(L)^{2/n}$$

for all lattices L of rank n is called the **Hermite constant**.

Exercise 16.2.8. This exercise is to show that $\gamma_2 = 2/\sqrt{3}$.

1. Let $\{\underline{b}_1, \underline{b}_2\}$ be a Lagrange-Gauss reduced basis (see Definition 17.1.1 of the next Section) for a dimension 2 lattice in $\mathbb{R}^2$. Define the quadratic form $N(x, y) = \|x\underline{b}_1 + y\underline{b}_2\|^2$. Show that, without loss of generality, $N(x, y) = ax^2 + 2bxy + cy^2$ with $a, b, c \geq 0$ and $a \leq c$.

2. Using $N(1, -1) \geq N(0, 1)$ (which follows from the property of being Lagrange-Gauss reduced), show that $2b \leq a$. Hence show that $3ac \leq 4(ac - b^2)$

3. Show that $\det(L)^2 = |b^2 - ac|$. Hence deduce that Hermite's constant satisfies $\gamma_2 \leq 2/\sqrt{3}$.

4. Show that the lattice $L \subset \mathbb{R}^2$ with basis $\{(1,0),(-1/2,\sqrt{3}/2)\}$ satisfies $\lambda_1^2 = (2/\sqrt{3})\det(L)$.

   (Optional) Show that L is equal to the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$. Show that centering balls of radius $1/2$ at each point of L gives the most dense lattice packing of balls in $\mathbb{R}^2$.

Section 6.5.2 of Nguyen [456] lists the first 8 values of γ_n, gives the bound $\frac{n}{2\pi e}+o(1) \leq \gamma_n \leq \frac{n}{\pi e}(1+o(1))$ and gives further references.

Theorem 16.2.9. *(Minkowski) Let L be a lattice of rank n in $\mathbb{R}^n$ with successive minima $\lambda_1,\ldots,\lambda_n$ for the Euclidean norm. Then*

$$\left(\prod_{i=1}^{n}\lambda_i\right)^{1/n} < \sqrt{n}\det(L)^{1/n}.$$

Proof: See Theorem 12.2.2 of [121]. (The term $\sqrt{n}$ can be replaced by $\sqrt{\gamma_n}$.) □

The **Gaussian heuristic** states that the shortest non-zero vector in a "random" lattice L of dimension n in $\mathbb{R}^n$ is expected to have length approximately

$$\sqrt{\frac{n}{2\pi e}}\det(L)^{1/n}.$$

We refer to Section 6.5.3 of [456] and Section 6.5.3 of [289] for discussion and references.

16.3 Computational Problems in Lattices

There are several natural computational problems relating to lattices. We start by listing some problems that can be efficiently solved using linear algebra (in particular, the Hermite normal form).

1. **lattice membership**: Given an $n \times m$ basis matrix B for a lattice $L \subseteq \mathbb{Z}^m$ and a vector $\underline{v} \in \mathbb{Z}^m$ determine whether $\underline{v} \in L$.

2. **lattice basis**: Given a set of vectors $\underline{b}_1,\ldots,\underline{b}_n$ in $\mathbb{Z}^m$ (possibly linearly dependent) find a basis for the lattice generated by them.

3. **kernel lattice**: Given an $m \times n$ integer matrix A compute a basis for the lattice $\ker(A) = \{\underline{x} \in \mathbb{Z}^m : \underline{x}A = \underline{0}\}$.

4. **kernel lattice modulo** M: Given an $m \times n$ integer matrix A and an integer M compute a basis for the lattice $\{\underline{x} \in \mathbb{Z}^m : \underline{x}A \equiv \underline{0} \pmod{M}\}$.

Exercise 16.3.1.★ Describe explicit algorithms for the above problems and determine their complexity.

Now we list some computational problems that seem to be hard in general.

Definition 16.3.2. Let L be a lattice in $\mathbb{Z}^m$.

1. The **shortest vector problem (SVP)** is the computational problem: given a basis matrix B for L, compute a non-zero vector $\underline{v} \in L$ such that $\|\underline{v}\|$ is minimal (i.e., $\|\underline{v}\| = \lambda_1$).

2. The **closest vector problem (CVP)** is the computational problem: given a basis matrix B for L and a vector $\underline{w} \in \mathbb{Q}^m$ (one can work with high-precision approximations in $\mathbb{R}^m$, but this is essentially still working in $\mathbb{Q}^m$), compute $v \in L$ such that $\|\underline{w} - \underline{v}\|$ is minimal.

3. The **decision closest vector problem (DCVP)** is: given a basis matrix B for a lattice L, a vector $\underline{w} \in \mathbb{Q}^m$ and a real number $r > 0$, decide whether or not there is a vector $\underline{v} \in L$ such that $\|\underline{w} - \underline{v}\| \leq r$.

4. The **decision shortest vector problem** is: given a basis matrix B for a lattice L and a real number $r > 0$ to decide whether or not there is a non-zero $\underline{v} \in L$ such that $\|\underline{v}\| \leq r$.

5. Fix $\gamma > 1$. The **approximate SVP problem** is: given a basis matrix B for L, compute a non-zero vector $\underline{v} \in L$ such that $\|\underline{v}\| \leq \gamma\lambda_1$.

6. Fix $\gamma > 1$. The **approximate CVP problem** is: given a basis matrix B for L and a vector $\underline{w} \in \mathbb{Q}^m$, compute $\underline{v} \in L$ such that $\|\underline{w} - \underline{v}\| \leq \gamma\|\underline{w} - \underline{x}B\|$ for all $\underline{x} \in \mathbb{Z}^n$.

7. Fix $0 < \alpha < 1$. The **bounded distance decoding problem (BDD)** is: given a basis matrix B for a lattice L and a vector $\underline{w} \in \mathbb{Q}^m$ such that there is a lattice point $\underline{v} \in L$ with $\|\underline{w} - \underline{v}\| \leq \alpha\lambda_1(L)$, to compute $\underline{v}$. In other words, this is a CVP instance that is especially close to a lattice point.

In general, these computational problems are known to be hard[2] when the rank is sufficiently large. It is known that CVP is NP-hard (this is shown by relating CVP with subset-sum; for details see Chapter 3 of [422]). Also, SVP is NP-hard under randomised reductions and non-uniform reductions (see Chapter 4 of [422] for explanation of these terms and proofs). Nguyen [456] gives a summary of the complexity results and current best running times of algorithms for these problems.

On the other hand, if a lattice is sufficiently nice then these problems may be easy.

Example 16.3.3. Let $L \subset \mathbb{R}^2$ be the lattice with basis matrix

$$B = \begin{pmatrix} 1001 & 0 \\ 0 & 2008 \end{pmatrix}.$$

Then every lattice vector is of the form $(1001a, 2008b)$ where $a, b \in \mathbb{Z}$. Hence the shortest non-zero vectors are clearly $(1001, 0)$ and $(-1001, 0)$. Similarly, the closest vector to $\underline{w} = (5432, 6000)$ is clearly $(5005, 6024)$.

Why is this example so easy? The reason is that the basis vectors are orthogonal. Even in large dimensions, the SVP and CVP problems are easy if one has an orthogonal basis for a lattice. When given a basis that is not orthogonal it is less obvious whether there exists a non-trivial linear combination of the basis vectors that gives a vector strictly shorter than the shortest basis vector. A basis for a lattice that is "as close to orthogonal as it can be" is therefore convenient for solving some computational problems.

[2]We do not give details of complexity theory in this book; in particular we do not define the term "NP-hard".

Chapter 17

Lattice Basis Reduction

The goal of lattice basis reduction is to transform a given lattice basis into a "nice" lattice basis consisting of vectors that are short and close to orthogonal. To achieve this one needs both a suitable mathematical definition of "nice basis" and an efficient algorithm to compute a basis satisfying this definition.

Reduction of lattice bases of rank 2 in $\mathbb{R}^2$ was given by Lagrange[1] and Gauss. The algorithm is closely related to Euclid's algorithm and we briefly present it in Section 17.1. The main goal of this section is to present the lattice basis reduction algorithm of Lenstra, Lenstra and Lovász, known as the LLL or L^3 algorithm.[2] This is a very important algorithm for practical applications. Some basic references for the LLL algorithm are Section 14.3 of Smart [572], Section 2.6 of Cohen [136] and Chapter 17 of Trappe and Washington [609]. More detailed treatments are given in von zur Gathen and Gerhard [238], Grötschel, Lovász and Schrijver [269], Section 1.2 of Lovász [395], and Nguyen and Vallée [464]. I also highly recommend the original paper [373].

The LLL algorithm generalises the Lagrange-Gauss algorithm and exploits the Gram-Schmidt orthogonalisation. Note that the Gram-Schmidt process is not useful, in general, for lattices since the coefficients $\mu_{i,j}$ do not usually lie in $\mathbb{Z}$ and so the resulting vectors are not usually elements of the lattice. The LLL algorithm uses the Gram-Schmidt vectors to determine the quality of the lattice basis, but ensures that the linear combinations used to update the lattice vectors are all over $\mathbb{Z}$.

17.1 Lattice Basis Reduction in Two Dimensions

Let $\underline{b}_1, \underline{b}_2 \in \mathbb{R}^2$ be linear independent vectors and denote by L the lattice for which they are a basis. The goal is to output a basis for the lattice such that the lengths of the basis

[1] The algorithm was first written down by Lagrange and later by Gauss, but is usually called the "Gauss algorithm". We refer to [455] or Chapter 2 of [464] for the original references.

[2] Chapter 1 of [464] gives an excellent survey of the historical development of the algorithm.

vectors are as short as possible (in this case, successive minima). Lagrange and Gauss gave the following criteria for a basis to be reduced and then developed Algorithm 23 to compute such a basis.

Definition 17.1.1. An ordered basis $\underline{b}_1, \underline{b}_2$ for $\mathbb{R}^2$ is **Lagrange-Gauss reduced** if $\|\underline{b}_1\| \leq \|\underline{b}_2\| \leq \|\underline{b}_2 + q\underline{b}_1\|$ for all $q \in \mathbb{Z}$.

The following theorem shows that the vectors in a Lagrange-Gauss reduced basis are as short as possible. This result holds for any norm, though the algorithm presented below is only for the Euclidean norm.

Theorem 17.1.2. *Let λ_1, λ_2 be the successive minima of L. If L has an ordered basis $\{\underline{b}_1, \underline{b}_2\}$ that is Lagrange-Gauss reduced then $\|\underline{b}_i\| = \lambda_i$ for $i = 1, 2$.*

Proof: By definition we have

$$\|\underline{b}_2 + q\underline{b}_1\| \geq \|\underline{b}_2\| \geq \|\underline{b}_1\|$$

for all $q \in \mathbb{Z}$.

Let $\underline{v} = l_1\underline{b}_1 + l_2\underline{b}_2$ be any non-zero point in L. If $l_2 = 0$ then $\|\underline{v}\| \geq \|\underline{b}_1\|$. If $l_2 \neq 0$ then write $l_1 = ql_2 + r$ with $q, r \in \mathbb{Z}$ such that $0 \leq r < |l_2|$. Then $\underline{v} = r\underline{b}_1 + l_2(\underline{b}_2 + q\underline{b}_1)$ and, by the triangle inequality

$$\begin{aligned} \|\underline{v}\| &\geq |l_2|\,\|\underline{b}_2 + q\underline{b}_1\| - r\|\underline{b}_1\| \\ &= (|l_2| - r)\|\underline{b}_2 + q\underline{b}_1\| + r(\|\underline{b}_2 + q\underline{b}_1\| - \|\underline{b}_1\|) \\ &\geq \|\underline{b}_2 + q\underline{b}_1\| \geq \|\underline{b}_2\| \geq \|\underline{b}_1\|. \end{aligned}$$

This completes the proof. □

Definition 17.1.3. Let $\underline{b}_1, \ldots, \underline{b}_n$ be a list of vectors in $\mathbb{R}^n$. We write[3] $B_i = \|\underline{b}_i\|^2 = \langle \underline{b}_i, \underline{b}_i \rangle$.

A crucial ingredient for the Lagrange-Gauss algorithm is that

$$\|\underline{b}_2 - \mu\underline{b}_1\|^2 = B_2 - 2\mu\langle \underline{b}_1, \underline{b}_2 \rangle + \mu^2 B_1 \tag{17.1}$$

is minimised at $\mu = \langle \underline{b}_1, \underline{b}_2 \rangle / B_1$ (to see this, note that the graph as a function of μ is a parabola and that the minimum can be found by differentiating with respect to μ). Since we are working in a lattice we therefore replace $\underline{b}_2$ by $\underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$ where $\lfloor \mu \rceil$ is the nearest integer to μ. Hence lines 3 and 9 of Algorithm 23 reduce the size of $\underline{b}_2$ as much as possible using $\underline{b}_1$. In the one-dimensional case the formula $\underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$ is the familiar operation $r_{i+1} = r_{i-1} - \lfloor r_{i-1}/r_i \rceil r_i$ from Euclid's algorithm.

Lemma 17.1.4. *An ordered basis $\{\underline{b}_1, \underline{b}_2\}$ is Lagrange-Gauss reduced if and only if*

$$\|\underline{b}_1\| \leq \|\underline{b}_2\| \leq \|\underline{b}_2 \pm \underline{b}_1\|.$$

Proof: The forward implication is trivial. For the converse, suppose $\|\underline{b}_2\| \leq \|\underline{b}_2 \pm \underline{b}_1\|$. We use the fact that the graph of $F(\mu) = \|\underline{b}_2 + \mu\underline{b}_1\|^2$ is a parabola. It follows that the miniumum of $F(\mu)$ is taken for $-1 < \mu < 1$. Hence $\|\underline{b}_2\| \leq \|\underline{b}_2 + q\underline{b}_1\|$ for $q \in \mathbb{Z}$ such that $|q| > 1$. □

Algorithm 23 gives the Lagrange-Gauss algorithm for lattices in $\mathbb{Z}^2$. Note that the computation of μ is as an exact value in $\mathbb{Q}$. All other arithmetic is exact integer arithmetic.

[3]The reader is warned that the notation B_i will have a different meaning when we are discussing the LLL algorithm.

Algorithm 23 Lagrange-Gauss lattice basis reduction

INPUT: Basis $\underline{b}_1, \underline{b}_2 \in \mathbb{Z}^2$ for a lattice L
OUTPUT: Basis $(\underline{b}_1, \underline{b}_2)$ for L such that $\|\underline{b}_i\| = \lambda_i$

```
B_1 = ||b_1||^2
μ = ⟨b_1, b_2⟩/B_1
b_2 = b_2 − ⌊μ⌉ b_1
B_2 = ||b_2||^2
while B_2 < B_1 do
    Swap b_1 and b_2
    B_1 = B_2
    μ = ⟨b_1, b_2⟩/B_1
    b_2 = b_2 − ⌊μ⌉ b_1
    B_2 = ||b_2||^2
end while
return (b_1, b_2)
```

Lemma 17.1.5. *Algorithm 23 terminates and outputs a Lagrange-Gauss reduced basis for the lattice L.*

Exercise 17.1.6. Prove Lemma 17.1.5.

Example 17.1.7. We run the Lagrange-Gauss algorithm on $\underline{b}_1 = (1, 5)$ and $\underline{b}_2 = (6, 21)$. In the first step, $\mu = 111/26 \approx 4.27$ and so we update $\underline{b}_2 = \underline{b}_2 - 4\underline{b}_1 = (2, 1)$. We then swap $\underline{b}_1$ and $\underline{b}_2$ so that the values in the loop are now $\underline{b}_1 = (2, 1)$ and $\underline{b}_2 = (1, 5)$. This time, $\mu = 7/5 = 1.4$ and so we set $\underline{b}_2 = \underline{b}_2 - \underline{b}_1 = (-1, 4)$. Since $\|\underline{b}_2\| > \|\underline{b}_1\|$ the algorithm halts and outputs $\{(2, 1), (-1, 4)\}$.

Exercise 17.1.8. Run the Lagrange-Gauss reduction algorithm on the basis $\{(3, 8), (5, 14)\}$.

Lemma 17.1.9. *Let $\underline{b}_1, \underline{b}_2$ be the initial vectors in an iteration of the Lagrange-Gauss algorithm and suppose $\underline{b}_1' = \underline{b}_2 - m\underline{b}_1$ and $\underline{b}_2' = \underline{b}_1$ are the vectors that will be considered in the next step of the algorithm. Then $\|\underline{b}_1'\|^2 < \|\underline{b}_1\|^2/3$, except perhaps for the last two iterations.*

Proof: Note that $m = \lfloor \mu \rceil = \lfloor \langle \underline{b}_1, \underline{b}_2 \rangle / \langle \underline{b}_1, \underline{b}_1 \rangle \rceil = \langle \underline{b}_1, \underline{b}_2 \rangle / \langle \underline{b}_1, \underline{b}_1 \rangle + \epsilon$ where $|\epsilon| \leq 1/2$. Hence,

$$\langle \underline{b}_1, \underline{b}_1' \rangle = \langle \underline{b}_1, \underline{b}_2 - (\langle \underline{b}_1, \underline{b}_2 \rangle / \langle \underline{b}_1, \underline{b}_1 \rangle + \epsilon)\, \underline{b}_1 \rangle = -\epsilon \langle \underline{b}_1, \underline{b}_1 \rangle = -\epsilon \|\underline{b}_1\|^2.$$

We show that $\|\underline{b}_1'\|^2 < \|\underline{b}_1\|^2/3$ unless we are in the last two iterations of the algorithm. To do this, suppose that $\|\underline{b}_1'\|^2 \geq \|\underline{b}_1\|^2/3$. Then

$$|\langle \underline{b}_1', \underline{b}_2' \rangle| = |\langle \underline{b}_1', \underline{b}_1 \rangle| = |\epsilon| \|\underline{b}_1\|^2 \leq \tfrac{1}{2} \|\underline{b}_1\|^2 \leq \tfrac{3}{2} \|\underline{b}_1'\|^2.$$

It follows that, in the next iteration of the algorithm, we will be taking $m = \lfloor \mu \rceil \in \{-1, 0, 1\}$ and so the next iteration would, at most, replace $\underline{b}_1'$ with $\underline{b}_2' \pm \underline{b}_1' = \underline{b}_1 \pm (\underline{b}_2 - m\underline{b}_1)$. But, if this were smaller than $\underline{b}_1'$ then we would have already computed $\underline{b}_1'$ differently in the current iteration. Hence, the next step is the final iteration. □

Theorem 17.1.10. *Let $X \in \mathbb{Z}_{\geq 2}$ and let $\underline{b}_1, \underline{b}_2$ be vectors in $\mathbb{Z}^2$ such that $\|\underline{b}_i\|^2 \leq X$. Then the Lagrange-Gauss algorithm performs $O(\log(X)^3)$ bit operations.*

Proof: Lemma 17.1.9 shows that there are $O(\log(X))$ iterations in the Lagrange-Gauss algorithm. Since the squared Euclidean lengths of all vectors in the algorithm are bounded by X, it follows that entries of vectors are integers bounded by $\sqrt{X}$. Similarly, the numerator and denominator of $\mu \in \mathbb{Q}$ require $O(\log(X))$ bits. The result follows. □

A much more precise analysis of the Lagrange-Gauss reduction algorithm is given by Vallée [614]. Indeed, the algorithm has complexity $O(\log(X)^2)$ bit operations; see Nguyen and Stehlé [455].

The above discussion is for the Euclidean norm, but the Lagrange-Gauss reduction algorithm can be performed for any norm (the only change is how one computes μ). We refer to Kaib and Schnorr [326] for analysis and details.

Finally, we remark that there is a natural analogue of Definition 17.1.1 for any dimension. Hence, it is natural to try to generalise the Lagrange-Gauss algorithm to higher dimensions. Generalisations to dimension three have been given by Vallée [613] and Semaev [538]. There are a number of problems when generalising to higher dimensions. For example, choosing the right linear combination to size reduce $\underline{b}_n$ using $\underline{b}_1, \ldots, \underline{b}_{n-1}$ is solving the CVP in a sublattice (which is a hard problem). Furthermore, there is no guarantee that the resulting basis actually has good properties in high dimension. We refer to Nguyen and Stehlé [461] for a full discussion of these issues and an algorithm that works in dimensions 3 and 4.

17.1.1 Connection Between Lagrange-Gauss Reduction and Euclid's Algorithm

The Lagrange-Gauss algorithm is closely related to Euclid's algorithm. We briefly discuss some similarities and differences. Recall that if $a, b \in \mathbb{Z}$ then Euclid's algorithm (using signed remainders) produces a sequence of integers r_i, s_i, t_i such that

$$as_i + bt_i = r_i$$

where $|r_i t_i| < |a|$ and $|r_i s_i| < |b|$. The precise formulae are $r_{i+1} = r_{i-1} - qr_i$ and $s_{i+1} = s_{i-1} - qs_i$ where $q = \lfloor r_{i-1}/r_i \rceil$. The sequence $|r_i|$ is strictly decreasing. The initial values are $r_{-1} = a, r_0 = b, s_{-1} = 1, s_0 = 0, t_{-1} = 0, t_0 = 1$. In other words the lattice with basis matrix

$$B = \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} = \begin{pmatrix} s_0 & r_0 \\ s_{-1} & r_{-1} \end{pmatrix}$$

contains the vectors

$$(s_i, r_i) = (t_i, s_i)B.$$

These vectors are typically shorter than the original vectors of the lattice.

We claim that if s_i is sufficiently small compared with r_i then one step of the Lagrange-Gauss algorithm on B corresponds to one step of Euclid's algorithm (with negative remainders).

To see this, let $\underline{b}_1 = (s_i, r_i)$ and consider the Lagrange-Gauss algorithm with $\underline{b}_2 = (s_{i-1}, r_{i-1})$. First compute the value

$$\mu = \frac{\langle \underline{b}_1, \underline{b}_2 \rangle}{\langle \underline{b}_1, \underline{b}_1 \rangle} = \frac{s_i s_{i-1} + r_i r_{i-1}}{s_i^2 + r_i^2}.$$

If s_i is sufficiently small relative to r_i (e.g., in the first step, when $s_0 = 0$) then

$$\lfloor \mu \rceil = \lfloor r_i r_{i-1} / r_i^2 \rceil = \lfloor r_{i-1}/r_i \rceil = q.$$

Hence the operation $\underline{v} = \underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$ is $\underline{v} = (s_{i-1} - qs_i, r_{i-1} - qr_i)$, which agrees with Euclid's algorithm. Finally, the Lagrange-Gauss algorithm compares the lengths of the vectors $\underline{v}$ and $\underline{b}_1$ to see if they should be swapped. When s_{i+1} is small compared with r_{i+1} then $\|\underline{v}\|$ is smaller than $\|b_1\|$. Hence the vectors are swapped and the matrix becomes

$$\begin{pmatrix} s_{i-1} - qs_i & r_{i-1} - qr_i \\ s_i & r_i \end{pmatrix}.$$

just as in Euclid's algorithm.

The algorithms start to deviate once s_i become large (this can already happen on the second iteration, as the below example shows). Further, Euclid's algorithm runs until $r_i = 0$ (in which case $s_i \approx b$) whereas Lagrange-Gauss reduction stops when $r_i \approx s_i$.

Example 17.1.11. Let $a = 19$ and $b = 8$. The sequence of remainders in the signed Euclidean algorithm is $3, -1$ while the Lagrange-Gauss lattice basis reduction algorithm computes remainders $3, 2$.

Example 17.1.12. Consider $a = 8239876$ and $b = 1020301$, which have gcd equal to one. Let

$$B = \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}.$$

Running the Lagrange-Gauss algorithm on this matrix gives

$$\begin{pmatrix} 540 & 379 \\ 619 & -1455 \end{pmatrix}.$$

One can verify that

$$379 = 540a + t_4 b \text{ where } t_4 = -4361$$

and

$$-1455 = 619a + t_5 b \text{ where } t_5 = -4999.$$

17.2 LLL-Reduced Lattice Bases

This section presents the crucial definition from [373] and some of its consequences. The main result is Theorem 17.2.12, which shows that an LLL-reduced lattice basis does have good properties.

Recall first that if $\underline{b}_1, \ldots, \underline{b}_n$ is a set of vectors in $\mathbb{R}^m$ then one can define the Gram-Schmidt orthogonalisation $\underline{b}_1^*, \ldots, \underline{b}_n^*$ as in Section A.10.2. We use the notation $\mu_{i,j} = \langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$ throughout.

As we have noted in Example 16.3.3, computational problems in lattices can be easy if one has a basis that is orthogonal, or "sufficiently close to orthogonal". A simple but important observation is that one can determine when a basis is close to orthogonal by considering the lengths of the Gram-Schmidt vectors. More precisely, a lattice basis is "close to orthogonal" if the lengths of the Gram-Schmidt vectors do not decrease too rapidly.

Example 17.2.1. Two bases for $\mathbb{Z}^2$ are $\{(1,0),(0,1)\}$ and $\{(23,24),(24,25)\}$. In the first case, the Gram-Schmidt vectors both have length 1. In the second case the Gram-Schmidt vectors are $\underline{b}_1^* = (23,24)$ and $\underline{b}_2^* = (24/1105, -23/1105)$, which have lengths $\sqrt{1105} \approx 33.24$ and $1/\sqrt{1105} \approx 0.03$ respectively. The fact that the lengths of the Gram-Schmidt vectors dramatically decrease reveals that the original basis is not of good quality.

We now list some easy properties of the Gram-Schmidt orthogonalisation.

Lemma 17.2.2. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be linearly independent in $\mathbb{R}^m$ and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation.*

1. *$\|\underline{b}_i^*\| \leq \|\underline{b}_i\|$ for $1 \leq i \leq n$.*
2. *$\langle \underline{b}_i, \underline{b}_i^* \rangle = \langle \underline{b}_i^*, \underline{b}_i^* \rangle$ for $1 \leq i \leq n$.*
3. *Let $j, k \in \mathbb{N}$ be such that $1 < k \leq n$ and $1 \leq j < k$. Denote the closest integer to $\mu_{k,j}$ by $\lfloor \mu_{k,j} \rceil$. If $\underline{b}_k' = \underline{b}_k - \lfloor \mu_{k,j} \rceil \underline{b}_j$ and $\mu_{k,j}' = \langle \underline{b}_k', \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$ then $|\mu_{k,j}'| \leq 1/2$.*

Exercise 17.2.3. Prove Lemma 17.2.2.

Definition 17.2.4. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an ordered basis for a lattice. Denote by $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ the Gram-Schmidt orthogonalisation and write $B_i = \|\underline{b}_i^*\|^2 = \langle \underline{b}_i^*, \underline{b}_i^* \rangle$. Let

$$\mu_{i,j} = \langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$$

for $1 \leq j < i \leq n$ be the coefficients from the Gram-Schmidt process. Fix $1/4 < \delta < 1$. The (ordered) basis is **LLL reduced** (with factor δ) if the following conditions hold:

- (Size reduced) $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$.
- (Lovász condition)
$$B_i \geq \left(\delta - \mu_{i,i-1}^2\right) B_{i-1}$$
for $2 \leq i \leq n$.

It is traditional to choose $\delta = 3/4$ in the Lovász condition.

Exercise 17.2.5. Which of the following basis matrices represents an LLL reduced basis (with $\delta = 3/4$)?

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 10 & 0 \\ 0 & 9 \end{pmatrix}.$$

Exercise 17.2.6. Prove that an equivalent formulation (more in the flavour of the Lagrange-Gauss method) of the Lovász condition is

$$B_i + \mu_{i,i-1}^2 B_{i-1} = \|\underline{b}_i^* + \mu_{i,i-1}\underline{b}_{i-1}^*\|^2 \geq \delta B_{i-1}.$$

Exercise 17.2.7. Find an ordered basis $\{\underline{b}_1, \underline{b}_2\}$ in $\mathbb{R}^2$ that is LLL-reduced, but has the property that $\|\underline{b}_2\| < \|\underline{b}_1\|$ and that the ordered basis $\{\underline{b}_2, \underline{b}_1\}$ is not LLL-reduced.

For the moment we do not concern ourselves with the question of whether an LLL reduced basis can exist for every lattice L. In Section 17.4 we will present the LLL algorithm, which constructs such a basis for any lattice (hence giving a constructive existence proof for an LLL reduced basis).

The following properties of an LLL reduced basis hold.

Lemma 17.2.8. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an LLL reduced basis with $\delta = 3/4$ for a lattice $L \subset \mathbb{R}^m$. Let the notation be as above. In particular, $\|\underline{b}\|$ is the Euclidean norm.*

1. *$B_j \leq 2^{i-j} B_i$ for $1 \leq j \leq i \leq n$.*
2. *$B_i \leq \|\underline{b}_i\|^2 \leq (\frac{1}{2} + 2^{i-2}) B_i$ for $1 \leq i \leq n$.*

3. $\|\underline{b}_j\| \leq 2^{(i-1)/2}\|\underline{b}_i^*\|$ *for* $1 \leq j \leq i \leq n$.

Proof:

1. The Lovász condition implies $B_i \geq (\frac{3}{4} - \frac{1}{4})B_{i-1} = \frac{1}{2}B_{i-1}$ and the result follows by induction.

2. From $\underline{b}_i = \underline{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j}\underline{b}_j^*$ we have

$$\begin{aligned} \|\underline{b}_i\|^2 &= \langle \underline{b}_i, \underline{b}_i \rangle \\ &= \left\langle \underline{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j}\underline{b}_j^* \ , \ \underline{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j}\underline{b}_j^* \right\rangle \\ &= B_i + \sum_{j=1}^{i-1} \mu_{i,j}^2 B_j, \end{aligned}$$

   which is clearly $\geq B_i$. By part 1 this is at most $B_i(1+\frac{1}{4}\sum_{j=1}^{i-1} 2^{i-j}) = B_i(1+\frac{1}{4}(2^i - 2)) = B_i(\frac{1}{2} + 2^{i-2})$.

3. Since $j \geq 1$ we have $\frac{1}{2} + 2^{j-2} \leq 2^{j-1}$. Part 2 can therefore be written as $\|b_j\|^2 \leq 2^{j-1}B_j$. By part 1, $B_j \leq 2^{i-j}B_i$ and so $\|b_j\|^2 \leq 2^{j-1}2^{i-j}B_i = 2^{i-1}B_i$. Taking square roots gives the result.

□

We now give the same result for a slightly different value of δ.

Lemma 17.2.9. *Let* $\{\underline{b}_1, \ldots, \underline{b}_n\}$ *be an LLL reduced basis with* $\delta = 1/4 + 1/\sqrt{2} \approx 0.957$ *for a lattice* $L \subset \mathbb{R}^m$. *Let the notation be as above. In particular,* $\|\underline{b}\|$ *is the Euclidean norm.*

1. $B_j \leq 2^{(i-j)/2}B_i$ *for* $1 \leq j \leq i \leq n$.
2. $B_i \leq \|\underline{b}_i\|^2 \leq (\frac{1}{6} + 2^{(i-1)/2})B_i$ *for* $1 \leq i \leq n$.
3. $\|\underline{b}_j\| \leq 2^{i/4}\|\underline{b}_i^*\|$ *for* $1 \leq j \leq i \leq n$.

Exercise 17.2.10.★ Prove Lemma 17.2.9.

Lemma 17.2.11. *Let* $\{\underline{b}_1, \ldots, \underline{b}_n\}$ *be an ordered basis for a lattice* $L \subset \mathbb{R}^m$ *and let* $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ *be the Gram-Schmidt orthogonalisation. Let* λ_1 *be the length of the shortest non-zero vector in the lattice. Then*

$$\lambda_1 \geq \min_{1 \leq i \leq n} \|\underline{b}_i^*\|.$$

Furthermore, let $\underline{w}_1, \ldots, \underline{w}_i \in L$ *be linearly independent lattice vectors such that* $\max\{\|\underline{w}_1\|, \ldots, \|\underline{w}_i\|\} = \lambda_i$, *as in the definition of successive minima. Write* $\underline{w}_j = \sum_{k=1}^{n} z_{j,k}\underline{b}_k$. *For* $1 \leq j \leq i$ *denote by* $k(j)$ *the largest value for* k *such that* $1 \leq k \leq n$ *and* $z_{j,k} \neq 0$. *Then* $\|\underline{w}_j\| \geq \|\underline{b}_{k(j)}^*\|$.

Proof: Let $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ be arbitrary such that $\underline{x} \neq \underline{0}$. Let i be the largest index such that $x_i \neq 0$. We will show that $\|\underline{x}B\| \geq \|b_i^*\|$, from which the result follows.

We have $\underline{x}B = \sum_{j=1}^{i} x_j\underline{b}_j$. Since $\underline{b}_i^*$ is orthogonal to the span of $\{\underline{b}_1, \ldots, \underline{b}_{i-1}\}$ we have $\langle \underline{x}B, \underline{b}_i^* \rangle = x_i\langle \underline{b}_i^*, \underline{b}_i^* \rangle = x_i\|\underline{b}_i^*\|^2$. Since $x_i \in \mathbb{Z}$ and $x_i \neq 0$ it follows that $|\langle \underline{x}B, \underline{b}_i^* \rangle| \geq \|\underline{b}_i^*\|^2$. By part 4 of Lemma A.10.3 it follows that

$$\|\underline{x}B\| \geq \|\underline{b}_i^*\|,$$

which completes the proof. □

Theorem 17.2.12 shows that an LLL reduced lattice basis has good properties. In particular, the first vector of an LLL-reduced lattice basis has length at most $2^{(n-1)/2}$ times the length of a shortest non-zero vector.

Theorem 17.2.12. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an LLL reduced basis with $\delta = 3/4$ for a lattice $L \subset \mathbb{R}^m$. Let the notation be as above. In particular, $\|\underline{b}\|$ is the Euclidean norm.*

1. $\|\underline{b}_1\| \leq 2^{(n-1)/2}\lambda_1$.
2. $\|\underline{b}_j\| \leq 2^{(n-1)/2}\lambda_i$ *for* $1 \leq j \leq i \leq n$. *(This may look strange, but it tends to be used for fixed i and varying j, rather than the other way around.)*
3. $2^{(1-i)/2}\lambda_i \leq \|\underline{b}_i\| \leq 2^{(n-1)/2}\lambda_i$.
4. $\det(L) \leq \prod_{i=1}^{n} \|\underline{b}_i\| \leq 2^{n(n-1)/4} \det(L)$.
5. $\|\underline{b}_1\| \leq 2^{(n-1)/4} \det(L)^{1/n}$.

Proof:

1. From part 1 of Lemma 17.2.8 we have $\|b_i^*\| \geq 2^{(i-1)/2}\|b_1^*\|$. Hence, part 1 implies

$$\begin{aligned} \lambda_1 &\geq \min_{1 \leq i \leq n} \|\underline{b}_i^*\| \\ &\geq \min_{1 \leq i \leq n} 2^{(1-i)/2}\|\underline{b}_1^*\| \\ &= 2^{(1-n)/2}\|\underline{b}_1^*\|. \end{aligned}$$

   The result follows since $\underline{b}_1^* = \underline{b}_1$.

2. Let $\underline{w}_1, \ldots, \underline{w}_i \in L$ be linearly independent lattice vectors such that $\max\{\|\underline{w}_1\|, \ldots, \|\underline{w}_i\|\} = \lambda_i$. Let $k(j)$ be defined as in Lemma 17.2.11 so that $\|\underline{w}_j\| \geq \|\underline{b}_{k(j)}^*\|$.

   Renumber the vectors $\underline{w}_j$ so that $k(1) \leq k(2) \leq \cdots \leq k(i)$. We claim that $j \leq k(j)$. If not then $\underline{w}_1, \ldots, \underline{w}_j$ would belong to the span of $\{\underline{b}_1, \ldots, \underline{b}_{j-1}\}$ and would be linearly dependent.

   Finally,

$$\|\underline{b}_j\| \leq 2^{(k(j)-1)/2}\|\underline{b}_{k(j)}^*\| \leq 2^{(n-1)/2}\|\underline{w}_j\| \leq 2^{(n-1)/2}\lambda_i,$$

   which proves the result.

3. The upper bound on $\|\underline{b}_i\|$ is given by part 2.

   Since $\{\underline{b}_1, \ldots, \underline{b}_i\}$ are linearly independent we have $\lambda_i \leq \max_{1 \leq j \leq i} \|\underline{b}_j\|$ and by part 3 of Lemma 17.2.8 each $\|\underline{b}_j\| \leq 2^{(i-1)/2}\|\underline{b}_i^*\|$. Using $\|\underline{b}_i^*\| \leq \|\underline{b}_i\|$ we obtain the lower bound on $\|\underline{b}_i\|$.

4. By Lemma 16.1.14 we have $\det(L) = \prod_{i=1}^{n} \|\underline{b}_i^*\|$. The result follows from $\|\underline{b}_i^*\| \leq \|\underline{b}_i\| \leq 2^{(i-1)/2}\|\underline{b}_i^*\|$.

5. By part 3 of Lemma 17.2.8 we have $\|\underline{b}_1\| \leq 2^{(i-1)/2}\|\underline{b}_i^*\|$ and so

$$\|\underline{b}_1\|^n \leq \prod_{i=1}^{n} 2^{(i-1)/2}\|\underline{b}_i^*\| = 2^{n(n-1)/4} \det(L).$$

□

Exercise 17.2.13. Show that taking $\delta \to 1$ in the LLL algorithm would give $\|\underline{b}_1\| \leq (\frac{4}{3})^{(n-1)/2}\lambda_1(L)$ and $\|\underline{b}_1\| \leq (\frac{4}{3})^{(n-1)/4}\det(L)^{1/n}$.

Corollary 17.2.14. *If $\|\underline{b}_1\| \leq \|\underline{b}_i^*\|$ for all $1 \leq i \leq n$ then $\underline{b}_1$ is a correct solution to SVP.*

Exercise 17.2.15. Prove Corollary 17.2.14.

Exercise 17.2.16. Suppose L is a lattice in $\mathbb{Z}^m$ and let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an LLL-reduced basis. Rename these vectors as $\underline{v}_1, \ldots, \underline{v}_n$ such that $1 \leq \|\underline{v}_1\| \leq \|\underline{v}_2\| \leq \cdots \leq \|\underline{v}_n\|$. Show that one does not necessarily have $\|\underline{v}_1\| = \|\underline{b}_1\|$. Show that, for $1 \leq i \leq n$,

$$\|\underline{v}_i\| \leq \left(2^{n(n-1)/4}\det(L)\right)^{1/(n+1-i)}.$$

As a final remark, the results in this section have only given upper bounds on the sizes of $\|\underline{b}_i\|$ in an LLL-reduced lattice basis. In many practical instances, one finds that LLL-reduced lattice vectors are much shorter than these bounds might suggest.

17.3 The Gram-Schmidt Algorithm

The LLL algorithm requires computing a Gram-Schmidt basis. For the complexity analysis of the LLL algorithm it is necessary to give a more careful description and analysis of the Gram-Schmidt algorithm than was done in Section A.10.2. We present pseudocode in Algorithm 24 (the "downto" in line 4 is not necessary, but we write it that way for future reference in the LLL algorithm).

Algorithm 24 Gram-Schmidt algorithm

INPUT: $\{\underline{b}_1, \ldots, \underline{b}_n\}$ in $\mathbb{R}^m$
OUTPUT: $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ in $\mathbb{R}^m$
1: $\underline{b}_1^* = \underline{b}_1$
2: **for** $i = 2$ to n **do**
3: $\quad \underline{v} = \underline{b}_i$
4: $\quad$ **for** $j := i - 1$ downto 1 **do**
5: $\quad\quad \mu_{i,j} = \langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$
6: $\quad\quad \underline{v} = \underline{v} - \mu_{i,j}\underline{b}_j^*$
7: $\quad$ **end for**
8: $\quad \underline{b}_i^* = \underline{v}$
9: **end for**
10: **return** $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$

When working in $\mathbb{R}$ the standard way to implement this algorithm is using floating-point arithmetic. However, problems can arise (especially if the $\underline{b}_i^*$ decrease quickly in size). Such issues are beyond the scope of this book; we refer to Higham [285] for details.

If the input vectors lie in $\mathbb{Z}^m$ then one can perform Algorithm 24 using exact arithmetic over $\mathbb{Q}$. However, the integers can become very large (this is called **coefficient explosion**). We now analyse the size of the integers and prove the complexity of the exact version of the Gram-Schmidt algorithm. These results are used later when determining the complexity of LLL using exact arithmetic.

Definition 17.3.1. Let $\underline{b}_1, \ldots, \underline{b}_n$ be an ordered set of vectors in $\mathbb{Z}^m$. Define $B_i = \|\underline{b}_i^*\|^2$ (as before). For $1 \leq i \leq n-1$ define the $i \times m$ matrix $B_{(i)}$ whose rows are $\underline{b}_1, \ldots, \underline{b}_i$. Define $d_0 = 1$ and, for $1 \leq i \leq n$,

$$d_i = \det(B_{(i)}B_{(i)}^T) \;=\; \det(\langle \underline{b}_j, \underline{b}_k \rangle_{1 \leq j,k \leq i}) \;\in\; \mathbb{Z},$$

which is the square of the volume of the sublattice generated by $B_{(i)}$.

Lemma 17.3.2. *Let the notation be as above.*

1. $d_i = \prod_{j=1}^{i} B_j$ *for* $1 \leq i \leq n$.
2. $B_i = d_i/d_{i-1}$ *for* $1 \leq i \leq n$.
3. $d_{i-1}\underline{b}_i^* \in L \subseteq \mathbb{Z}^n$ *for* $1 \leq i \leq n$, *where* L *is the lattice spanned by* $\{\underline{b}_1, \ldots, \underline{b}_n\}$.
4. $d_j\mu_{i,j} \in \mathbb{Z}$ *for* $1 \leq j < i \leq n$.

Proof:

1. Write $L_{(i)}$ for the lattice spanned by the first i vectors (i.e., L is given by the matrix $B_{(i)}$). Then $d_i = \det(L_{(i)})^2 = \prod_{j=1}^{i} \|\underline{b}_j^*\|^2 = \prod_{j=1}^{i} B_j$ by Lemma 16.1.14.
2. This property follows immediately from the previous one.
3. Write $\underline{b}_i^* = \underline{b}_i - \sum_{j=1}^{i-1} a_{i,j}\underline{b}_j$ for some $a_{i,j} \in \mathbb{R}$. Note that the sum is over vectors $\underline{b}_j$ not $\underline{b}_j^*$, so the $a_{i,j}$ are not the same as the $\mu_{i,j}$. Since $\langle \underline{b}_l, \underline{b}_i^* \rangle = 0$ for $1 \leq l < i$ we have
$$\langle \underline{b}_l, \underline{b}_i \rangle = \sum_{j=1}^{i-1} a_{i,j} \langle \underline{b}_l, \underline{b}_j \rangle,$$
which corresponds to the matrix product
$$(\langle \underline{b}_i, \underline{b}_1 \rangle, \ldots, \langle \underline{b}_i, \underline{b}_{i-1} \rangle) = (a_{i,1}, \ldots, a_{i,i-1}) B_{(i-1)} B_{(i-1)}^T.$$
Inverting $B_{(i-1)}B_{(i-1)}^T$ to solve for the $a_{i,j}$ gives $d_{i-1}a_{i,j} \in \mathbb{Z}$. It follows that $d_{i-1}\underline{b}_i^* \in L \subset \mathbb{Z}^n$ as required.
4. By the previous results we have $d_j\mu_{i,j} = d_{j-1}B_j\langle \underline{b}_i, \underline{b}_j^* \rangle / B_j = \langle \underline{b}_i, d_{j-1}\underline{b}_j^* \rangle \in \mathbb{Z}$.

□

Exercise 17.3.3. Consider the vector $\underline{v} = \underline{b}_i - \sum_{k=j}^{i-1} \mu_{i,k}\underline{b}_k^*$ in line 6 of Algorithm 24 during iteration j. Show that

$$\|\underline{v}\|^2 = \|\underline{b}_i\|^2 - \sum_{k=j}^{i-1} \mu_{i,k}^2 \|\underline{b}_k^*\|^2.$$

Deduce that $\|\underline{v}\| \leq \|\underline{b}_i\|$ and that $d_{i-1}\underline{v} \in \mathbb{Z}^m$ throughout the loop in line 4 of the algorithm.

Theorem 17.3.4. *Let* $\underline{b}_1, \ldots, \underline{b}_n$ *be vectors in* $\mathbb{Z}^m$. *Let* $X \in \mathbb{Z}_{\geq 2}$ *be such that* $\|\underline{b}_i\|^2 \leq X$ *for* $1 \leq i \leq n$. *Then the Gram-Schmidt algorithm performs* $O(n^4 m \log(X)^2)$ *bit operations. The output size is* $O(n^2 m \log(X))$.

Proof: One runs Algorithm 24 using exact $\mathbb{Q}$ arithmetic for the vectors $\underline{b}_i^*$. Lemma 17.3.2 shows that the denominators in $\underline{b}_i^*$ are all factors of d_{i-1}, which has size $\prod_{j=1}^{i-1} B_j \leq \prod_{j=1}^{i-1} \|\underline{b}_j\|^2 \leq X^{i-1}$. Also, $\|\underline{b}_i^*\| \leq \|\underline{b}_i\| \leq X$, so the numerators are bounded by X^i. The size of each vector $\underline{b}_i^*$ and, by Exercise 17.3.3, the intermediate steps $\underline{v}$ in the computation are therefore $O(mi\log(X))$ bits, which gives the output size of the algorithm. The computation $\langle \underline{b}_i, \underline{b}_j^* \rangle$ requires $O(mn\log(X)^2)$ bit operations and the computation $\langle \underline{b}_j^*, \underline{b}_j^* \rangle$ requires $O(mn^2\log(X)^2)$ bit operations. As there are $O(n^2)$ vector operations to perform, one gets the stated running time. □

Corollary 17.3.5. *Let the notation be as in Theorem 17.3.4 and let L be the lattice in $\mathbb{Z}^m$ with basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$. Then one can compute $\det(L)^2$ in $O(n^4 m \log(X)^2)$ bit operations.*[4]

Proof: Lemma 16.1.14 implies $\det(L)^2 = \prod_{i=1}^{n} \|\underline{b}_i^*\|^2$. One computes $\underline{b}_i^*$ using exact (naive) arithmetic over $\mathbb{Q}$ in $O(n^4 m \log(X)^2)$ bit operations. One computes each $\|\underline{b}_i^*\|^2 \in \mathbb{Q}$ in $O(mn^2 \log(X)^2)$ bit operations. Since $\|\underline{b}_i^*\|^2 \leq X$ and $d_{i-1}\|\underline{b}_i^*\|^2 \in \mathbb{Z}$ it follows that $\|\underline{b}_i^*\|^2$ is a ratio of integers bounded by X^n. One computes the product of the $\|\underline{b}_i^*\|^2$ in $O(n^3 \log(X)^2)$ bit operations (since the integers in the product are bounded by X^{n^2}). Finally, one can reduce the fraction using Euclid's algorithm and division in $O(n^4 \log(X)^2)$ bit operations. □

17.4 The LLL Algorithm

The Lenstra-Lenstra-Lovász (LLL) algorithm is an iterative algorithm that transforms a given lattice basis into an LLL-reduced one. Since the definition of LLL-reduced uses Gram-Schmidt vectors, the algorithm performs the Gram-Schmidt method as a subroutine. The first condition of Definition 17.2.4 is easily met by taking suitable integer linear combinations. If the second condition is not met then $\underline{b}_i$ is not significantly longer than $\underline{b}_{i-1}$. In this case we swap $\underline{b}_i$ and $\underline{b}_{i-1}$ and backtrack. The swapping of vectors is familiar from the Lagrange-Gauss 2-dimensional lattice basis reduction algorithm and also Euclid's algorithm. We give the precise details in Algorithm 25.

Algorithm 25 LLL algorithm with Euclidean norm (typically, choose $\delta = 3/4$)

INPUT: $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^m$.
OUTPUT: LLL reduced basis $\underline{b}_1, \ldots, \underline{b}_n$

Compute the Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$ and coefficients $\mu_{i,j}$ for $1 \leq j < i \leq n$
Compute $B_i = \langle \underline{b}_i^*, \underline{b}_i^* \rangle = \|\underline{b}_i^*\|^2$ for $1 \leq i \leq n$
$k = 2$
while $k \leq n$ **do**
    for $j = (k-1)$ downto 1 **do** ▷ Perform size reduction
        Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $\underline{b}_k = \underline{b}_k - q_j \underline{b}_j$
        Update the values $\mu_{k,j}$ for $1 \leq j < k$
    end for
    if $B_k \geq (\delta - \mu_{k,k-1}^2) B_{k-1}$ **then** ▷ Check Lovász condition
        $k = k + 1$
    else
        Swap $\underline{b}_k$ with $\underline{b}_{k-1}$
        Update the values $\underline{b}_k^*$, $\underline{b}_{k-1}^*$, B_k, B_{k-1}, $\mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \leq j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \leq n$
        $k = \max\{2, k-1\}$
    end if
end while

Lemma 17.4.1. *Throughout the LLL algorithm the values $\underline{b}_i^*$ and B_i for $1 \leq i \leq n$ and $\mu_{i,j}$ for $1 \leq j < i \leq n$ are all correct Gram-Schmidt values.*

[4]Since $\det(L)^2 \in \mathbb{Z}$ while $\det(L)$ may not be rational if $n < m$, we prefer to work with $\det(L)^2$.

Exercise 17.4.2. Prove Lemma 17.4.1. In other words, show that line 6 of the LLL algorithm does not change $\underline{b}_i^*$ or B_i for $1 \leq i \leq n$. Similarly, line 12 of the algorithm does not change any values except those mentioned in line 13.

It is illuminating to compare the LLL algorithm with the Lagrange-Gauss reduction algorithm. The basic concept of size reduction followed by a swap is the same, however there are two crucial differences.

1. The size reduction operation in the Lagrange-Gauss algorithm gives the minimal value for $\|\underline{b}_2 + q\underline{b}_1\|$ over $q \in \mathbb{Z}$. In LLL the coefficient $\mu_{k,j}$ is chosen to depend on $\underline{b}_k$ and $\underline{b}_j^*$ so it does not necessarily minimise $\|\underline{b}_k\|$. Indeed $\|\underline{b}_k\|$ can grow during the algorithm. Of course, in the two-dimensional case of LLL then $\mu_{2,1}$ is the same as the value used in the Lagrange-Gauss algorithm and so the size reduction step is the same.

2. The size check in LLL (the Lovász condition) is on the lengths of the Gram-Schmidt vectors, unlike the size check in the Lagrange-Gauss algorithm, which is on the length of the basis vectors themselves.

These features of LLL may seem counterintuitive, but they are essential to the proof that the algorithm runs in polynomial-time.

Lemma 17.4.3. *If $\underline{b}_k$ and $\underline{b}_{k-1}$ are swapped then the Gram-Schmidt vectors $\underline{b}_i^*$ for $1 \leq i \leq n$ are changed as follows*

1. *For $1 \leq i < k-1$ and $k < i < n$ then $\underline{b}_i^*$ is unchanged.*

2. *The new value for $\underline{b}_{k-1}^*$ is $\underline{b}_k^* + \mu_{k,k-1}\underline{b}_{k-1}^*$ and the new value for B_{k-1} is $B'_k = B_k + \mu_{k,k-1}^2 B_{k-1}$.*

3. *The new value for $\underline{b}_k^*$ is $(B_k/B'_{k-1})\underline{b}_{k-1}^* - (\mu_{k,k-1}B_{k-1}/B'_{k-1})\underline{b}_k^*$ and the new value for B_k is $B_{k-1}B_k/B'_{k-1}$.*

Proof: Denote by $\underline{b}'_i$ the new basis (i.e., $\underline{b}'_{k-1} = \underline{b}_k$ and $\underline{b}'_k = \underline{b}_{k-1}$), $\underline{b}_i'^*$ and $\mu'_{i,j}$ the new Gram-Schmidt values and B'_i the squares of the lengths of the $\underline{b}_i'^*$. Clearly $\underline{b}_i'^* = \underline{b}_i^*$ for $1 \leq i < k-1$ and $\mu'_{i,j} = \mu_{i,j}$ for $1 \leq j < i < k-1$. Now

$$\begin{aligned}
\underline{b}_{k-1}'^* &= \underline{b}'_{k-1} - \sum_{j=1}^{k-2} \mu'_{k-1,j}\underline{b}_j'^* \\
&= \underline{b}_k - \sum_{j=1}^{k-2} \mu_{k,j}\underline{b}_j^* \\
&= \underline{b}_k^* + \mu_{k,k-1}\underline{b}_{k-1}^*.
\end{aligned}$$

Hence, $B'_{k-1} = B_k + \mu_{k,k-1}^2 B_{k-1}$.

Similarly,

$$\begin{aligned}
\underline{b'_k}^* &= \underline{b}'_k - \sum_{j=1}^{k-1} \mu'_{k,j} \underline{b'_j}^* \\
&= \underline{b}_{k-1} - \sum_{j=1}^{k-2} \mu_{k-1,j} \underline{b}^*_j \quad - \quad \left(\langle \underline{b}_{k-1}, \underline{b'}^*_{k-1} \rangle / B'_{k-1}\right) \underline{b'}^*_{k-1} \\
&= \underline{b}^*_{k-1} - \left(\langle \underline{b}_{k-1}, \underline{b}^*_k + \mu_{k,k-1} \underline{b}^*_{k-1} \rangle / B'_{k-1}\right) (\underline{b}^*_k + \mu_{k,k-1} \underline{b}^*_{k-1}) \\
&= \underline{b}^*_{k-1} - \left(\mu_{k,k-1} B_{k-1} / B'_{k-1}\right) (\underline{b}^*_k + \mu_{k,k-1} \underline{b}^*_{k-1}) \\
&= \left(1 - \mu^2_{k,k-1} B_{k-1} / B'_{k-1}\right) \underline{b}^*_{k-1} - \left(\mu_{k,k-1} B_{k-1} / B'_{k-1}\right) \underline{b}^*_k.
\end{aligned}$$

The result for $\underline{b'_k}^*$ follows since $1 - \mu^2_{k,k-1} B_{k-1}/B'_{k-1} = B_k / B'_{k-1}$. Finally,

$$B'_k = (B^2_k \langle \underline{b}^*_{k-1}, \underline{b}^*_{k-1} \rangle / {B'_{k-1}}^2 + \mu^2_{k,k-1} B^2_{k-1} \langle \underline{b}^*_k, \underline{b}^*_k \rangle / {B'_{k-1}}^2 = B_{k-1} B_k / B'_{k-1}.$$

□

Exercise 17.4.4. Give explicit formulae for updating the other Gram-Schmidt values in lines 7 and 13 of Algorithm 25.

Exercise 17.4.5. Show that it is not necessary to store or update the values $\underline{b}^*_i$ for $1 \leq i \leq n$ in the LLL algorithm once the values B_i have been computed.

Exercise 17.4.6. Show that the condition in line 9 of Algorithm 25 can be checked immediately after $\mu_{k,k-1}$ has been computed. Hence, show that the cases $1 \leq j < k-1$ in the loop in lines 5 to 8 of Algorithm 25 can be postponed to line 10.

Lemma 17.4.7. *If the LLL algorithm terminates then the output basis is LLL reduced.*

Exercise 17.4.8. Prove Lemma 17.4.7. Indeed, the fact that the Lovász conditions are satisfied is immediate. Prove the bounds on the $\mu_{i,j}$ using the three following steps. Let $1 \leq j < k$ and let $b'_k = b_k - \lfloor \mu_{k,j} \rceil b_j$.

1. Prove that $\langle b_j, b^*_j \rangle = \langle b^*_j, b^*_j \rangle$ and $\langle b_j, b^*_i \rangle = 0$ if $j < i$.
2. Hence, writing $\mu'_{k,j} = \langle b'_k, b^*_j \rangle / \langle b^*_j, b^*_j \rangle$, prove that $|\mu'_{k,j}| \leq 1/2$ for $1 \leq j < k$.
3. For $j < i < k$ denote $\mu'_{k,i} = \langle b'_k, b^*_i \rangle / \langle b^*_i, b^*_i \rangle$. Prove that $\mu'_{k,i} = \mu_{k,i}$.

In the next section we show that the LLL algorithm does terminate. Before then we give an example and some further discussion.

Example 17.4.9. Let L be the lattice with basis matrix

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & 15 \\ 0 & 0 & 3 \end{pmatrix}.$$

We will perform the LLL algorithm to reduce this lattice basis.

We start with $k = 2$ and compute $\mu_{2,1} = 4/1 = 4$. So $q_1 = 4$ and we define

$$\underline{b}_2 = \underline{b}_2 - 4\underline{b}_1 = (4, 2, 15) - (4, 0, 0) = (0, 2, 15).$$

We now want to check the second LLL condition. To do this we need $\underline{b}^*_2$. We compute $\mu_{2,1} = 0$ and hence $\underline{b}^*_2 = \underline{b}_2$. Then $B_1 = 1$ and $B_2 = \langle \underline{b}^*_2, \underline{b}^*_2 \rangle = 229$. Clearly, $B_2 >$

$(3/4 - \mu_{2,1}^2)B_1$ and so we set $k = 3$. Now consider $\underline{b}_3$. We compute $\mu_{3,2} = 45/229 \approx 0.19$ and, since $q_2 = 0$ there is no reduction to be performed on $\underline{b}_3$. We compute $\mu_{3,1} = 0$, so again no size reduction is required. We now compute

$$\underline{b}_3^* = \underline{b}_3 - \tfrac{45}{229}\underline{b}_2^* = (0, -90/229, 12/229).$$

We have $B_2 = 229$ and $B_3 = \langle \underline{b}_3^*, \underline{b}_3^* \rangle = 8244/52441 \approx 0.157$. From this one can check that $B_3 < (3/4 - \mu_{3,2}^2)B_2 \approx 166.1$. Hence we swap $\underline{b}_2$ and $\underline{b}_3$ and set $k = 2$.

At this point we have the vectors

$$\underline{b}_1 = (1, 0, 0) \text{ and } \underline{b}_2 = (0, 0, 3)$$

and $\underline{b}_1^* = \underline{b}_1$, $\underline{b}_2^* = \underline{b}_2$. First check that $\mu_{2,1} = 0$ and so no size reduction on $\underline{b}_2$ is required. Second, $B_1 = 1$ and $B_2 = 9$ and one checks that $B_2 > (3/4 - \mu_{2,1}^2)B_1 = 0.75$. Hence we set $k = 3$. Now

$$\underline{b}_3 = (0, 2, 15)$$

and we compute $\mu_{3,2} = 45/9 = 5$. Hence we reduce

$$\underline{b}_3 = \underline{b}_3 - 5\underline{b}_2 = (0, 2, 0).$$

Now compute $\mu_{3,1} = 0$, so no reduction is required.

One computes $\mu_{3,2} = 0$, $\underline{b}_3^* = \underline{b}_3$ and $B_3 = 4$. Hence, $B_3 < (3/4 - \mu_{3,2}^2)B_2 = 27/4 = 6.75$ and so we should swap $\underline{b}_2$ and $\underline{b}_3$ and set $k = 2$. One can check that the $k = 2$ phase runs without making any changes. We have $B_1 = 1$ and $B_2 = 4$. Consider now $k = 3$ again. We have $\mu_{3,2} = \mu_{3,1} = 0$ and so $\underline{b}_3$ remains unchanged. Finally, $B_3 = 9 > (3/4 - \mu_{3,2}^2)B_2 = 3$ and so we set $k = 4$ and halt. The output is $(1, 0, 0)$, $(0, 2, 0)$ and $(0, 0, 3)$.

Exercise 17.4.10. Perform the LLL algorithm by hand on the basis

$$\{(-1, 5, 0),\ (2, 5, 0),\ (8, 6, 16)\}.$$

Exercise 17.4.11. Perform the LLL algorithm by hand on the basis

$$\{(0, 3, 4), (-1, 3, 3), (5, 4, -7)\}.$$

Remark 17.4.12. Part 1 of Theorem 17.2.12 shows we have $\|\underline{b}_1\| \leq 2^{(n-1)/2}\lambda_1$. In other words, the LLL algorithm solves SVP up to an exponential factor but is not guaranteed to output a shortest vector in the lattice. Hence, LLL does not officially solve SVP.

In practice, at least for relatively small dimensions, the vector $\underline{b}_1$ output by the LLL algorithm is often much closer to the shortest vector than this bound would suggest, and in many cases will be a shortest vector in the lattice. In Example 17.4.9, the theoretical bound gives $\|\underline{b}_1\| \leq 2$, so $(0, 2, 0)$ would have been a possible value for $\underline{b}_1$ (but it wasn't).

17.5 Complexity of LLL

We now show that the LLL algorithm terminates and runs in polynomial-time for lattices in $\mathbb{Z}^m$. The original paper of Lenstra, Lenstra and Lovász [373] proves polynomial termination for any lattice in $\mathbb{R}^m$ but only gives a precise complexity for lattices in $\mathbb{Z}^m$.

Theorem 17.5.1. *Let L be a lattice in $\mathbb{Z}^m$ with basis $\underline{b}_1, \ldots, \underline{b}_n$ and let $X \in \mathbb{Z}_{\geq 2}$ be such that $\|\underline{b}_i\|^2 \leq X$ for $1 \leq i \leq n$. Let $1/4 < \delta < 1$. Then the LLL algorithm with factor δ terminates and performs $O(n^2 \log(X))$ iterations.*

Proof: We need to bound the number of "backtracks" in Algorithm 25. This number is at most n plus the number of swaps. So it suffices to bound the number of swaps by $O(n^2 \log(X))$.

For $1 \leq i \leq n-1$ define the $i \times m$ matrix $B_{(i)}$ formed by the first i basis vectors for the lattice. Define $d_i = \det(B_{(i)} B_{(i)}^T) \in \mathbb{Z}$, which is the square of the volume of the sublattice generated by the rows of $B_{(i)}$. Hence

$$d_i = \prod_{j=1}^{i} B_j = \prod_{j=1}^{i} \|\underline{b}_i^*\|^2 \leq \prod_{j=1}^{i} \|\underline{b}_i\|^2 \leq X^i.$$

Define

$$D = \prod_{i=1}^{n-1} d_i = \prod_{i=1}^{n-1} B_i^{n-i}.$$

It follows that $D \leq X^{(n-1)n/2}$.

Two vectors $\underline{b}_k$ and $\underline{b}_{k-1}$ are swapped when $B_k < (\delta - \mu_{k,k-1}^2) B_{k-1}$. By Lemma 17.4.3, the new values for B_{k-1} and B_k are $B'_{k-1} = B_k + \mu_{k,k-1}^2 B_{k-1}$ and $B'_k = B_{k-1} B_k / B'_{k-1}$. Let d'_i be the new values for the d_i. We have $d'_i = d_i$ when $1 \leq i < k-1$. By the Lovász condition $B'_{k-1} \leq \delta B_{k-1}$. Hence, $d'_{k-1} \leq \delta d_{k-1}$. Finally, since $B'_{k-1} B'_k = B_{k-1} B_k$ we have $d'_i = d_i$ for $k \leq i \leq n$. Hence, swapping $\underline{b}_k$ and $\underline{b}_{k-1}$ always strictly reduces D.

On the other hand, we always have[5] $d_i \in \mathbb{Z}$ and so $D \geq 1$. It follows that the number of swaps in the LLL algorithm is at most[6] $\log_\delta(X^{(n-1)n/2}) = O(n^2 \log(X))$. Hence the algorithm requires $O(n^2 \log(X))$ iterations of the main loop. □

Algorithm 25 and Theorem 17.5.1 provide a proof that an LLL-reduced basis exists for every lattice.

Exercise 17.5.2. Let $n \in \mathbb{N}$. Show that Hermite's constant (see Definition 16.2.7) satisfies $\gamma_n \leq 2^{(n-1)/2}$ (this bound can be improved to $(4/3)^{(n-1)/2}$; see [373]).

It is clear that if $L \subset \mathbb{Z}^m$ then LLL can be implemented using exact $\mathbb{Q}$ arithmetic, and hence exact integer arithmetic. But we need to show that the size of the integers does not explode. The analysis given already for the Gram-Schmidt algorithm (for example, Lemma 17.3.2) provides most of the tools we need.

Theorem 17.5.3. *Let L be a lattice in $\mathbb{Z}^m$ with basis $\underline{b}_1, \ldots, \underline{b}_n$ and let $X \in \mathbb{Z}_{\geq 2}$ be such that $\|\underline{b}_i\|^2 \leq X$ for $1 \leq i \leq n$. Then the LLL algorithm requires arithmetic operations on integers of size $O(n \log(X))$.*

Proof: (Sketch) The bounds on the sizes of the $\underline{b}_i^*$ follow the same methods as used in the proof of Theorem 17.3.4. Since $\|\underline{b}_i^*\|$ is never increased during the algorithm (indeed, the vectors are specifically permuted to reduce the $\|\underline{b}_i^*\|$) we have $\|\underline{b}_i^*\| \leq X^{1/2}$ at the end of each iteration. Since $d_{i-1} \underline{b}_i^* \in \mathbb{Z}^n$ and $|d_{i-1}| \leq X^{i-1}$ it follows that the entries of $\underline{b}_i^*$ can be written as $n_{i,j}^* / d_{i-1}$ where $|n_{i,j}^*| \leq X^i$.

Let us now consider the values $\|\underline{b}_i\|^2$ at the end of each iteration. These values all start bounded by X. As the algorithm proceeds the values are either not yet changed (and hence still bounded by X) or have been modified so that the Gram-Schmidt basis is size reduced (and possibly swapped to an earlier position in the list of vectors). After

[5] To apply this argument it is necessary to use the square of the determinant. An integer lattice that does not have full rank does not necessarily have integer determinant.

[6] Recall that $1/4 < \delta < 1$ is considered as a fixed constant.

each size reduction step (and before swapping) we have

$$\underline{b}_i = \underline{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \underline{b}_j^*$$

with $-1/2 \leq \mu_{i,j} \leq 1/2$ and so

$$\|\underline{b}_i\|^2 = \|\underline{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\underline{b}_j^*\|^2 \leq nX. \tag{17.2}$$

Hence, we have $\|\underline{b}_i\| \leq \sqrt{nX}$ at the end of each iteration and so the entries of $\underline{b}_i$ are all integers bounded by $\sqrt{nX}$.

The remaining detail is to bound the sizes of the $\mu_{i,j}$ and the sizes of intermediate values in line 6 of Algorithm 25. We refer to the proof of Proposition 1.26 of [373] for the bounds $|\mu_{i,j}| \leq 2^{n-i}(nX^{n-1})^{1/2}$ and for further details. □

Corollary 17.5.4. *Let L be a lattice in $\mathbb{Z}^m$ with basis $\underline{b}_1, \ldots, \underline{b}_n$ and let $X \in \mathbb{Z}_{\geq 2}$ be such that $\|\underline{b}_i\|^2 \leq X$ for $1 \leq i \leq n$. Then the LLL algorithm requires $O(n^3 m \log(X))$ arithmetic operations on integers of size $O(n \log(X))$. Using naive arithmetic gives running time $O(n^5 m \log(X)^3)$ bit operations.*

Proof: Theorem 17.5.1 implies that the algorithm requires $O(n^2 \log(X))$ iterations of the main loop. Within each iteration there are n operations on vectors of length m. Hence $O(n^3 m \log(X))$ arithmetic operations. Theorem 17.5.3 implies that all arithmetic operations are on integers of size $O(n \log(X))$. □

Remark 17.5.5.

1. Since the input size is $O(nm \log(X))$ and $n \leq m$ the running time is cubic in the input size.

2. Note that the bounds on the sizes of integers involved in the LLL algorithm are $O(n \log(X))$ bits for the values $\mu_{i,j}$ and entries of $\underline{b}_i^*$ while only $O(\log(n) + \log(X))$ bits are needed for the entries in the vectors $\underline{b}_i$. This is not just an artifact of the proof, but is a genuine phenomenon; it can already be seen in Example 17.4.9 where the $\underline{b}_i$ all have very small integer coordinates and yet $\mu_{2,1} = 45/229$.

   This leads to the idea of representing the $\mu_{i,j}$ and $\underline{b}_i^*$ using approximate (floating-point) arithmetic and keeping exact integer arithmetic only for the $\underline{b}_i$. Variants of LLL using floating-point arithmetic for the Gram-Schmidt vectors are much faster than the basic LLL algorithm presented in this chapter. Indeed, the basic algorithm is almost never used in practice.

   A problem with using floating-point approximations is that comparisons now become inexact, and this leads to problems with both termination and correctness of the output. Implementing and analysing floating-point LLL algorithms is beyond the scope of this book. We refer to Stehlé [582] and Schnorr [525] for surveys of this topic.

3. One can show (e.g., using equation (17.2)) that the complexity statement holds also for $X = \max\{\|\underline{b}_i^*\| : 1 \leq i \leq n\}$, which could be smaller than $\max\{\|\underline{b}_i\| : 1 \leq i \leq n\}$.

4. Sometimes one is interested in reducing lattice bases that are in $\mathbb{Q}^m$ and not $\mathbb{Z}^m$. Suppose all rational numbers in the basis B have numerator and denominator bounded by X. One can obtain an integer matrix by multiplying B by an integer that clears all denominators, but the resulting integers could be as big as X^{mn}.

This gives a worst-case complexity of $O(n^8 m^4 \log(X)^3)$ bit operations for lattice basis reduction.

Some applications such as simultaneous Diophantine approximation (see Section 19.5) and the hidden number problem (see Section 21.7.1) have at most m non-integer entries, giving a complexity of $O(n^5 m^4 \log(X)^3)$ bit operations.

17.6 Variants of the LLL Algorithm

There are many refinements of the LLL algorithm that are beyond the scope of the brief summary in this book. We list some of these now.

- As mentioned earlier, it is necessary to use floating-point arithmetic to obtain a fast version of the LLL algorithm. A variant of floating-point LLL whose running time grows quadratically in $\log(X)$ (rather than cubicly, as usual) is the L^2 algorithm of Nguyen and Stehlé [454] (also see Stehlé [582]).

- Schnorr-Euchner "deep insertions". The idea is that, rather than just swapping $\underline{b}_k$ and $\underline{b}_{k-1}$ in the LLL algorithm, one can move $\underline{b}_k$ much earlier in the list of vectors if B_k is sufficiently small. With standard LLL we have shown that swapping $\underline{b}_k$ and $\underline{b}_{k-1}$ changes B_k to $B_k + \mu_{k,k-1}^2 B_{k-1}$. A similar argument shows that inserting $\underline{b}_k$ between $\underline{b}_{i-1}$ and $\underline{b}_i$ for some $1 < i < k$ changes B_k to

$$B = B_k + \sum_{j=1}^{k-1} \mu_{k,j}^2 B_j$$

  Hence, one can let i be the smallest index such that $B < \frac{3}{4} B_i$ and insert $\underline{b}_k$ between $\underline{b}_{i-1}$ and $\underline{b}_i$ (i.e., reorder the vectors $\underline{b}_i, \ldots, \underline{b}_k$ as $\underline{b}_k, \underline{b}_i, \ldots, \underline{b}_{k-1}$). We refer to Schnorr and Euchner [526] and Section 2.6.2 of Cohen [136] for more details.

- Our presentation of the LLL algorithm was for the Euclidean norm. The algorithm has been extended to work with any norm by Lovász and Scarf [396] (also see Kaib and Ritter [325]).

  In practice, if one wants results for a norm other than the Euclidean norm, one usually performs ordinary LLL reduction with respect to the Euclidean norm and then uses the standard relations between norms (Lemma A.10.2) to determine the quality of the resulting vectors.

- Another important approach to lattice basis reduction is the block Korkine-Zolotarev algorithm due to Schnorr [521]. We mention this further in Section 18.5.

Chapter 18

Algorithms for the Closest and Shortest Vector Problems

This chapter presents several algorithms to find lattice vectors close to a given vector. First we consider two methods due to Babai that, although not guaranteed to solve the closest vector problem, are useful in several situations in the book. Then we present an exponential-time algorithm to enumerate all vectors close to a given point. This algorithm can be used to solve the closest and shortest vector problems. We then briefly mention a lattice basis reduction algorithm that is guaranteed to yield better approximate solutions to the shortest vector problem.

The closest vector problem (CVP) was defined in Section 16.3. First, we remark that the shortest distance from a given vector $\underline{w} \in \mathbb{R}^n$ to a lattice vector $\underline{v} \in L$ can be quite large compared with the lengths of short vectors in the lattice.

Example 18.0.1. Consider the lattice in $\mathbb{R}^2$ with basis $(1, 0)$ and $(0, 1000)$. Then $\underline{w} = (0, 500)$ has distance 500 from the closest lattice point, despite the fact that the first successive minimum is 1.

Exercise 18.0.2. Let $L = \mathbb{Z}^n$ and $\underline{w} = (1/2, \ldots, 1/2)$. Show that $\|\underline{w} - \underline{v}\| \geq \sqrt{n}/2$ for all $\underline{v} \in L$. Hence, show that if $n > 4$ then $\|\underline{w} - \underline{v}\| > \lambda_n$ for all $\underline{v} \in L$.

18.1 Babai's Nearest Plane Method

Let L be a full rank lattice given by an (ordered) basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the corresponding Gram-Schmidt basis. Let $\underline{w} \in \mathbb{R}^n$. Babai [18] presented a method to inductively find a lattice vector close to $\underline{w}$. The vector $\underline{v} \in L$ output by Babai's method is not guaranteed to be such that $\|\underline{w} - \underline{v}\|$ is minimal. Theorem 18.1.6 shows that if the lattice basis is LLL-reduced then $\|\underline{w} - \underline{v}\|$ is within an exponential factor of the minimal value.

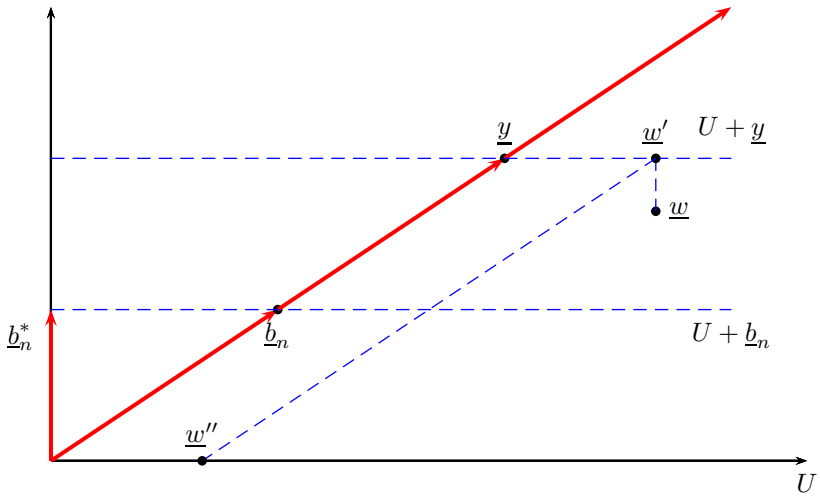


Figure 18.1: Illustration of the Babai nearest plane method. The x-axis represents the subspace U (which has dimension $n-1$) and the y-axis is perpendicular to U.

We now describe the method. Define $U = \text{span}\{\underline{b}_1, \ldots, \underline{b}_{n-1}\}$ and let $L' = L \cap U$ be the sublattice spanned by $\{\underline{b}_1, \ldots, \underline{b}_{n-1}\}$. The idea of the nearest plane method is to find a vector $\underline{y} \in L$ such that the distance from $\underline{w}$ to the plane $U + \underline{y}$ is minimal. One then sets $\underline{w}'$ to be the orthogonal projection of $\underline{w}$ onto the plane $U + \underline{y}$ (in other words, $\underline{w}' \in U + \underline{y}$ and $\underline{w} - \underline{w}' \in U^\perp$). Let $\underline{w}'' = \underline{w}' - \underline{y} \in U$. Note that if $\underline{w} \notin L$ then $\underline{w}'' \notin L$. One inductively solves the (lower dimensional) closest vector problem of $\underline{w}''$ in L' to get $\underline{y}' \in L'$. The solution to the original instance of the CVP is $\underline{v} = \underline{y} + \underline{y}'$.

We now explain how to algebraically find $\underline{y}$ and $\underline{w}'$.

Lemma 18.1.1. *Let*

$$\underline{w} = \sum_{j=1}^{n} l_j \underline{b}_j^* \tag{18.1}$$

with $l_j \in \mathbb{R}$. Define $\underline{y} = \lfloor l_n \rceil \underline{b}_n \in L$ (where $\lfloor l_n \rceil$ denotes rounding to the nearest integer) and $\underline{w}' = \sum_{j=1}^{n-1} l_j \underline{b}_j^* + \lfloor l_n \rceil \underline{b}_n^*$. Then $\underline{y}$ is such that the distance between $\underline{w}$ and $U + \underline{y}$ is minimal, and $\underline{w}'$ is the orthogonal projection of $\underline{w}$ onto $U + \underline{y}$.

Proof: We use the fact that $U = \text{span}\{\underline{b}_1^*, \ldots, \underline{b}_{n-1}^*\}$. The distance from $\underline{w}$ to $U + \underline{y}$ is

$$\inf_{\underline{u} \in U} \|\underline{w} - (\underline{u} + \underline{y})\|.$$

Let $\underline{w}$ be as in equation (18.1) and let $\underline{y} = \sum_{j=1}^{n} l'_j \underline{b}_j$ be any element of L for $l'_j \in \mathbb{Z}$. One can write $\underline{y} = \sum_{j=1}^{n-1} l''_j \underline{b}_j^* + l'_n \underline{b}_n^*$ for some $l''_j \in \mathbb{R}$, $1 \leq j \leq n-1$.

Lemma A.10.5 shows that, for fixed $\underline{w}$ and $\underline{y}$, $\|\underline{w} - (\underline{u} + \underline{y})\|^2$ is minimised by $\underline{u} = \sum_{j=1}^{n-1} (l_j - l''_j) \underline{b}_j^* \in U$. Indeed,

$$\|\underline{w} - (\underline{u} + \underline{y})\|^2 = (l_n - l'_n)^2 \|\underline{b}_n^*\|^2.$$

It follows that one must take $l'_n = \lfloor l_n \rceil$, and so the choice of $\underline{y}$ in the statement of the Lemma is correct (note that one can add any element of L' to $\underline{y}$ and it is still a valid choice).

The vector $\underline{w}'$ satisfies

$$\underline{w}' - \underline{y} = \sum_{j=1}^{n-1} l_j \underline{b}_j^* + \lfloor l_n \rceil (b_n^* - \underline{b}_n) \in U,$$

which shows that $\underline{w}' \in U + \underline{y}$. Also,

$$\underline{w} - \underline{w}' = \sum_{j=1}^{n} l_j \underline{b}_j^* - \sum_{j=1}^{n-1} l_j \underline{b}_j^* - \lfloor l_n \rceil \underline{b}_n^* = (l_n - \lfloor l_n \rceil)\underline{b}_n^*, \tag{18.2}$$

which is orthogonal to U. Hence, $\underline{w}'$ is the orthogonal projection of $\underline{w}$ onto $U + \underline{y}$. □

Exercise 18.1.2. Let the notation be as above and write $\underline{b}_n = \underline{b}_n^* + \sum_{i=1}^{n-1} \mu_{n,i} \underline{b}_i^*$. Show that

$$\underline{w}'' = \sum_{i=1}^{n-1} (l_i - \lfloor l_n \rceil \mu_{n,i}) \underline{b}_i^*.$$

Exercise 18.1.3. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an ordered basis for a lattice L. Let $\underline{w} \in \mathbb{R}^n$ and suppose that there is an element $\underline{v} \in L$ such that $\|\underline{v} - \underline{w}\| < \frac{1}{2}\|\underline{b}_i^*\|$ for all $1 \leq i \leq n$. Prove that the nearest plane algorithm outputs $\underline{v}$.

The following Lemma is needed to prove the main result, namely Theorem 18.1.6.

Lemma 18.1.4. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be LLL reduced (with respect to the Euclidean norm, and with factor $\delta = 3/4$). If $\underline{v}$ is the output of Babai's nearest plane algorithm on input $\underline{w}$ then*

$$\|\underline{w} - \underline{v}\|^2 \leq \tfrac{2^n - 1}{4} \|\underline{b}_n^*\|^2.$$

Proof: We prove the result by induction. Certainly if $n = 1$ then $\|\underline{w} - \underline{v}\|^2 \leq \frac{1}{4}\|\underline{b}_1^*\|^2$ as required.

Now suppose $n \geq 2$. Recall that the output of the method is $\underline{v} = \underline{y} + \underline{y}'$ where $\underline{y} \in L$ minimises the distance from $\underline{w}$ to $U + \underline{y}$, $\underline{w}'$ is the orthogonal projection of $\underline{w}$ onto $U + \underline{y}$, and $\underline{y}'$ is the output of the algorithm on $\underline{w}'' = \underline{w}' - \underline{y}$ in L'. By the inductive hypothesis we know that $\|\underline{w}'' - \underline{y}'\|^2 \leq \frac{1}{4}(2^{n-1} - 1)\|\underline{b}_{n-1}^*\|^2$. Hence

$$\begin{aligned} \|\underline{w} - (\underline{y} + \underline{y}')\|^2 &= \|\underline{w} - \underline{w}' + \underline{w}' - (\underline{y} + \underline{y}')\|^2 \\ &= \|\underline{w} - \underline{w}'\|^2 + \|\underline{w}'' - \underline{y}'\|^2 \\ &\leq \tfrac{1}{4}\|\underline{b}_n^*\|^2 + \tfrac{2^{n-1}-1}{4}\|\underline{b}_{n-1}^*\|^2 \end{aligned}$$

using equation (18.2).

Finally, part 1 of Lemma 17.2.8 implies that this is

$$\leq \left(\tfrac{1}{4} + 2\tfrac{2^{n-1}-1}{4}\right) \|\underline{b}_n^*\|^2$$

from which the result follows. □

Exercise 18.1.5. Prove that if $\underline{v}$ is the output of the nearest plane algorithm on input $\underline{w}$ then

$$\|\underline{v} - \underline{w}\|^2 \leq \tfrac{1}{4} \sum_{i=1}^{n} \|\underline{b}_i^*\|^2.$$

Theorem 18.1.6. *If the basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is LLL-reduced (with respect to the Euclidean norm and with factor $\delta = 3/4$) then the output of the Babai nearest plane algorithm on $\underline{w} \in \mathbb{R}^n$ is a vector $\underline{v}$ such that $\|\underline{v} - \underline{w}\| < 2^{n/2}\|\underline{u} - \underline{w}\|$ for all $\underline{u} \in L$.*

Proof: We prove the result by induction. For $n = 1$, $\underline{v}$ is a correct solution to the closest vector problem and so the result holds.

Let $n \geq 2$ and let $\underline{u} \in L$ be a closest vector to $\underline{w}$. Let $\underline{y}$ be the vector chosen in the first step of the Babai method. We consider two cases.

1. Case $\underline{u} \in U + \underline{y}$. Then $\|\underline{u} - \underline{w}\|^2 = \|\underline{u} - \underline{w}'\|^2 + \|\underline{w}' - \underline{w}\|^2$ so $\underline{u}$ is also a closest vector to $\underline{w}'$. Hence $\underline{u} - \underline{y}$ is a closest vector to $\underline{w}'' = \underline{w}' - \underline{y} \in U$. Let $\underline{y}'$ be the output of the Babai nearest plane algorithm on $\underline{w}''$. By the inductive hypothesis,

$$\|\underline{y}' - \underline{w}''\| < 2^{(n-1)/2}\|\underline{u} - \underline{y} - \underline{w}''\|.$$

   Substituting $\underline{w}' - \underline{y}$ for $\underline{w}''$ gives

$$\|\underline{y} + \underline{y}' - \underline{w}'\| < 2^{(n-1)/2}\|\underline{u} - \underline{w}'\|.$$

   Now

$$\|\underline{v} - \underline{w}\|^2 = \|\underline{y} + \underline{y}' - \underline{w}'\|^2 + \|\underline{w}' - \underline{w}\|^2 < 2^{n-1}\|\underline{u} - \underline{w}'\|^2 + \|\underline{w}' - \underline{w}\|^2.$$

   Using $\|\underline{u} - \underline{w}'\|, \|\underline{w}' - \underline{w}\| \leq \|\underline{u} - \underline{w}\|$ and $2^{n-1} + 1 \leq 2^n$ gives the result.

2. Case $\underline{u} \notin U + \underline{y}$. Since the distance from $\underline{w}$ to $U + \underline{y}$ is $\leq \frac{1}{2}\|\underline{b}_n^*\|$, we have $\|\underline{w} - \underline{u}\| \geq \frac{1}{2}\|\underline{b}_n^*\|$. By Lemma 18.1.4 we find

$$\tfrac{1}{2}\|\underline{b}_n^*\| \geq \tfrac{1}{2}\sqrt{\frac{4}{2^n - 1}}\|\underline{w} - \underline{v}\|.$$

   Hence, $\|\underline{w} - \underline{v}\| < 2^{n/2}\|\underline{w} - \underline{u}\|$.

This completes the proof. □

One can obtain a better result by using the result of Lemma 17.2.9.

Theorem 18.1.7. *If the basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is LLL-reduced with respect to the Euclidean norm and with factor $\delta = 1/4 + 1/\sqrt{2}$ then the output of the Babai nearest plane algorithm on $\underline{w} \in \mathbb{R}^n$ is a vector $\underline{v}$ such that*

$$\|\underline{v} - \underline{w}\| < \frac{2^{n/4}}{\sqrt{\sqrt{2} - 1}}\|\underline{u} - \underline{w}\| < (1.6)2^{n/4}\|\underline{u} - \underline{w}\|$$

for all $\underline{u} \in L$.

Exercise 18.1.8. Prove Theorem 18.1.7.
[Hint: First prove that the analogue of Lemma 18.1.4 in this case is $\|\underline{w} - \underline{v}\|^2 \leq (2^{n/2} - 1)/(4(\sqrt{2} - 1))\|\underline{b}_n^*\|^2$. Then follow the proof of Theorem 18.1.6 using the fact that $\left(2^{(n-1)/4}/\sqrt{\sqrt{2} - 1}\right)^2 + 1 \leq \left(2^{n/4}/\sqrt{\sqrt{2} - 1}\right)^2$.]

Algorithm 26 is the Babai nearest plane algorithm. We use the notation $\underline{y}_n = \underline{y}$, $\underline{w}_n = \underline{w}$, $\underline{w}_{n-1} = \underline{w}''$ etc. Note that Babai's algorithm can be performed using exact arithmetic over $\mathbb{Q}$ or using floating point arithmetic.

Algorithm 26 Babai nearest plane algorithm

INPUT: $\{\underline{b}_1, \ldots, \underline{b}_n\}, \underline{w}$
OUTPUT: $\underline{v}$
  Compute Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$
  Set $\underline{w}_n = \underline{w}$
  for $i = n$ downto 1 **do**
    Compute $l_i = \langle \underline{w}_i, \underline{b}_i^* \rangle / \langle \underline{b}_i^*, \underline{b}_i^* \rangle$
    Set $\underline{y}_i = \lfloor l_i \rceil \underline{b}_i$
    Set $\underline{w}_{i-1} = \underline{w}_i - (l_i - \lfloor l_i \rceil)\underline{b}_i^* - \lfloor l_i \rceil \underline{b}_i$
  end for
  return $\underline{v} = \underline{y}_1 + \cdots + \underline{y}_n$

Exercise 18.1.9. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a basis for a lattice in $\mathbb{Z}^n$. Let $X \in \mathbb{R}_{>0}$ be such that $\|\underline{b}_i\| \leq X$ for $1 \leq i \leq n$. Show that the complexity of the Babai nearest plane algorithm (not counting LLL) when using exact arithmetic over $\mathbb{Q}$ is $O(n^5 \log(X)^2)$ bit operations.

Exercise 18.1.10. If $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is an ordered LLL-reduced basis then $\underline{b}_1$ is likely to be shorter than $\underline{b}_n$. It would therefore be more natural to start with $\underline{b}_1$ and define U to be the orthogonal complement of $\underline{b}_1$. Why is this not possible?

Example 18.1.11. Consider the LLL-reduced basis

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 0 & -3 \\ 3 & -7 & 3 \end{pmatrix}$$

and the vector $\underline{w} = (10, 6, 5) \in \mathbb{R}^3$. We perform the nearest plane method to find a lattice vector close to $\underline{w}$.

First compute the Gram-Schmidt basis $\underline{b}_1^* = (1, 2, 3)$, $\underline{b}_2^* = (24/7, 6/7, -12/7)$ and $\underline{b}_3^* = (10/3, -20/3, 10/3)$. Write

$$\underline{w} = \tfrac{37}{14}\underline{b}_1^* + 2\underline{b}_2^* + \tfrac{3}{20}\underline{b}_3^*.$$

Since $\lfloor 3/20 \rceil = 0$ we have $\underline{y}_3 = 0$ and $\underline{w}'' = \underline{w}' = \frac{37}{14}\underline{b}_1^* + 2\underline{b}_2^* = (19/2, 7, 9/2)$. The process is continued inductively, so write $\underline{w} = \underline{w}''$. Then one takes $\underline{y}_2 = 2\underline{b}_2 = (6, 0, -6)$ and $\underline{w}'' = \underline{w} - \underline{y}_2 = (7/2, 7, 21/2) = \frac{7}{2}\underline{b}_1^*$. Since $\lfloor 7/2 \rceil = 3$ we return the solution

$$3\underline{b}_1 + 2\underline{b}_2 = (9, 6, 3).$$

Exercise 18.1.12. Show that the vector $\underline{v}$ output by the Babai nearest plane method lies in the parallelepiped

$$\left\{ \underline{w} + \sum_{j=1}^{n} l_j \underline{b}_j^* : l_j \in \mathbb{R}, |l_j| \leq \tfrac{1}{2} \right\}$$

centered on $\underline{w}$. Show that this parallelepiped has volume equal to the volume of the lattice. Hence show that if $\underline{w}$ does not lie in the lattice then there is exactly one lattice point in this parallelepiped.

Show that if there exists a vector $\underline{v} \in L$ such that $\|\underline{v} - \underline{w}\| \leq \frac{1}{2} \min\{\|\underline{b}_i^*\| : 1 \leq i \leq n\}$ then the Babai nearest plane algorithm on input $\underline{w}$ outputs $\underline{v}$.

Some improvements to the Babai nearest plane algorithm are listed in Section 3.4 of [256] (where they are credited to Coppersmith). Similar methods (but using a randomised choice of plane) were used by Klein [341] to solve the CVP when the target vector is particularly close to a lattice point. Another variant of the nearest plane algorithm is given by Lindner and Peikert [390]. The nearest plane algorithm is known by the name "VBLAST" in the communications community (see [440]).

18.2 Babai's Rounding Technique

An alternative to the nearest plane method is the rounding technique. This is simpler to compute in practice, since it does not require the computation of a Gram-Schmidt basis, but harder to analyse in theory. This method is also not guaranteed to solve CVP. Let $\underline{b}_1, \ldots, \underline{b}_n$ be a basis for a full rank lattice in $\mathbb{R}^n$. Given a target $\underline{w} \in \mathbb{R}^n$ we can write

$$\underline{w} = \sum_{i=1}^{n} l_i \underline{b}_i$$

with $l_i \in \mathbb{R}$. One computes the coefficients l_i by solving the system of linear equations (since the lattice is full rank we can also compute the vector $(l_1, \ldots, l_n)$ as $\underline{w}B^{-1}$). The rounding technique is simply to set

$$\underline{v} = \sum_{i=1}^{n} \lfloor l_i \rceil \underline{b}_i$$

where $\lfloor l \rceil$ means take the closest integer to the real number l. This procedure can be performed using any basis for the lattice. Babai has proved that $\|\underline{v} - \underline{w}\|$ is within an exponential factor of the minimal value if the basis is LLL-reduced. The method trivially generalises to non-full-rank lattices as long as $\underline{w}$ lies in the $\mathbb{R}$-span of the basis.

Theorem 18.2.1. *Let $\underline{b}_1, \ldots, \underline{b}_n$ be an LLL-reduced basis (with respect to the Euclidean norm and with factor $\delta = 3/4$) for a lattice $L \subseteq \mathbb{R}^n$. Then the output $\underline{v}$ of the Babai rounding method on input $\underline{w} \in \mathbb{R}^n$ satisfies*

$$\|\underline{w} - \underline{v}\| \leq (1 + 2n(9/2)^{n/2})\|\underline{w} - \underline{u}\|$$

for all $\underline{u} \in L$.

Proof: See Babai [18]. □

Babai rounding gives a lattice point $\underline{v}$ such that $\underline{w} - \underline{v} = \sum_{i=1}^{n} m_i \underline{b}_i$ where $|m_i| \leq 1/2$. In other words, $\underline{v}$ lies in the parallelepiped, centered at $\underline{w}$, defined by the basis vectors. Since the volume of the parallelepiped is equal to the volume of the lattice, if $\underline{w}$ is not in the lattice then there is exactly one lattice point in the parallelepiped. The geometry of the parallelepiped determines whether or not an optimal solution to the CVP is found. Hence, though the rounding method can be used with any basis for a lattice, the result depends on the quality of the basis.

Example 18.2.2. Let $\underline{b}_1 = (3, 2)$ and $\underline{b}_2 = (2, 1)$ generate the lattice $\mathbb{Z}^2$. Let $\underline{w} = (-0.4, 0.4)$ so that the solution to CVP is $(0, 0)$. One can verify that $(-0.4, 0.4) = 1.2\underline{b}_1 - 2\underline{b}_2$ and so Babai rounding yields $\underline{b}_1 - 2\underline{b}_2 = (-1, 0)$. Figure 18.2 shows the parallelepiped centered at $\underline{w}$ corresponding to the basis. One can see that $(-1, 0)$ is the only lattice point within that parallelepiped.

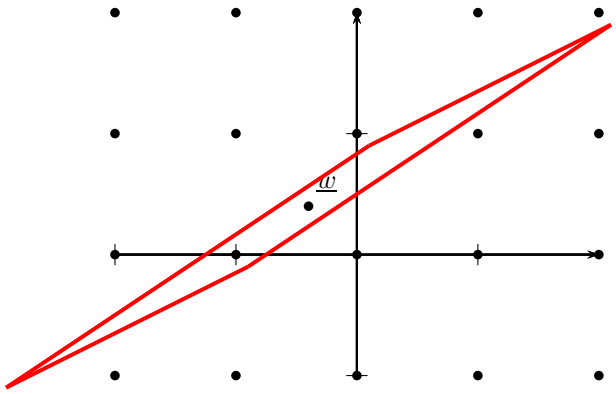


Figure 18.2: Parallelepiped centered at $(-0.4, 0.4)$ corresponding to lattice basis $(3, 2)$ and $(2, 1)$.

Exercise 18.2.3. Consider the vector $\underline{w} = (-0.4, 0.4)$ as in Example 18.2.2 again. Using the basis $\{(1, 0), (0, 1)\}$ for $\mathbb{Z}^2$ use the Babai rounding method to find the closest lattice vector in $\mathbb{Z}^2$ to $\underline{w}$. Draw the parallelepiped centered on $\underline{w}$ in this case.

We stress that the rounding method is not the same as the nearest plane method. The next example shows that the two methods can give different results.

Example 18.2.4. Consider the CVP instance in Example 18.1.11. We have

$$\underline{w} = \tfrac{141}{40}\underline{b}_1 + \tfrac{241}{120}\underline{b}_2 + \tfrac{3}{20}\underline{b}_3.$$

Hence one sets

$$\underline{v} = 4\underline{b}_1 + 2\underline{b}_2 = (10, 8, 6) \neq (9, 6, 3).$$

Note that this is a different solution to the one found in Example 18.1.11, though both solutions satisfy $\|\underline{w} - \underline{v}\| = \sqrt{5}$.

Exercise 18.2.5. Prove that if $\underline{b}_1, \ldots, \underline{b}_n$ are orthogonal basis vectors for a lattice L then the Babai rounding technique produces a correct solution to the CVP with respect to the Euclidean norm. Show also that the Babai rounding technique gives the same result as the Babai nearest plane method in this case.

Exercise 18.2.6. Show that the nearest plane and rounding methods produce a linear combination of the lattice basis where the vector $\underline{b}_n$ has the same coefficient.

Exercise 18.2.7. Consider the lattice with basis

$$\begin{pmatrix} 7 & 0 & 1 \\ 1 & 17 & 1 \\ -3 & 0 & 10 \end{pmatrix}$$

and let

$$\underline{w} = (100, 205, 305).$$

Find a lattice vector $\underline{v}$ close to $\underline{w}$ using the rounding technique. What is $\|\underline{v} - \underline{w}\|$?

The Babai rounding algorithm is known by the name "zero forcing" in the communications community (see [440]).

18.3 The Embedding Technique

Another way to solve CVP is the **embedding technique**, due to Kannan (see page 437 onwards of [330]). Let B be a basis matrix for a lattice L and suppose $\underline{w} \in \mathbb{R}^n$ (in practice we assume $\underline{w} \in \mathbb{Q}^n$). A solution to the CVP corresponds to integers $l_1, \ldots, l_n$ such that

$$\underline{w} \approx \sum_{i=1}^{n} l_i \underline{b}_i.$$

The crucial observation is that $\underline{e} = \underline{w} - \sum_{i=1}^{n} l_i \underline{b}_i$ is such that $\|\underline{e}\|$ is small.

The idea of the embedding technique is to define a lattice L' that contains the short vector $\underline{e}$. Let $M \in \mathbb{R}_{>0}$ (for example $M = 1$). The lattice L' is defined by the vectors (which are a basis for $\mathbb{R}^{n+1}$)

$$(\underline{b}_1, 0),\ \cdots,\ (\underline{b}_n, 0),\ (\underline{w}, M). \tag{18.3}$$

One sees that taking the linear combination of rows with coefficients $(-l_1, \ldots, -l_n, 1)$ gives the vector

$$(\underline{e}, M).$$

Hence, we might be able to find $\underline{e}$ by solving the SVP problem in the lattice L'. One can then solve the CVP by subtracting $\underline{e}$ from $\underline{w}$.

Example 18.3.1. Consider the basis matrix

$$B = \begin{pmatrix} 35 & 72 & -100 \\ -10 & 0 & -25 \\ -20 & -279 & 678 \end{pmatrix}$$

for a lattice in $\mathbb{R}^3$. We solve the CVP instance with $\underline{w} = (100, 100, 100)$.

Apply the LLL algorithm to the basis matrix (taking $M = 1$)

$$\begin{pmatrix} 35 & 72 & -100 & 0 \\ -10 & 0 & -25 & 0 \\ -20 & -279 & 678 & 0 \\ 100 & 100 & 100 & 1 \end{pmatrix}$$

for the lattice L'. This gives the basis matrix

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 5 & 0 & 1 & 0 \\ 0 & 5 & 1 & -4 \\ 5 & 5 & -21 & -4 \end{pmatrix}.$$

The first row is $(0, 1, 0, 1)$, so we know that $(0, 1, 0)$ is the difference between $\underline{w}$ and a lattice point $\underline{v}$. One verifies that $\underline{v} = (100, 100, 100) - (0, 1, 0) = (100, 99, 100)$ is a lattice point.

The success of the embedding technique depends on the size of $\underline{e}$ compared with the lengths of short vectors in the original lattice L. As we have seen in Exercise 18.0.2, $\underline{e}$ can be larger than λ_n, in which case the embedding technique is not likely to be a good way to solve the closest vector problem.

Lemma 18.3.2. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a basis for a lattice $L \subseteq \mathbb{Z}^n$ and denote by λ_1 the shortest Euclidean length of a non-zero element of L. Let $\underline{w} \in \mathbb{R}^n$ and let $\underline{v} \in L$ be a closest lattice point to $\underline{w}$. Define $\underline{e} = \underline{w} - \underline{v}$. Suppose that $\|\underline{e}\| < \lambda_1/2$ and let $M = \|\underline{e}\|$. Then $(\underline{e}, M)$ is a shortest non-zero vector in the lattice L' of the embedding technique.*

Proof: All vectors in the lattice L' are of the form

$$l_{n+1}(\underline{e}, M) + \sum_{i=1}^{n} l_i(\underline{b}_i, 0)$$

for some $l_1, \ldots, l_{n+1} \in \mathbb{Z}$. Every non-zero vector with $l_{n+1} = 0$ is of length at least λ_1. Since

$$\|(\underline{e}, M)\|^2 = \|\underline{e}\|^2 + M^2 = 2M^2 < 2\lambda_1^2/4$$

the vector $(\underline{e}, \pm M)$ has length at most $\lambda_1/\sqrt{2}$. Since $\underline{v}$ is a closest vector to $\underline{w}$ it follows that $\|\underline{e}\| \leq \|\underline{e} + \underline{x}\|$ for all $\underline{x} \in L$ and so every other vector $(\underline{u}, M) \in L'$ has length at least as large. Finally, suppose $|l_{n+1}| \geq 2$. Then

$$\|(\underline{u}, l_{n+1}M)\|^2 \geq \|(0, l_{n+1}M)\|^2 \geq (2M)^2$$

and so $\|(\underline{u}, l_{n+1}M)\| \geq 2\|(\underline{e}, M)\|$. □

Lemma 18.3.2 shows that the CVP can be reduced to SVP as long as the target vector is very close to a lattice vector, and assuming one has a good guess M for the distance. However, when using algorithms such as LLL that solve the approximate SVP it is not possible, in general, to make rigorous statements about the success of the embedding technique. As mentioned earlier, the LLL algorithm often works better than the theoretical analysis predicts. Hence the embedding technique can potentially be useful even when $\underline{w}$ is not so close to a lattice point. For further discussion see Lemma 6.15 of Kannan [330].

Exercise 18.3.3. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a basis for a lattice in $\mathbb{R}^n$ and let $\underline{w} \in \mathbb{R}^n$. Let $M = \max_{1 \leq i \leq n} \|\underline{b}_i\|$. Show that the output $(\underline{e}, M)$ of the embedding technique (using LLL) on the basis of equation (18.3) is the same as the output of the Babai nearest plane algorithm when run on the LLL-reduced basis.

Exercise 18.3.4. Solve the following CVP instance using the embedding technique and a computer algebra package.

$$B = \begin{pmatrix} -265 & 287 & 56 \\ -460 & 448 & 72 \\ -50 & 49 & 8 \end{pmatrix}, \qquad \underline{w} = (100, 80, 100).$$

18.4 Enumerating all Short Vectors

We present a method to enumerate all short vectors in a lattice, given any basis. We will show later that the performance of this enumeration algorithm depends on the quality of the lattice basis. Throughout this section, $\|\underline{v}\|$ denotes the Euclidean norm.

The first enumeration method was given by Pohst in 1981. Further variants were given by Finke and Pohst, Kannan [329, 330], Helfrich [281] and Schnorr and Euchner [526]. These methods are all deterministic and are guaranteed to output a non-zero vector of minimum length. The time complexity is exponential in the lattice dimension, but the storage requirements are polynomial. This approach is known by the name "sphere decoding" in the communications community (see [440]).

Exercise 18.4.1. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an (ordered) basis in $\mathbb{R}^m$ for a lattice and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation. Let $\underline{v} \in \mathbb{R}^m$. Show that the projection of $\underline{v}$ onto $\underline{b}_i^*$ is

$$\frac{\langle \underline{v}, \underline{b}_i^* \rangle}{\|\underline{b}_i^*\|^2} \underline{b}_i^*.$$

Show that if $\underline{v} = \sum_{j=1}^n x_j \underline{b}_j$ then this projection is

$$\left(x_i + \sum_{j=i+1}^n x_j \mu_{j,i} \right) \underline{b}_i^*.$$

Lemma 18.4.2. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an (ordered) basis for a lattice and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation. Fix $A \in \mathbb{R}_{>0}$ and write $B_i = \|\underline{b}_i^*\|^2$. Let $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i$ be such that $\|\underline{v}\|^2 \leq A$. For $1 \leq i \leq n$ define*

$$z_i = x_i + \sum_{j=i+1}^n \mu_{j,i} x_j.$$

Then for $1 \leq i < n$

$$\sum_{i=1}^n z_i^2 B_i \leq A.$$

Proof: Exercise 18.4.1 gives a formula $z_i \underline{b}_i^*$ for the projection of $\underline{v}$ onto each $\underline{b}_i^*$. Since the vectors $\underline{b}_i^*$ are orthogonal we have

$$\|\underline{v}\|^2 = \sum_{i=1}^n \|z_i \underline{b}_i^*\|^2 = \sum_{i=1}^n z_i^2 B_i.$$

The result follows. □

Theorem 18.4.3. *Let the notation be as in Lemma 18.4.2. Then one has $x_n^2 \leq A / \|\underline{b}_n^*\|^2$ and, for $1 \leq i < n$,*

$$\left(x_i + \sum_{j=i+1}^n \mu_{j,i} x_j \right)^2 B_i \leq A - \sum_{j=i+1}^n z_j^2 B_j.$$

Proof: Note that $z_n = x_n$ and Lemma 18.4.2 implies $z_n^2 B_n \leq A$, which proves the first statement. The second statement is also just a re-writing of Lemma 18.4.2. □

We now sketch the enumeration algorithm for finding all short lattice vectors $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i$, which follows from the above results. First, without loss of generality we may assume that $x_n \geq 0$. By Theorem 18.4.3 we know $0 \leq x_n \leq \sqrt{A/B_n}$. For each candidate x_n one knows that

$$(x_{n-1} + \mu_{n,n-1} x_n)^2 B_{n-1} \leq A - x_n^2 B_n$$

and so

$$|x_{n-1} + \mu_{n,n-1} x_n| \leq \sqrt{(A - x_n^2 B_n)/B_{n-1}}.$$

To phrase this as a bound on x_{n-1} one uses the fact that for any $a \in \mathbb{R}, b \in \mathbb{R}_{\geq 0}$, the solutions $x \in \mathbb{R}$ to $|x + a| \leq b$ satisfy $-(b + a) \leq x \leq b - a$. Hence, writing $M_1 = \sqrt{(A - x_n^2 B_n)/B_{n-1}}$ one has

$$-(M_1 + \mu_{n,n-1} x_n) \leq x_{n-1} \leq M_1 - \mu_{n,n-1} x_n.$$

Exercise 18.4.4. Generalise the above discussion to show that for $1 \leq i < n$ one has

$$-(M_1 + M_2) \leq x_i \leq M_1 - M_2$$

where

$$M_1 = \sqrt{\left(A - \sum_{j=i+1}^{n} x_j^2 B_j \right) / B_i}$$

and $M_2 = \sum_{j=i+1}^{n} \mu_{j,i} x_j$.

Exercise 18.4.5. Write pseudocode for the algorithm to enumerate all short vectors of a lattice.

The algorithm to find a non-zero vector of minimal length is then straightforward. Set A to be $\|\underline{b}_1\|^2$, enumerate all vectors of length at most A and, for each vector, compute the length. One is guaranteed to find a shortest vector in the lattice. Schnorr and Euchner [526] organised the search in a manner to minimise the running time.

The running time of this algorithm depends on the quality of the basis in several ways. First, it is evidently important to have a good bound A for the length of the shortest vector. Taking $A = \|\underline{b}_1\|^2$ is only sensible if $\underline{b}_1$ is already rather short; alternatively one may choose, say, $A = \sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}$ using the Gaussian heuristic (one can choose a small bound for A and then, if the search fails, increase A accordingly). Second, one sees that if $\underline{b}_n^*$ is very short then the algorithm searches a huge range of values for x_n, and similarly if $\underline{b}_{n-1}^*$ is very short etc. Hence, the algorithm performs best if the values $\|\underline{b}_i^*\|$ descrease rather gently.

To solve SVP in practice using enumeration one first performs LLL and other pre-computation to get a sufficiently nice basis. We refer to Kannan [329, 330], Schnorr and Euchner [526] and Agrell et al [7] for details. The best complexity statement in the literature is due to Hanrot and Stehlé.

Theorem 18.4.6. *(Hanrot and Stehlé [275]) There exists a polynomial $p(x, y) \in \mathbb{R}[x, y]$ such that, for any n-dimensional lattice L in $\mathbb{Z}^m$ with basis consisting of vectors with coefficients bounded by B, one can compute all the shortest non-zero vectors in L in at most $p(\log(B), m) n^{n/2e + o(n)}$ bit operations.*

Exercise 18.4.7. Let L be a lattice in $\mathbb{Z}^n$ that contains $q\mathbb{Z}^n$ for some integer q. Let $M \in \mathbb{N}$ be a fixed bound. Give an algorithm based on Wagner's technique (see Section 13.8) for finding vectors in L with all entries bounded by M. Determine the complexity of this algorithm.

Due to lack of space we refer to the original papers for further details about enumeration algorithms. Pujol and Stehlé [491] give an analysis of issues related to floating point implementation.

In practice the most efficient enumeration methods for the SVP are heuristic "pruning" methods. These methods are still exponential in the lattice dimension, and are not guaranteed to output the shortest vector. The extreme pruning algorithm of Gama, Nguyen and Regev [235] is currently the most practical method.

A quite different approach, leading to non-deterministic algorithms (in other words, the output is a non-zero vector in the lattice that, with high probability, has minimal length) is due to Ajtai, Kumar and Sivakumar (see [357] for a survey). The running time and storage requirements of the algorithm are both exponential in the lattice dimension. For some experimental results we refer to Nguyen and Vidick [465]. Micciancio and Voulgaris [424] have given an improved algorithm, still requiring exponential time and storage.

18.4.1 Enumeration of Closest Vectors

The above ideas can be adapted to list lattice points close to some $\underline{w} \in \mathbb{R}^n$. Let $A \in \mathbb{R}_{>0}$ and suppose we seek all $\underline{v} \in L$ such that $\|\underline{v} - \underline{w}\|^2 \leq A$. Write $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i = \sum_{i=1}^n z_i \underline{b}_i^*$ as before and write

$$\underline{w} = \sum_{i=1}^n y_i \underline{b}_i^*.$$

Then $\|\underline{v} - \underline{w}\|^2 \leq A$ is equivalent to

$$\sum_{i=1}^n (z_i - y_i)^2 \|\underline{b}_i^*\|^2 \leq A.$$

It follows that

$$y_n - \sqrt{A/B_n} \leq x_n \leq y_n + \sqrt{A/B_n}$$

and so on.

Lemma 18.4.8. *Let the notation be as above and define*

$$M_i = \sqrt{\left(A - \sum_{j=i+1}^n (z_j - y_j)^2 B_j\right)/B_i} \quad \text{and} \quad N_i = \sum_{j=i+1}^n \mu_{j,i} x_j$$

for $1 \leq i \leq n$. *If* $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i$ *satisfies* $\|\underline{v} - \underline{w}\|^2 \leq A$ *then, for* $1 \leq i \leq n$,

$$y_i - M_i - N_i \leq x_i \leq y_i + M_i - N_i$$

Exercise 18.4.9. Prove Lemma 18.4.8.

The paper by Agrell, Eriksson, Vardy and Zeger [7] gives an excellent survey and comparison of the various enumeration techniques. They conclude that the Schnorr-Euchner variant is much more efficient than the Pohst or Kannan versions.

18.5 Korkine-Zolotarev Bases

We present a notion of reduced lattice basis that has better properties than an LLL-reduced basis.

Definition 18.5.1. Let L be a lattice of rank n in $\mathbb{R}^m$. An ordered basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ for L is **Korkine-Zolotarev reduced**[1] if

1. $\underline{b}_1$ is a non-zero vector of minimal length in L;
2. $|\mu_{i,1}| < 1/2$ for $2 \leq i \leq n$;
3. the basis $\{\underline{b}_2 - \mu_{2,1}\underline{b}_1, \ldots, \underline{b}_n - \mu_{n,1}\underline{b}_1\}$ is Korkine-Zolotarev reduced (this is the orthogonal projection of the basis of L onto the orthogonal complement of $\underline{b}_1$)

where $\underline{b}_i^*$ is the Gram-Schmidt orthogonalisation and $\mu_{i,j} = \langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$.

One problem is that there is no known polynomial-time algorithm to compute a Korkine-Zolotarev basis.

[1] Some authors also call it Hermite-Korkine-Zolotarev (HKV) reduced.

Theorem 18.5.2. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a Korkine-Zolotarev reduced basis of a lattice L. Then*

1. *for $1 \leq i \leq n$,*
$$\frac{4}{i+3}\lambda_i^2 \leq \|\underline{b}_i\|^2 \leq \frac{i+3}{4}\lambda_i^2;$$
2.
$$\prod_{i=1}^{n} \|\underline{b}_i\|^2 \leq \left(\gamma_n^n \prod_{i=1}^{n} \frac{i+3}{4}\right) \det(L)^2.$$

Proof: See Theorem 2.1 and 2.3 of Lagarias, Lenstra and Schnorr [361]. □

As we have seen, for lattices of relatively small dimension it is practical to enumerate all short vectors. Hence one can compute a Korkine-Zolotarev basis for lattices of small dimension. Schnorr has developed the **block Korkine-Zolotarev** lattice basis reduction algorithm, which computes a Korkine-Zolotarev basis for small dimensional projections of the original lattice and combines this with the LLL algorithm. The output basis can be proved to be of a better quality than an LLL-reduced basis. This is the most powerful algorithm for finding short vectors in lattices of large dimension. Due to lack of space we are unable to present this algorithm; we refer to Schnorr [521] for details.

Chapter 19

Coppersmith's Method and Related Applications

An important application of lattice basis reduction is finding small solutions to polynomial equations $F(x) \equiv 0 \pmod{M}$ of degree $d > 1$. The main purpose of this chapter is to present some results of Coppersmith [141] on this problem. We also discuss finding small roots of bivariate integer polynomials and some other applications of these ideas.

In general, finding solutions to modular equations is easy if we know the factorisation of the modulus, see Section 2.12. However, if the factorisation of the modulus M is not known then finding solutions can be hard. For example, if we can find a solution to $x^2 \equiv 1 \pmod{M}$ that is not $x = \pm 1$ then we can split M. Hence, we do not expect efficient algorithms for finding all solutions to modular equations in general.

Suppose then that the polynomial equation has a "small" solution. It is not so clear that finding the roots is necessarily a hard problem. The example $x^2 \equiv 1 \pmod{M}$ no longer gives any intuition since the two non-trivial roots both have absolute value at least $\sqrt{M}$. As we will explain in this chapter, if $F(x) \equiv 0 \pmod{M}$ of degree d has a solution x_0 such that $|x_0| < M^{1/d-\epsilon}$ for small $\epsilon > 0$ then it can be found in polynomial-time. This result has a number of important consequences.

General references for the contents of this chapter are Coppersmith [141, 142], May [410, 411], Nguyen and Stern [463] and Nguyen [456].

19.1 Coppersmith's Method for Modular Univariate Polynomials

19.1.1 First Steps to Coppersmith's Method

We sketch the basic idea of the method, which goes back to Håstad. Let $F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a monic polynomial of degree d with integer coefficients. Suppose we know that there exist one or more integers x_0 such that $F(x_0) \equiv 0 \pmod{M}$ and that $|x_0| < M^{1/d}$. The problem is to find all such roots.

Since $|x_0^i| < M$ for all $0 \leq i \leq d$ then, if the coefficients of $F(x)$ are small enough, one might have $F(x_0) = 0$ over $\mathbb{Z}$. The problem of finding integer roots of integer polynomials is easy: we can find roots over $\mathbb{R}$ using numerical analysis (e.g., Newton's method) and then round the approximations of the roots to the nearest integer and check whether they are solutions of $F(x)$.

The problem is therefore to deal with polynomials $F(x)$ having a small solution but whose coefficients are not small. Coppersmith's idea (in the formulation of Howgrave-Graham [296]) is to build from $F(x)$ a polynomial $G(x)$ that still has the same solution x_0, but which has coefficients small enough that the above logic does apply.

Example 19.1.1. Let $M = 17 \cdot 19 = 323$ and let

$$F(x) = x^2 + 33x + 215.$$

We want to find the small solution to $F(x) \equiv 0 \pmod{M}$ (in this case, $x_0 = 3$ is a solution, but note that $F(3) \neq 0$ over $\mathbb{Z}$).

We seek a related polynomial with small coefficients. For this example,

$$G(x) = 9F(x) - M(x+6) = 9x^2 - 26x - 3$$

satisfies $G(3) = 0$. This root can be found using Newton's method over $\mathbb{R}$ (or even the quadratic formula).

We introduce some notation for the rest of this section. Let $M, X \in \mathbb{N}$ and let $F(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$. Suppose $x_0 \in \mathbb{Z}$ is a solution to $F(x) \equiv 0 \pmod{M}$ such that $|x_0| < X$. We associate with the polynomial $F(x)$ the row vector

$$b_F = (a_0, a_1 X, a_2 X^2, \cdots, a_d X^d). \tag{19.1}$$

Vice versa, any such row vector corresponds to a polynomial. Throughout this section we will interpret polynomials as row vectors, and row vectors as polynomials, in this way.

Theorem 19.1.2. *(Howgrave-Graham [296]) Let $F(x), X, M, b_F$ be as above (i.e., there is some x_0 such that $|x_0| \leq X$ and $F(x_0) \equiv 0 \pmod{M}$). If $\|b_F\| < M/\sqrt{d+1}$ then $F(x_0) = 0$.*

Proof: Recall the Cauchy-Schwarz inequality $(\sum_{i=1}^{n} x_i y_i)^2 \leq (\sum_{i=1}^{n} x_i^2)(\sum_{i=1}^{n} y_i^2)$ for $x_i, y_i \in \mathbb{R}$. Taking $x_i \geq 0$ and $y_i = 1$ for $1 \leq i \leq n$ one has

$$\sum_{i=1}^{n} x_i \leq \sqrt{n \sum_{i=1}^{n} x_i^2}.$$

Now

$$|F(x_0)| = \left| \sum_{i=0}^{d} a_i x_0^i \right| \leq \sum_{i=0}^{d} |a_i||x_0|^i \leq \sum_{i=0}^{d} |a_i| X^i \leq \sqrt{d+1}\|b_F\| < \sqrt{d+1} M/\sqrt{d+1} = M$$

where the third inequality is Cauchy-Schwarz. so $-M < F(x_0) < M$. But $F(x_0) \equiv 0 \pmod{M}$ and so $F(x_0) = 0$. □

Let $F(x) = \sum_{i=0}^{d} a_i x^i$ be a monic polynomial. We assume that $F(x)$ has at least one solution x_0 modulo M such that $|x_0| < X$ for some specified integer X. If $F(x)$ is not monic but $\gcd(a_d, M) = 1$ then one can multiply $F(x)$ by $a_d^{-1} \pmod{M}$ to make it monic. If $\gcd(a_d, M) > 1$ then one can split M and reduce the problem to two (typically easier) problems. As explained above, to find x_0 it will be sufficient to find a polynomial $G(x)$ with the same root x_0 modulo M but with sufficiently small coefficients.

To do this, consider the $d+1$ polynomials $G_i(x) = Mx^i$ for $0 \leq i < d$ and $F(x)$. They all have the solution $x = x_0$ modulo M. Define the lattice L with basis corresponding to these polynomials (by associating with a polynomial the row vector in equation (19.1)). Therefore, the basis matrix for the lattice L is

$$B = \begin{pmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & MX & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & MX^{d-1} & 0 \\ a_0 & a_1 X & \cdots & a_{d-1}X^{d-1} & X^d \end{pmatrix}. \tag{19.2}$$

Every element of this lattice is a row vector that can be interpreted as a polynomial $F(x)$ (via equation (19.1) such that $F(x_0) \equiv 0 \pmod{M}$.

Lemma 19.1.3. *The dimension of the lattice L defined in equation (19.2) above is $d+1$ and the determinant is*

$$\det(L) = M^d X^{d(d+1)/2}.$$

Exercise 19.1.4. Prove Lemma 19.1.3.

One now runs the LLL algorithm on this (row) lattice basis. Let $G(x)$ be the polynomial corresponding to the first vector $\underline{b}_1$ of the LLL-reduced basis (since every row of B has the form of equation (19.1) then so does $\underline{b}_1$).

Theorem 19.1.5. *Let the notation be as above and let $G(x)$ be the polynomial corresponding to the first vector in the LLL-reduced basis for L. Set $c_1(d) = 2^{-1/2}(d+1)^{-1/d}$. If $X < c_1(d)M^{2/d(d+1)}$ then any root x_0 of $F(x)$ modulo M such that $|x_0| \leq X$ satisfies $G(x_0) = 0$ in $\mathbb{Z}$.*

Proof: Recall that $\underline{b}_1$ satisfies

$$\|\underline{b}_1\| \leq 2^{(n-1)/4} \det(L)^{1/n} = 2^{d/4} M^{d/(d+1)} X^{d/2}.$$

For $\underline{b}_1$ to satisfy the conditions of Howgrave-Graham's theorem (i.e., $\|\underline{b}_1\| < M/\sqrt{d+1}$) it is sufficient that

$$2^{d/4} M^{d/(d+1)} X^{d/2} < M/\sqrt{d+1}.$$

This can be written as

$$\sqrt{d+1}\, 2^{d/4} X^{d/2} < M^{1/(d+1)},$$

which is equivalent to the condition in the statement of the Theorem. □

In other words, if $d = 2$ then it is sufficient that $X \approx M^{1/3}$ to find the small solution using the above method. If $d = 3$ then it is sufficient that $X \approx M^{1/6}$. This is the result of Håstad. Of course, LLL often works better than the worst-case bound, so small solutions x_0 may be found even when x_0 does not satisfy the condition of the Theorem.

Example 19.1.6. Let $M = 10001$ and consider the polynomial

$$F(x) = x^3 + 10x^2 + 5000x - 222.$$

One can check that $F(x)$ is irreducible, and that $F(x)$ has the small solution $x_0 = 4$ modulo M. Note that $|x_0| < M^{1/6}$ so one expects to be able to find x_0 using the above method. Suppose $X = 10$ is the given bound on the size of x_0. Consider the basis matrix

$$B = \begin{pmatrix} M & 0 & 0 & 0 \\ 0 & MX & 0 & 0 \\ 0 & 0 & MX^2 & 0 \\ -222 & 5000X & 10X^2 & X^3 \end{pmatrix}.$$

Running LLL on this matrix gives a reduced basis, the first row of which is

$$(444, 10, -2000, -2000).$$

The polynomial corresponding to this vector is

$$G(x) = 444 + x - 20x^2 - 2x^3.$$

Running Newton's root finding method on $G(x)$ gives the solution $x_0 = 4$.

19.1.2 The Full Coppersmith Method

The method in the previous section allows one to find small roots of modular polynomials, but it can be improved further. Looking at the proof of Theorem 19.1.5 one sees that the requirement for success is essentially $M^d X^{d(d+1)/2} = \det(L) < M^{d+1}$ (more precisely, it is $2^{d/4} M^{d/(d+1)} X^{d/2} < M/\sqrt{d+1}$). There are two strategies to extend the utility of the method (i.e., to allow bigger values for X). The first is to increase the dimension n by adding rows to L that contribute less than M to the determinant. The second is to increase the power of M on the right hand side. One can increase the dimension without increasing the power of M by using the so-called "x-shift" polynomials $xF(x), x^2F(x), \ldots, x^kF(x)$; Example 19.1.7 gives an example of this. One can increase the power of M on the right hand side by using powers of $F(x)$ (since if $F(x_0) \equiv 0 \pmod{M}$ then $F(x_0)^k \equiv 0 \pmod{M^k}$).

Example 19.1.7. Consider the problem of Example 19.1.6. The lattice has dimension 4 and determinant M^3X^3. The condition for LLL to output a sufficiently small vector is

$$2^{3/4} \left(M^3 X^6\right)^{1/4} \leq \frac{M}{\sqrt{4}}$$

which, taking $M = 10001$, leads to $X \approx 2.07$. (Note that the method worked for a larger value of x_0; this is because the bound used on LLL only applies in the worst case.)

Consider instead the basis matrix that also includes rows corresponding to the polynomials $xF(x)$ and $x^2F(x)$

$$B = \begin{pmatrix} M & 0 & 0 & 0 & 0 & 0 \\ 0 & MX & 0 & 0 & 0 & 0 \\ 0 & 0 & MX^2 & 0 & 0 & 0 \\ -222 & 5000X & 10X^2 & X^3 & 0 & 0 \\ 0 & -222X & 5000X^2 & 10X^3 & X^4 & 0 \\ 0 & 0 & -222X^2 & 5000X^3 & 10X^4 & X^5 \end{pmatrix}.$$

The dimension is 6 and the determinant is M^3X^{15}. The condition for LLL to output a sufficiently small vector is

$$2^{5/4}\left(M^3X^{15}\right)^{1/6} \leq \frac{M}{\sqrt{6}},$$

which leads to $X \approx 3.11$. This indicates that some benefit can be obtained by using x-shifts.

Exercise 19.1.8. Let $G(x)$ be a polynomial of degree d. Show that taking d x-shifts $G(x), xG(x), \ldots, x^{d-1}G(x)$ gives a method that works for $X \approx M^{1/(2d-1)}$.

Exercise 19.1.8 shows that when $d = 3$ we have improved the result from $X \approx M^{1/6}$ to $X \approx M^{1/5}$. Coppersmith [141] exploits both x-shifts and powers of $F(x)$. We now present the method in full generality.

Theorem 19.1.9. *(Coppersmith) Let $0 < \epsilon < \min\{0.18, 1/d\}$. Let $F(x)$ be a monic polynomial of degree d with one or more small roots x_0 modulo M such that $|x_0| < \frac{1}{2}M^{1/d-\epsilon}$. Then x_0 can be found in time bounded by a polynomial in $d, 1/\epsilon$ and $\log(M)$.*

Proof: Let $h > 1$ be an integer that depends on d and ϵ and will be determined in equation (19.3) below. Consider the lattice L corresponding (via the construction of the previous section) to the polynomials $G_{i,j}(x) = M^{h-1-j}F(x)^j x^i$ for $0 \leq i < d$, $0 \leq j < h$. Note that $G_{i,j}(x_0) \equiv 0 \pmod{M^{h-1}}$. The dimension of L is dh. One can represent L by a lower triangular basis matrix with diagonal entries $M^{h-1-j}X^{jd+i}$. Hence the determinant of L is

$$\det(L) = M^{(h-1)hd/2}X^{(dh-1)dh/2}.$$

Running LLL on this basis outputs an LLL-reduced basis with first vector $\underline{b}_1$ satisfying

$$\|\underline{b}_1\| < 2^{(dh-1)/4}\det(L)^{1/dh} = 2^{(dh-1)/4}M^{(h-1)/2}X^{(dh-1)/2}.$$

This vector corresponds to a polynomial $G(x)$ of degree $dh-1$ such that $G(x_0) \equiv 0 \pmod{M^{h-1}}$. If $\|\underline{b}_1\| < M^{h-1}/\sqrt{dh}$ then Howgrave-Graham's result applies and we have $G(x_0) = 0$ over $\mathbb{Z}$.

Hence, it is sufficient that

$$\sqrt{dh}2^{(dh-1)/4}M^{(h-1)/2}X^{(dh-1)/2} < M^{h-1}.$$

Rearranging gives

$$\sqrt{dh}2^{(dh-1)/4}X^{(dh-1)/2} < M^{(h-1)/2},$$

which is equivalent to

$$c(d,h)X < M^{(h-1)/(dh-1)}$$

where $c(d,h) = (\sqrt{dh}2^{(dh-1)/4})^{2/(dh-1)} = \sqrt{2}(dh)^{1/(dh-1)}$.

Now

$$\frac{h-1}{dh-1} = \frac{1}{d} - \frac{d-1}{d(dh-1)}.$$

Equating $(d-1)/(d(dh-1)) = \epsilon$ gives

$$h = ((d-1)/(d\epsilon)+1)/d \approx 1/(d\epsilon). \tag{19.3}$$

Note that $dh = 1 + (d-1)/(d\epsilon)$ and so $c(d,h) = \sqrt{2}(1+(d-1)/(d\epsilon))^{d\epsilon/(d-1)}$, which converges to $\sqrt{2}$ as $\epsilon \to 0$. Since $X < \frac{1}{2}M^{1/d-\epsilon}$ we require $\frac{1}{2} \leq \frac{1}{c(d,h)}$. Writing $x =$

$d\epsilon/(d-1)$ this is equivalent to $(1+1/x)^x \leq \sqrt{2}$, which holds for $0 \leq x \leq 0.18$. Therefore, assume $\epsilon \leq (d-1)/d$.

Rounding h up to the next integer gives a lattice such that if

$$|x_0| < \tfrac{1}{2} M^{1/d-\epsilon}$$

then the LLL algorithm and polynomial root finding leads to x_0.

Since the dimension of the lattice is $dh \approx 1/\epsilon$ and the coefficients of the polynomials $G_{i,j}$ are bounded by M^h it follows that the running time of LLL depends on $d, 1/\epsilon$ and $\log(M)$. □

Exercise 19.1.10. Show that the precise complexity of Coppersmith's method is $O((1/\epsilon)^9 \log(M)^3)$ bit operations (recall that $1/\epsilon > d$). Note that if one fixes d and ϵ and considers the problem as M tends to infinity then one has a polynomial-time algorithm in $\log(M)$.

We refer to Section 3 of [142] for some implementation tricks that improve the algorithm. For example, one can add basis vectors to the lattice corresponding to polynomials of the form $M^{h-1}x(x-1)\cdots(x-i+1)/i!$.

Example 19.1.11. Let $p = 2^{30}+3$, $q = 2^{32}+15$ and $M = pq$. Consider the polynomial

$$\begin{aligned} F(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 \\ &= 1942528644709637042 + 1234567890123456789x + 98765432198765432 1x^2 + x^3, \end{aligned}$$

which has a root x_0 modulo M such that $|x_0| \leq 2^{14}$. Set $X = 2^{14}$. Note that $X \approx M^{1/4.4}$. One can verify that the basic method in Section 19.1.1 does not find the small root.

Consider the basis matrix (this is of smaller dimension than the lattice in the proof of Theorem 19.1.9 in the case $d = 3$ and $h = 3$)

$$\begin{pmatrix} M^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & M^2X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & M^2X^2 & 0 & 0 & 0 & 0 \\ Ma_0 & Ma_1X & Ma_2X^2 & MX^3 & 0 & 0 & 0 \\ 0 & Ma_0X & Ma_1X^2 & Ma_2X^3 & MX^4 & 0 & 0 \\ 0 & 0 & Ma_0X^2 & Ma_1X^3 & Ma_2X^4 & MX^5 & 0 \\ a_0^2 & 2a_0a_1X & (a_1^2+2a_0a_2)X^2 & (2a_0+2a_1a_2)X^3 & (a_2^2+2a_1)X^4 & 2a_2X^5 & X^6 \end{pmatrix}.$$

The dimension is 7 and the determinant is M^9X^{21}. The first vector of the LLL reduced basis is

$$(-369928294330603367352173305173409792, 14510574420259948322599626704027975 68, \ldots)$$

This corresponds to the polynomial

$$\begin{aligned} &-369928294330603367352173305173409792 + 8856551770178191114867936220720 2x \\ &\quad -34399873572584417286085706 59x^2 + 44635805764555189681925 8x^3 \\ &\quad +4564259979987386926x^4 - 1728007960413053x^5 - 21177681998x^6 \end{aligned}$$

which has $x_0 = 16384 = 2^{14}$ as a real root.

Exercise 19.1.12. Let $M = (2^{20}+7)(2^{21}+17)$ and $F(x) = x^3 + (2^{25} - 2883584)x^2 + 46976195x + 227$. Use Coppersmith's algorithm to find an integer x_0 such that $|x_0| < 2^9$ and $F(x_0) \equiv 0 \pmod{M}$.

Remark 19.1.13. It is natural to wonder whether one can find roots right up to the limit $X = M^{1/d}$. Indeed, the $-\epsilon$ term can be eliminated by performing an exhaustive search over the top few bits of the root x_0. An alternative way to proceed is to set $\epsilon = 1/\log_2(M)$, break the range $|x_0| < M^{1/d}$ of size $2M^{1/d}$ into $M^{2\epsilon} = 4$ intervals of size $2M^{1/d-2\epsilon} = M^{1/d-\epsilon}$, and perform Coppersmith's algorithm for each subproblem in turn.

Another question is whether one can go beyond the boundary $X = M^{1/d}$. A first observation is that for $X > M^{1/d}$ one does not necessarily expect a constant number of solutions; see Exercise 19.1.14. Coppersmith [142] gives further arguments why $M^{1/d}$ is the best one can hope for.

Exercise 19.1.14. Let $M = p^2$ and consider $F(x) = x^2 + px$. Show that if $X = M^{1/2+\epsilon}$ where $0 < \epsilon < 1/2$ then the number of solutions $|x| < X$ to $F(x) \equiv 0 \pmod{M}$ is $2M^{\epsilon}$,

Exercise 19.1.15. Let $N = pq$ be a product of two primes of similar size and let $e \in \mathbb{N}$ be a small integer such that $\gcd(e, \varphi(N)) = 1$. Let $1 < a, y < N$ be such that there is an integer $0 \leq x < N^{1/e}$ satisfying $(a + x)^e \equiv y \pmod{N}$. Show that, given N, e, a, y one can compute x in polynomial-time.

19.2 Multivariate Modular Polynomial Equations

Suppose one is given $F(x, y) \in \mathbb{Z}[x, y]$ and integers X, Y and M and is asked to find one or more roots (x_0, y_0) to $F(x, y) \equiv 0 \pmod{M}$ such that $|x_0| < X$ and $|y_0| < Y$. One can proceed using similar ideas to the above, hoping to find two polynomials $F_1(x, y), F_2(x, y) \in \mathbb{Z}[x, y]$ such that $F_1(x_0, y_0) = F_2(x_0, y_0) = 0$ over $\mathbb{Z}$, and such that the resultant $R_x(F_1(x, y), F_2(x, y)) \neq 0$ (i.e., that $F_1(x, y)$ and $F_2(x, y)$ are **algebraically independent**). This yields a heuristic method in general, since it is hard to guarantee the independence of $F_1(x, y)$ and $F_2(x, y)$.

Theorem 19.2.1. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a polynomial of total degree d (i.e., every monomial $x^i y^j$ satisfies $i + j \leq d$). Let $X, Y, M \in \mathbb{N}$ be such that $XY < M^{1/d-\epsilon}$ for some $0 < \epsilon < 1/d$. Then one can compute (in time polynomial in $\log(M)$ and $1/\epsilon > d$) polynomials $F_1(x, y), F_2(x, y) \in \mathbb{Z}[x, y]$ such that, for all $(x_0, y_0) \in \mathbb{Z}^2$ with $|x_0| < X$, $|y_0| < Y$ and $F(x_0, y_0) \equiv 0 \pmod{M}$, one has $F_1(x_0, y_0) = F_2(x_0, y_0) = 0$ over $\mathbb{Z}$.*

Proof: We refer to Jutla [324] and Section 6.2 of Nguyen and Stern [463] for a sketch of the details. □

19.3 Bivariate Integer Polynomials

We now consider $F(x, y) \in \mathbb{Z}[x, y]$ and seek a root $(x_0, y_0) \in \mathbb{Z}^2$ such that both $|x_0|$ and $|y_0|$ are small. Coppersmith has proved the following important result.

Theorem 19.3.1. *Let $F(x, y) \in \mathbb{Z}[x, y]$ and let $d \in \mathbb{N}$ be such that $\deg_x(F(x, y)), \deg_y(F(x, y)) \leq d$. Write*

$$F(x, y) = \sum_{0 \leq i,j \leq d} F_{i,j} x^i y^j.$$

For $X, Y \in \mathbb{N}$ define

$$W = \max_{0 \leq i,j, \leq d} |F_{i,j}| X^i Y^j.$$

If $XY < W^{2/(3d)}$ then there is an algorithm that takes as input $F(x, y), X, Y$, runs in time (bit operations) bounded by a polynomial in $\log(W)$ and 2^d, and outputs all pairs $(x_0, y_0) \in \mathbb{Z}^2$ such that $F(x_0, y_0) = 0$, $|x_0| \leq X$ and $|y_0| \leq Y$.

The condition in Theorem 19.3.1 is somewhat self-referential. If one starts with a polynomial $F(x,y)$ and bounds X and Y on the size of roots, then one can compute W and determine whether or not the algorithm will succeed in solving the problem.

Proof: (Outline) There are two proofs of this theorem, both of which are rather technical. The original by Coppersmith can be found in [141]. We sketch a simpler proof by Coron [150].

As usual we consider shifts of the polynomial $F(x,y)$. Choose $k \in \mathbb{N}$ (sufficiently large) and consider the k^2 polynomials

$$s_{a,b}(x,y) = x^a y^b F(x,y) \quad \text{for} \quad 0 \leq a,b < k$$

in the $(d+k)^2$ monomials $x^i y^j$ with $0 \leq i,j < d+k$. Coron chooses a certain set of k^2 monomials (specifically of the form $x^{i_0+i}y^{j_0+j}$ for $0 \leq i,j < k$ and fixed $0 \leq i_0, j_0 \leq d$) and obtains a $k^2 \times k^2$ matrix S with non-zero determinant M. (The most technical part of [150] is proving that this can always be done and bounding the size of M.)

One can now consider the $(d+k)^2$ polynomials Mx^iy^j for $0 \leq i,j < d+k$. Writing each polynomial as a row vector of coefficients, we now have a $k^2 + (d+k)^2$ by $(d+k)^2$ matrix. One can order the rows such that the matrix is of the form

$$\begin{pmatrix} S & * \\ MI_{k^2} & 0 \\ 0 & MI_w \end{pmatrix}$$

where $w = (d+k)^2 - k^2$, $*$ represents a $k^2 \times w$ matrix, and I_w denotes the $w \times w$ identity matrix.

Now, since $M = \det(S)$ there exists an integer matrix S' such that $S'S = MI_{k^2}$. Perform the row operations

$$\begin{pmatrix} I_{k^2} & 0 & 0 \\ -S' & I_{k^2} & 0 \\ 0 & 0 & I_w \end{pmatrix} \begin{pmatrix} S & * \\ MI_{k^2} & 0 \\ 0 & MI_w \end{pmatrix} = \begin{pmatrix} S & * \\ 0 & T \\ 0 & MI_w \end{pmatrix}$$

for some $k^2 \times w$ matrix T. Further row operations yield a matrix of the form

$$\begin{pmatrix} S & * \\ 0 & T' \\ 0 & 0 \end{pmatrix}$$

for some $w \times w$ integer matrix T'.

Coron considers a lattice L corresponding to T' (where the entries in a column corresponding to monomial x^iy^j are multiplied by X^iY^j as in equation (19.2)) and computes the determinant of this lattice. Lattice basis reduction yields a short vector that corresponds to a polynomial $G(x,y)$ with small coefficients such that every root of $F(x,y)$ is a root of $G(x,y)$ modulo M. If (x_0,y_0) is a sufficiently small solution to $F(x,y)$ then, using an analogue of Theorem 19.1.2, one infers that $G(x_0,y_0) = 0$ over $\mathbb{Z}$.

A crucial detail is that $G(x,y)$ has no common factor with $F(x,y)$. To show this suppose $G(x,y) = F(x,y)A(x,y)$ for some polynomial (we assume that $F(x,y)$ is irreducible, if not then apply the method to its factors in turn). Then $G(x,y) = \sum_{0 \leq i,j < k} A_{i,j} x^i y^j F(x,y)$ and so the vector of coefficients of $G(x,y)$ is a linear combination of the coefficient vectors of the k^2 polynomials $s_{a,b}(x,y)$ for $0 \leq a,b < k$. But this vector is also a linear combination of the rows of the matrix $(0\ T')$ in the original lattice. Considering the first k^2 columns (namely the columns of S), one has a linear dependence of the rows in S. Since $\det(S) \neq 0$ this is a contradiction.

It follows that the resultant $R_x(F,G)$ is a non-zero polynomial, and so one can find all solutions by finding the integer roots of $R_x(F,G)(y)$ and then solving for x.

To determine the complexity it is necessary to compute the determinant of T' and to bound M. Coron shows that the method works if $XY < W^{2/(3d)-1/k}2^{-9d}$. To get the stated running time for $XY < W^{2/(3d)}$ Coron proposes setting $k = \lfloor \log(W) \rfloor$ and performing exhaustive search on the $O(d)$ highest-order bits of x_0 (i.e., running the algorithm a polynomial in 2^d times). □

Example 19.3.2. Consider $F(x,y) = axy + bx + cy + d = 127xy - 1207x - 1461y + 21$ with $X = 30, Y = 20$. Let $M = 127^4$ (see below).

Consider the 13×9 matrix (this is taking $k = 2$ in the above proof and introducing the powers X^iY^j from the start)

$$B = \begin{pmatrix} aX^2Y^2 & bX^2Y & cXY^2 & dXY & 0 & 0 & 0 & 0 & 0 \\ 0 & aX^2Y & 0 & cXY & bX^2 & 0 & dX & 0 & 0 \\ 0 & 0 & aXY^2 & bXY & 0 & cY^2 & 0 & dY & 0 \\ 0 & 0 & 0 & aXY & 0 & 0 & bX & cY & d \\ MX^2Y^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & MX^2Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & M \end{pmatrix}.$$

We take S to be the matrix

$$\begin{pmatrix} a & b & c & d \\ 0 & a & 0 & c \\ 0 & 0 & a & b \\ 0 & 0 & 0 & a \end{pmatrix}$$

corresponding to the monomials $x^{i_0+i}y^{j_0+j}$ for $0 \le i,j < 2$ and fixed $i_0 = j_0 = 1$. Note that $M = \det(S) = a^4 = 127^4$.

Rather than diagonalising using the method of the proof of Theorem 19.3.1 we compute the Hermite normal form of B. This gives the matrix

$$B' = \left(\begin{array}{ccccccccc} aX^2Y^2 & * & * & * & * & * & * & * & * \\ & aX^2Y & * & * & * & * & * & * & * \\ & & aXY^2 & * & * & * & * & * & * \\ & & & aXY & * & * & * & * & * \\ \hline & & & & 16129X^2 & 16129Y^2 & 100125X & 1064641Y & 202558777 \\ & & & & & 2048383Y^2 & * & * & * \\ & & & & & & 2048383X & * & * \\ & & & & & & & 260144641Y & * \\ & & & & & & & & 260144641 \\ \hline & & & & & & & & \end{array}\right)$$

where blanks are zeroes and $*$ denotes an entry whose value we do not bother to write down. Let L be the 5×5 diagonal matrix formed of columns 5 to 9 of rows 5 to 9 of B'. Performing LLL-reduction on L gives a matrix whose first row is

$$(-16129X^2, -16129Y^2, 1048258X, 983742Y, -28446222)$$

corresponding to the polynomial

$$G(x,y) = -16129x^2 - 16129y^2 + 1048258x + 983742y - 28446222.$$

Clearly $G(x,y)$ is not a multiple of $F(x,y)$, since it has no xy term. Computing resultants and factoring gives the solutions $(x,y) = (21,21)$ and $(23,19)$.

Exercise 19.3.3. The polynomial

$$F(x,y) = 131xy - 1400x + 20y - 1286$$

has an integer solution with $|x| < 30$ and $|y| < 20$. Use Coron's method as in Example 19.3.2 to find (x,y).

The results of this section can be improved by taking into account the specific shape of the polynomial $F(x,y)$. We refer to Blömer and May [72] for details.

Finally, we remark that results are also known for integer polynomials having three or more variables, but these are heuristic in the sense that the method produces a list of polynomials having small roots in common, but there is no guarantee that the polynomials are algebraically independent.

19.4 Some Applications of Coppersmith's method

19.4.1 Fixed Padding Schemes in RSA

As discussed in Chapter 1, it is necessary to use padding schemes for RSA encryption (for example, to increase the length of short messages and to prevent algebraic relationships between the messages and ciphertexts). One simple proposal for κ-bit RSA moduli is to take a κ' bit message and pad it by putting $(\kappa - \kappa' - 1)$ ones to the left hand side of it. This brings a short message to full length. This padding scheme is sometimes called **fixed pattern padding**; we discuss it further in Section 24.4.5.

Suppose short messages (for example, 128-bit AES keys K) are being encrypted using this padding scheme with $\kappa = 1024$. Then

$$\mathsf{m} = 2^{1024} - 2^{128} + K.$$

Suppose also that the encryption exponent is $e = 3$. Then the ciphertext is

$$\mathsf{c} = \mathsf{m}^3 \pmod{N}.$$

If such a ciphertext is intercepted then the cryptanalyst only needs to find the value for K. In this case we know that K is a solution to the polynomial

$$F(x) = (2^{1024} - 2^{128} + x)^3 - \mathsf{c} \equiv 0 \pmod{N}.$$

This is a polynomial of degree 3 with a root modulo N of size at most $N^{128/1024} = N^{1/8}$. So Coppersmith's method finds the solution K in polynomial-time.

Example 19.4.1. Let $N = 887355420159847950880463233536 1$ (which is a 103 bit integer) and suppose Bob is sending 10-bit keys K to Alice using the padding scheme $\mathsf{m} = 2^{100} - 2^{10} + K$.

Suppose we have intercepted the ciphertext $\mathsf{c} = 809057455777566200535445549107 6$ and wish to find K. Let $X = 2^{10}$. We write $F(x) = (x + 2^{100} - 2^{10})^3 - \mathsf{c} = x^3 + a_2x^2 + a_1x + a_0$ and define

$$B = \begin{pmatrix} N & 0 & 0 & 0 \\ 0 & NX & 0 & 0 \\ 0 & 0 & NX^2 & 0 \\ a_0 & a_1X & a_2X^2 & X^3 \end{pmatrix}.$$

Performing lattice reduction and taking the first row vector gives the polynomial with factorisation

$$(x - 987)(-9207355675409153762 97 + 726745175435904508x + 277605904865853x^2).$$

One can verify that the message is $K = 987$.

19.4.2 Factoring $N = pq$ with Partial Knowledge of p

Let $N = pq$ and suppose we are given an approximation $\tilde{p}$ to p such that $p = \tilde{p} + x_0$ where $|x_0| < X$. For example, suppose p is a 2κ-bit prime and $\tilde{p}$ is an integer that has the same κ most significant bits as p (so that $|p - \tilde{p}| < 2^\kappa$). Coppersmith used his ideas to get an algorithm for finding p given N and $\tilde{p}$. Note that Coppersmith originally used a bivariate polynomial method, but we present a simpler version following work of Howgrave-Graham, Boneh, Durfee and others.

The polynomial $F(x) = (x+\tilde{p})$ has a small solution modulo p. The problem is that we don't know p, but we do know a multiple of p (namely, N). The idea is to form a lattice corresponding to polynomials that have a small root modulo p and to apply Coppersmith's method to find this root x_0. Once we have x_0 then we compute p as $\gcd(N, F(x_0))$.

Theorem 19.4.2. *Let $N = pq$ with $p < q < 2p$. Let $0 < \epsilon < 1/4$, and suppose $\tilde{p} \in \mathbb{N}$ is such that $|p-\tilde{p}| \leq \frac{1}{2\sqrt{2}} N^{1/4-\epsilon}$. Then given N and $\tilde{p}$ one can factor N in time polynomial in $\log(N)$ and $1/\epsilon$.*

Proof: Write $F(x) = (x + \tilde{p})$ and note that $\sqrt{N/2} \leq p \leq \sqrt{N}$. Let $X = \lfloor \frac{1}{2\sqrt{2}} N^{1/4-\epsilon} \rfloor$.

We describe the lattice to be used. Let $h \geq 4$ be an integer to be determined later and let $k = 2h$. Consider the $k + 1$ polynomials

$$N^h, N^{h-1}F(x), N^{h-2}F(x)^2, \ldots, NF(x)^{h-1}, F(x)^h, xF(x)^h, \ldots, x^{k-h}F(x)^h.$$

Note that if $p = \tilde{p} + x_0$ and if $G(x)$ is one of these polynomials then $G(x_0) \equiv 0 \pmod{p^h}$.

Consider the lattice corresponding to the above polynomials. More precisely, a basis for the lattice is obtained by taking each polynomial $G(x)$ above and writing the vector of coefficients of the polynomial $G(x)$ as in equation (19.1). The lattice has dimension $k + 1$ and determinant $N^{h(h+1)/2}X^{k(k+1)/2}$.

Applying LLL gives a short vector and, to apply Howgrave-Graham's result, we need $2^{k/4} \det(L)^{1/(k+1)} < p^h/\sqrt{k+1}$. Hence, since $p > (N/2)^{1/2}$, it is sufficient that $\sqrt{k+1}\, 2^{k/4} N^{h(h+1)/(2(k+1))} X^{k/2} < (N/2)^{h/2}$. Re-arranging gives

$$X < N^{h/k - h(h+1)/(k(k+1))} 2^{-h/k} 2^{-1/2} / (k+1)^{1/k}.$$

Since $k \geq 7$ we have $(k+1)^{1/k} = 2^{\log_2(k+1)/k} \leq 2^{1/2}$ and so $1/(k+1)^{1/k} \geq 1/\sqrt{2}$.

Now, since $k = 2h$ we find that the result holds if

$$X < N^{1/2(1-(h+1)/(2h+1))} \frac{1}{2\sqrt{2}}.$$

Since $1/2(1-(h+1)/(2h+1)) = 1/4-1/(4(2h+1))$ the result will follow if $1/(4(2h+1)) < \epsilon$. Taking $h \geq \max\{4, 1/(4\epsilon)\}$ is sufficient. □

One can obtain a more general version of Theorem 19.4.2. If $p = N^\alpha$ and $|x| \leq N^\beta$ where $0 < \alpha, \beta < 1$ then, ignoring constants, the required condition in the proof is

$$\frac{h(h+1)}{2} + \frac{\beta k(k+1)}{2} < \alpha h(k+1).$$

Taking $h = \sqrt{\beta}k$ and simplifying gives $\beta < \alpha^2$. The case we have shown is $\alpha = 1/2$ and $\beta < 1/4$. For details see Exercise 19.4.5 or Theorems 6 and 7 of May [410].

Example 19.4.3. Let $N = 16803551$, $\tilde{p} = 2830$ and $X = 10$.

Let $F(x) = (x + \tilde{p})$ and consider the polynomials $N, F(x), xF(x) = (x^2 + \tilde{p}x)$ and $x^2F(x)$, which all have the same small solution x_0 modulo p.

We build the lattice corresponding to these polynomials (with the usual method of converting a polynomial into a row vector). This lattice has basis matrix

$$\begin{pmatrix} N & 0 & 0 & 0 \\ \tilde{p} & X & 0 & 0 \\ 0 & \tilde{p}X & X^2 & 0 \\ 0 & 0 & \tilde{p}X^2 & X^3 \end{pmatrix}.$$

The first row of the output of the LLL algorithm on this matrix is $(105, -1200, 800, 1000)$, which corresponds to the polynomial

$$G(x) = x^3 + 8x^2 - 120x + 105.$$

The polynomial has the root $x = 7$ over $\mathbb{Z}$. We can check that $p = \tilde{p} + 7 = 2837$ is a factor of N.

Exercise 19.4.4. Let $N = 22461580086470571723189523$ and suppose you are given the approximation $\tilde{p} = 2736273600000$ to p, which is correct up to a factor $0 \leq x < X = 50000$. Find the prime factorisation of N using Coppersmith's method.

Exercise 19.4.5. Let $\epsilon > 0$. Let $F(x)$ be a polynomial of degree d such that $F(x_0) \equiv 0 \pmod{M}$ for some $M \mid N$, $M = N^\alpha$ and $|x_0| \leq \frac{1}{2}N^{\alpha^2/d-\epsilon}$. Generalise the proof of Theorem 19.4.2 to show that given $F(x)$ and N one can compute x_0 in time polynomial in $\log(N)$, d and $1/\epsilon$.

Exercise 19.4.6. Coppersmith showed that one can factor N in time polynomial in $\log(N)$ given $\tilde{p}$ such that $|p - \tilde{p}| < N^{1/4}$. Prove this result.

Exercise 19.4.7. Use Coppersmith's method to give an integer factorisation algorithm requiring $\tilde{O}(N^{1/4})$ bit operations. (A factoring algorithm with this complexity was also given in Section 12.5.)

Exercise 19.4.8. Show that the method of this section also works if given $\tilde{p}$ such that $|\tilde{p} - kp| < N^{1/4}$ for some integer k such that $\gcd(k, N) = 1$.

Exercise 19.4.9. Coppersmith also showed that one can factor N in time polynomial in $\log(N)$ given $\tilde{p}$ such that $p \equiv \tilde{p} \pmod{M}$ where $M > N^{1/4}$. Prove this result.

Exercise 19.4.10. Let $N = pq$ with $p \approx q$. Show that if one knows half the high order bits of p then one also knows approximately half the high order bits of q as well.

19.4.3 Factoring $p^r q$

As mentioned in Section 24.1.2, moduli of the form $p^r q$, where p and q are distinct primes and $r \in \mathbb{N}$, can be useful for some applications. When r is large then p is relatively small compared with N and so a natural attack is to try to factor N using the elliptic curve method.

Boneh, Durfee and Howgrave-Graham [79] considered using Coppersmith's method to factor integers of the form $N = p^r q$ when r is large. They observed that if one knows r and an approximation $\tilde{p}$ to p then there is a small root of the polynomial equation

$$F(x) = (\tilde{p} + x)^r \equiv 0 \pmod{p^r}$$

and that p^r is a large factor of N. One can therefore apply the technique of Section 19.4.2

The algorithm is to repeat the above for all $\tilde{p}$ in a suitably chosen set. An analysis of the complexity of the method is given in [79]. It is shown that if $r \geq \log(p)$ then the algorithm runs in polynomial-time and that if $r = \sqrt{\log_2(p)}$ then the algorithm is asymptotically faster than using the elliptic curve method. One specific example mentioned in [79] is that if $p, q \approx 2^{512}$ and $r = 23$ then $N = p^r q$ should be factored more quickly by their method than with the elliptic curve method.

Exercise 19.4.11. Let $N = p^r q$ where $p \approx q$, and so $p \approx N^{1/(r+1)}$. Show that one can factor N in $O(N^{1/(r+1)^2+\epsilon})$ bit operations. In particular, one can factor integers $N = p^2 q$ in roughly $\tilde{O}(N^{1/9})$ bit operations and integers $N = p^3 q$ in roughly $\tilde{O}(N^{1/16})$ bit operations.

When r is small it is believed that moduli of the form $N = p^r q$ are still hard to factor. For 3076 bit moduli, taking $r = 3$ and $p, q \approx 2^{768}$ should be such that the best known attack requires at least 2^{128} bit operations.

Exercise 19.4.12. The integer 876701170324027 is of the form $p^3 q$ where $|p - 5000| < 10$. Use the method of this section to factor N.

19.4.4 Chinese Remaindering with Errors

Boneh [75], building on work of Goldreich, Ron and Sudan [257], used ideas very similar to Coppersmith's method to give an algorithm for the following problem in certain cases.

Definition 19.4.13. Let $X, p_1, \ldots, p_n, r_1, \ldots, r_n \in \mathbb{Z}_{\geq 0}$ be such that $p_1 < p_2 < \cdots < p_n$ and $0 \leq r_i < p_i$ for all $1 \leq i \leq n$. Let $1 \leq e \leq n$ be an integer. The **Chinese remaindering with errors problem** (or **CRT list decoding problem**) is to compute an integer $0 \leq x < X$ (if it exists) such that

$$x \equiv r_i \pmod{p_i}$$

for all but e of the indices $1 \leq i \leq n$.

Note that it is not assumed that the integers p_i are coprime, though in many applications they will be distinct primes or prime powers. Also note that there is not necessarily a solution to the problem (for example, if X and/or e are too small).

Exercise 19.4.14. A naive approach to this problem is to run the Chinese remainder algorithm for all subsets $S \subseteq \{p_1, \ldots, p_n\}$ such that $\#S = (n - e)$. Determine the complexity of this algorithm. What is the input size of a Chinese remainder with errors instance when $0 \leq r_i < p_i$? Show that this algorithm is not polynomial in the input size if $e > \log(n)$.

The basic idea of Boneh's method is to construct a polynomial $F(x) \in \mathbb{Z}[x]$ such that all solutions x to the Chinese remaindering with errors problem instance are roots of $F(x)$ over $\mathbb{Z}$. This is done as follows. Define $P = \prod_{i=1}^{n} p_i$ and let $0 \leq R < P$ be the solution to the Chinese remainder instance (i.e., $R \equiv r_i \pmod{p_i}$ for all $1 \leq i \leq n$). For an integer x define the **amplitude** $\mathrm{amp}(x) = \gcd(P, x - R)$ so that, if the p_i are coprime and S is the set of indices $1 \leq i \leq n$ such that $x \equiv r_i \pmod{p_i}$, then $\mathrm{amp}(x) = \prod_{i \in S} p_i$. Write $F(x) = x - R$. The problem is precisely to find an integer x such that $|x| < X$ and $F(x) \equiv 0 \pmod{M}$ for some large integer $M \mid P$. This is the problem solved by Coppersmith's algorithm in the variant of Exercise 19.4.5. Note that $p_1^n \leq P \leq p_n^n$ and so $n \log(p_1) \leq \log(P) \leq n \log(p_n)$.

Theorem 19.4.15. *Let $X, e, p_1, \ldots, p_n, r_1, \ldots, r_n$ be an instance of the Chinese remainder with errors problem, where $p_1 < p_2 < \cdots < p_n$. Let $P = p_1 \cdots p_n$. There is an algorithm to compute all $x \in \mathbb{Z}$ such that $|x| < X$ and $x \equiv r_i \pmod{p_i}$ for all but e values $1 \leq i \leq n$ as long as*

$$e \leq n - n\frac{\log(p_n)}{\log(p_1)}\sqrt{\log(X)/\log(P)}.$$

The algorithm is polynomial-time in the input size.

Proof: Boneh [75] gives a direct proof, but we follow Section 4.7 of May [411] and derive the result using Exercise 19.4.5.

Let $0 \leq x < X$ be an integer with $M = \mathrm{amp}(x)$ being divisible by at least $n - e$ of the values p_i. We have $n \log(p_1) \leq \log(P) \leq n \log(p_n)$ and $(n-e)\log(p_1) \leq M \leq n \log(p_n)$. Write $M = P^{\beta}$. Then Coppersmith's algorithm finds x if $X < P^{\beta^2}$ in polynomial-time in n and $\log(p_n)$ (note that Exercise 19.4.5 states the result for $X < P^{\beta^2 - \epsilon}$ but we can remove the ϵ using the same ideas as Remark 19.1.13). Hence, it is sufficient to give a bound on e so that $\log(X)/\log(P) < \beta^2$ (i.e., $\beta > \sqrt{\log(X)/\log(P)}$). Now, $\beta = \log(M)/\log(P) \geq (n-e)\log(p_1)/(n\log(p_n))$. Hence, it is sufficient that

$$(n-e)\frac{\log(p_1)}{\log(p_n)} \geq n\sqrt{\log(X)/\log(P)},$$

which is equivalent to the equation in the Theorem. □

For convenience we briefly recall how to perform the computation. One chooses appropriate integers $a, a' \in \mathbb{N}$ and considers the lattice corresponding to the polynomials

$$\begin{aligned} G_i(x) &= P^{a-i}(x-R)^i \quad \text{for } 0 \leq i < a \\ H_i(x) &= (x-R)^a x^i \quad \text{for } 0 \leq i < a' \end{aligned}$$

that, by assumption, have at least one common small root x_0 modulo M^a. Using lattice basis reduction one finds a polynomial $F(x)$ that has small coefficients and that still has the same root x_0 modulo M^a. Applying Theorem 19.1.2 one finds that $F(x_0) = 0$ over $\mathbb{Z}$ if M^a is sufficiently large compared with x_0.

Exercise 19.4.16. Suppose $p_1, \ldots, p_n$ are the first n primes. Show that the above algorithm works when $e \approx n - \sqrt{n \log(X) \log(n)}$. Hence verify that Boneh's algorithm is polynomial-time in situations where the naive algorithm of Exercise 19.4.14 would be superpolynomial-time.

Bleichenbacher and Nguyen [70] discuss a variant of the Chinese remaindering with errors problem (namely, solving $x \equiv r_i \pmod{p_i}$ for small x, where each r_i lies in a set of m possible values) and a related problem in polynomial interpolation. Section 5 of [70] gives some algorithms for this "noisy CRT" problem.

Smooth Integers in Short Intervals

The above methods can be used to find smooth integers in intervals. Let $I = [U, V] = \{x \in \mathbb{Z} : U \leq x \leq V\}$ and suppose we want to find a B-smooth integer $x \in I$ if one exists (i.e., all primes dividing x are at most B). We assume that $V < 2U$.

Exercise 19.4.17. Show that if $V \geq 2U$ then one can compute a power of 2 in $[U, V]$.

A serious problem is that only rather weak results have been proven about smooth integers in short intervals (see Section 4 of Granville [267], Sections 6.2 and 7.2 of Naccache and Shparlinski [450] or Section 15.3). Hence, we cannot expect to be able to prove anything rigorous in this section. On the other hand, it is natural to conjecture that, at least most of the time, the probability that a randomly chosen integer in an short interval $[U, V]$ is B-smooth is roughly equal to the probability that a randomly chosen integer of size V is B-smooth. Multiplying this probability by the length of the interval gives a rough guide to whether it is reasonable to expect a solution (see Remark 15.3.5). Hence, for the remainder of this section, we assume that such an integer x exists. We now sketch how the previous results might be used to find x.

Let $W = (U+V)/2$ and $X = (V-U)/2$ so that $I = [W-X, W+X]$. We seek all $x \in \mathbb{Z}$ such that $|x| \leq X$ and $x \equiv -W \pmod{p_i^{e_i}}$ for certain prime powers where $p_i \leq B$. Then $W + x$ is a potentially smooth integer in the desired interval (we know that $W + x$ has a large smooth factor, but this may not imply that all prime factors of $W + x$ are small if W is very large). One therefore chooses $P = \prod_{i=1}^{l} p_i^{e_i}$ where $p_1, \ldots, p_l$ are the primes up to B and the e_i are suitably chosen exponents (e.g. $e_i = \lceil \log(W)/(\log(B)\log(p_i)) \rceil$). One then applies Boneh's algorithm. The output is an integer with a large common divisor with P (indeed, this is a special case of the approximate GCD problem considered in Section 19.6). Note that this yields rather "dense" numbers, in the sense that they are divisible by most of the first l primes.

Example 19.4.18. Let $P = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 232792560$. Let $W = 100000007 = 10^8 + 7$ and $X = 1000000 = 10^6$. We want to find an integer x between $W - X$ and $W + X$ such that x is divisible by most of the prime powers dividing P.

Taking $R = -W$, $a = 4$ and $a' = 3$ in the notation of Theorem 19.4.15 gives the lattice given by the basis matrix

$$\begin{pmatrix} P^4 & 0 & 0 & 0 & 0 & 0 & 0 \\ -RP^3 & P^3X & 0 & 0 & 0 & 0 & 0 \\ R^2P^2 & -2RP^2X & P^2X^2 & 0 & 0 & 0 & 0 \\ -R^3P & 3R^2PX & -3RPX^2 & PX^3 & 0 & 0 & 0 \\ R^4 & -4R^3X & 6R^2X^2 & -4RX^3 & X^4 & 0 & 0 \\ 0 & R^4X & -4R^3X^2 & 6R^2X^3 & -4RX^4 & X^5 & 0 \\ 0 & 0 & R^4X^2 & -4R^3X^3 & 6R^2X^4 & -4RX^5 & X^6 \end{pmatrix}.$$

The polynomial corresponding to the first row of the LLL-reduced basis is

$$F(x) = -7^4(x + 231767)^4$$

giving the solution $x = -231767$. Indeed

$$W - 231767 = 2^4 \cdot 3^3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$

Note that the algorithm does not output $10^8 = 2^8 \cdot 5^8$, since that number does not have a very large gcd with P.

Exercise 19.4.19. Repeat the above example for $W = 150000001 = 1.5 \cdot 10^8 + 1$ and $W = 46558000$.

If this process fails one can make adjustments to the value of P (for example, by changing the exponents e_i). Analysing the probability of success of this approach is an open problem.

19.5 Simultaneous Diophantine Approximation

Let $\alpha \in \mathbb{R}$. It is well-known that the continued fraction algorithm produces a sequence of rational numbers p/q such that $|\alpha - p/q| < 1/q^2$. This is the subject of **Diophantine approximation**; see Section 1.1 of Lovász [395] for background and discussion. We now define a natural and important generalisation of this problem.

Definition 19.5.1. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ and let $\epsilon > 0$. Let $Q \in \mathbb{N}$ be such that $Q \geq \epsilon^{-n}$. The **simultaneous Diophantine approximation problem** is to find $q, p_1, \ldots, p_n \in \mathbb{Z}$ such that $0 < q \leq Q$ and

$$|\alpha_i - p_i/q| \leq \epsilon/q \tag{19.4}$$

for all $1 \leq i \leq n$.

A theorem of Dirichlet mentioned in Section 1.1 of [395] and Section 17.3 of [238] shows that there is a solution satisfying the constraints in Definition 19.5.1.

Exercise 19.5.2. Let $\epsilon \geq 1/2$. Prove that integers $p_1, \ldots, p_n$ satisfying equation (19.4) exist for any n and q.

A major application of lattice reduction is to give an algorithm to compute the integers $(q, p_1, \ldots, p_n)$ in Definition 19.5.1. In practice the real numbers $\alpha_1, \ldots, \alpha_n$ are given to some decimal precision (and so are rational numbers with coefficients of some size). The size of an instance of the simultaneous Diophantine approximation is the sum of the bit lengths of the numerator and denominator of the given approximations to the α_i, together with the bit length of the representation of ϵ and Q. Let X be a bound on the absolute value of all numerators and denominators of the α_i. The computational task is to find a solution $(q, p_1, \ldots, p_n)$ in time that is polynomial in n, $\log(X)$, $\log(1/\epsilon)$ and $\log(Q)$.

Theorem 19.5.3. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ be given as rational numbers with numerator and denominator bounded in absolute value by X. Let $0 < \epsilon < 1$. One can compute in polynomial-time integers $(q, p_1, \ldots, p_n)$ such that $0 < q < 2^{n(n+1)/4}\epsilon^{-(n+1)}$ and $|\alpha_i - p_i/q| \leq \epsilon/q$ for all $1 \leq i \leq n$.*

Proof: Let $Q = 2^{n(n+1)/4}\epsilon^{-n}$ and consider the lattice $L \subseteq \mathbb{Q}^{n+1}$ with basis matrix

$$\begin{pmatrix} \epsilon/Q & \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & & \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & & \cdots & -1 \end{pmatrix}. \tag{19.5}$$

The dimension is $n+1$ and the determinant is $\epsilon/Q = 2^{-n(n+1)/4}\epsilon^{n+1}$. Every vector in the lattice is of the form $(q\epsilon/Q, q\alpha_1 - p_1, q\alpha_2 - p_2, \ldots, q\alpha_n - p_n)$. The entries of the lattice are ratios of integers with absolute value bounded by $\max\{X, 2^{n(n+1)/4}/\epsilon^{n+1}\}$.

Note that the lattice L does not have a basis with entries in $\mathbb{Z}$, but rather in $\mathbb{Q}$. By Remark 17.5.5 the LLL algorithm applied to L runs in $O(n^6 \max\{n\log(X), n^2 + n\log(1/\epsilon)\}^3)$ bit operations (which is polynomial in the input size) and outputs a non-zero vector $\underline{v} = (q\epsilon/Q, q\alpha_1 - p_1, \ldots, q\alpha_n - p_n)$ such that

$$\|\underline{v}\| \leq 2^{n/4}\det(L)^{1/(n+1)} = 2^{n/4}2^{-n/4}\epsilon = \epsilon < 1.$$

If $q = 0$ then $\underline{v} = (0, -p_1, \ldots, -p_n)$ with some $p_i \neq 0$ and so $\|\underline{v}\| \geq 1$, and so $q \neq 0$. Without loss of generality, $q > 0$. Since $\|\underline{v}\|_\infty \leq \|\underline{v}\|$ it follows that $q\epsilon/Q \leq \epsilon < 1$ and so $0 < q < Q/\epsilon = 2^{n(n+1)/4}\epsilon^{-(n+1)}$. Similarly, $|q\alpha_i - p_i| < \epsilon$ for all $1 \leq i \leq n$. □

Exercise 19.5.4. Let $\alpha_1 = 1.555111$, $\alpha_2 = 0.771111$ and $\alpha_3 = 0.333333$. Let $\epsilon = 0.01$ and $Q = 10^6$. Use the method of this section to find a good simultaneous rational approximation to these numbers.

See Section 17.3 of [238] for more details and references.

19.6 Approximate Integer Greatest Common Divisors

The basic problem is the following. Suppose positive integers a and b exist such that $d = \gcd(a, b)$ is "large". Suppose that one is not given a and b, but only approximations $\tilde{a}, \tilde{b}$ to them. The problem is to find d, a and b. One issue is that there can be surprisingly many solutions to the problem (see Example 19.6.4), so it may not be feasible to compute all solutions for certain parameters. On the other hand, in the case $\tilde{b} = b$ (i.e., one of the values is known exactly, which often happens in practice) then there are relatively few solutions.

Howgrave-Graham [297] has considered these problems and has given algorithms that apply in various situations. We present one of the basic ideas. Let $a = \tilde{a} + x$ and $b = \tilde{b} + y$. Suppose $\tilde{a} < \tilde{b}$ and define $q_a = a/d$ and $q_b = b/d$. Then, since $q_a/q_b = a/b$, we have

$$\frac{\tilde{a}}{\tilde{b}} - \frac{q_a}{q_b} = \frac{q_a y - q_b x}{\tilde{b}q_b}. \tag{19.6}$$

If the right hand side of equation (19.6) is small then performing Euclid's algorithm on $\tilde{a}/\tilde{b}$ gives a sequence of possible values for q_a/q_b. For each such value one can compute

$$\lfloor \tilde{b}/q_b \rceil = \lfloor (dq_b - y)/q_b \rceil = d + \lfloor -y/q_b \rceil.$$

If $|y| < \frac{1}{2}q_b$ then one has computed d exactly and can solve $\tilde{a} + x \equiv \tilde{b} + y \equiv 0 \pmod{d}$. Note that one must use the basic extended Euclidean algorithm, rather than the improved method using negative remainders as in Algorithm 1.

Exercise 19.6.1. Show that if $a < b < \tilde{b}$, $b^{2/3} < d < 2b^{2/3}$ and $|x|, |y| < \frac{1}{4}b^{1/3}$ then the above method finds d, a and b.

Exercise 19.6.2. Let the notation be as above. Suppose $|x|, |y| < \tilde{b}^\beta$ and $d = \tilde{b}^\alpha$. Explain why it is natural to assume $\alpha > \beta$. Show that the above method succeeds if (ignoring constant factors) $\beta < -1 + 2\alpha$ and $\beta < 1 - \alpha$

Exercise 19.6.3. Re-formulate this method in terms of finding a short vector in a 2×2 matrix. Derive the same conditions on α and β as in Exercise 19.6.2.

Example 19.6.4. Let $\tilde{a} = 617283157$ and $\tilde{b} = 630864082$. The first few convergents q_a/q_b to $\tilde{a}/\tilde{b}$ are $1, 45/46, 91/93, 409/418, 500/511, 1409/1440$ and $1909/1951$. Computing approximations to $\tilde{a}/q_a$ and $\tilde{b}/q_b$ for these values (except the first) gives the following table.

$\tilde{a}/q_a$	13717403.5	6783331.4	1509249.8	1234566.3	438100.2	323354.2
$\tilde{b}/q_b$	13714436.6	6783484.8	1509244.2	1234567.7	438100.1	323354.2

Any values around these numbers can be used as a guess for d. For example, taking $d = 13717403$ one finds $\tilde{a} - 22 \equiv \tilde{b} + 136456 \equiv 0 \pmod{d}$, which is a not particularly good solution.

The four values $d_1 = 1234566$, $d_2 = 1234567$, $d_3 = 438100$ and $d_4 = 323354$ lead to the solutions $\tilde{a} - 157 \equiv \tilde{b} - 856 \equiv 0 \pmod{d_1}$, $\tilde{a} + 343 \equiv \tilde{b} - 345 \equiv 0 \pmod{d_2}$, $\tilde{a} - 257 \equiv \tilde{b} - 82 \equiv 0 \pmod{d_3}$ and $\tilde{a} - 371 \equiv \tilde{b} - 428 \equiv 0 \pmod{d_4}$.

Howgrave-Graham gives a more general method for solving the problem that does not require such a strict condition on the size of y. The result relies on heuristic assumptions about Coppersmith's method for bivariate integer polynomials. We state this result as Conjecture 19.6.5.

Conjecture 19.6.5. *(Algorithm 14 and Section 4 of [297]) Let $0 < \alpha < 2/3$ and $\beta < 1 - \alpha/2 - \sqrt{1 - \alpha - \alpha^2/2}$. There is a polynomial-time algorithm that takes as input $\tilde{a} < \tilde{b}$ and outputs all integers $d > \tilde{b}^\alpha$ such that there exist integers x, y with $|x|, |y| < \tilde{b}^\beta$ and $d \mid (\tilde{a} + x)$ and $d \mid (\tilde{b} + y)$.*

Exercise 19.6.6. Let $\tilde{a}, \tilde{b}, X, Y \in \mathbb{N}$ be given with $X < \tilde{a} < \tilde{b}$. Give a brute force algorithm to output all $d > Y$ such that there exist $x, y \in \mathbb{Z}$ with $|x|, |y| \leq X$ and $d = \gcd(\tilde{a} + x, \tilde{b} + y)$. Show that the complexity of this algorithm is $O(X^2 \log(\tilde{b})^2)$ bit operations.

We now mention the case when $\tilde{b} = b$ (in other words, b is known exactly). The natural approach is to consider the polynomial $F(x) = \tilde{a} + x$, which has a small solution to the equation $F(x) \equiv 0 \pmod{d}$ for some $d \mid b$. Howgrave-Graham applies the method used in Section 19.4.2 to solve this problem.

Theorem 19.6.7. *(Algorithm 12 and Section 3 of [297]) Let $0 < \alpha < 1$ and $\beta < \alpha^2$. There is a polynomial-time algorithm that takes as input $\tilde{a}, b$ and outputs all integers $d > b^\alpha$ such that there exists an integer x with $|x| < b^\beta$ and $d \mid (\tilde{a} + x)$ and $d \mid b$.*

19.7 Learning with Errors

The learning with errors problem was proposed by Regev. There is a large literature on this problem; we refer to Micciancio and Regev [423] and Regev [496] for background and references.

Definition 19.7.1. Let $q \in \mathbb{N}$ (typically prime), $\sigma \in \mathbb{R}_{>0}$, and $n, m \in \mathbb{N}$ with $m > n$.[1] Let $\underline{s} \in (\mathbb{Z}/q\mathbb{Z})^n$. The **LWE distribution** is the distribution on $(\mathbb{Z}/q\mathbb{Z})^{m \times n} \times (\mathbb{Z}/q\mathbb{Z})^m$ corresponding to choosing uniformly at random an $m \times n$ matrix A with entries in $\mathbb{Z}/q\mathbb{Z}$ and a length m vector

$$\underline{c} \equiv A\underline{s} + \underline{e} \pmod{q}$$

[1] For theoretical applications one should not assume a fixed number m of rows for A. Instead, the attacker is given an oracle that outputs pairs $(\underline{a}, c)$ where $\underline{a}$ is a row of A and $c = \underline{a}\,\underline{s} + e \pmod{q}$.

where the vector $\underline{e}$ has entries chosen independently from a discretised normal distribution[2] on $\mathbb{Z}$ with mean 0 and standard deviation σ. The **learning with errors** problem (**LWE**) is: Given $(A, \underline{c})$ drawn from the LWE distribution, to compute the vector $\underline{s}$. The **decision learning with errors** problem (**DLWE**) is: Given A as above and a vector $\underline{c} \in (\mathbb{Z}/q\mathbb{Z})^m$, to determine whether $(A, \underline{c})$ is drawn from the uniform distribution, or the LWE distribution.

It is necessary to argue that LWE is well-defined since, for any choice $\underline{s}'$, the value $\underline{c} - A\underline{s}' \pmod q$ is a possible choice for $\underline{e}$. But, when m is sufficiently large, one value for $\underline{s}$ is much more likely to have been used than any of the others. Hence, LWE is a maximum likelihood problem. Similarly, DLWE is well-defined when m is sufficiently large: if $\underline{c}$ is chosen uniformly at random and independent of A then there is not likely to be a choice for $\underline{s}$ such that $\underline{c} - A\underline{s} \pmod q$ is significantly smaller than the other values $\underline{c} - A\underline{s}' \pmod q$. We do not make these arguments precise. It follows that m must be significantly larger than n for these problems to be meaningful. It is also clear that increasing m (but keeping n fixed) does not make the LWE problem harder.

We refer to [423] and [496] for surveys of cryptographic applications of LWE and reductions, from computational problems in lattices that are believed to be hard, to LWE. Note that the values m, q and σ in an LWE instance are usually determined by constraints coming from the cryptographic application, while n is the main security parameter.

Example 19.7.2. Table 3 of Micciancio and Regev [423] suggests the parameters

$$(n, m, q, \sigma) = (233, 4536, 32749, 2.8).$$

Lindner and Peikert [390] suggest (using Figure 4 and the condition $m \geq 2n + \ell$ with $\ell = 128$)

$$(n, m, q, \sigma) = (256, 640, 4093, 3.3).$$

Exercise 19.7.3. Show that if one can determine $\underline{e}$ then one can solve LWE efficiently.

Exercise 19.7.4.★ Show that, when q is prime, LWE $\leq_R$ DLWE. Show that DLWE $\leq_R$ LWE.

We now briefly sketch two lattice attacks on LWE. These attacks can be avoided by taking appropriate parameters. For other attacks on LWE see [496].

Example 19.7.5. (Lattice attack on DLWE using short vectors in kernel lattice modulo q.) Suppose one can find a short vector $\underline{w}$ in the lattice

$$\{\underline{w} \in \mathbb{Z}^m : \underline{w}A \equiv \underline{0} \pmod q\}.$$

Then $\underline{w}\,\underline{c} = \underline{w}A\underline{s} + \underline{w}\,\underline{e} \equiv \underline{w}\,\underline{e} \pmod q$. If $\underline{w}$ is short enough then one might expect that $\underline{w}\,\underline{e}$ is a small integer. On the other hand, if $\underline{c}$ is independent of A then $\underline{w}\,\underline{c} \pmod q$ is a random integer modulo q. Hence, one might be able to distinguish the LWE distribution from the uniform distribution using short enough vectors $\underline{w}$.

Note that one is not obliged to use all the rows of A in this attack, and so one can replace m by a much smaller value m'. For analysis of the best value for m', and for parameters that resist this attack, see Section 5.4.1 (especially equation (10)) of [423].

Example 19.7.6. (Reducing LWE to bounded distance decoding (BDD) or CVP.) We now consider a natural approach to solving LWE using lattices. Since we always use row

[2] In other words, the probability that e_i is equal to $x \in \mathbb{Z}$ is proportional to $e^{-x^2/(2\sigma^2)}$.

lattices, it is appropriate to take the transpose of LWE. Hence, suppose $\underline{c}, \underline{s}$ and $\underline{e}$ are row vectors (of lengths m, n and m respectively) such that $\underline{c} = \underline{s}A^T + \underline{e} \pmod{q}$.

Consider the lattice

$$L = \left\{ \underline{v} \in \mathbb{Z}^m : \underline{v} \equiv \underline{u}A^T \pmod{q} \text{ for some } \underline{u} \in \mathbb{Z}^n \right\}.$$

Then L has rank m and a basis matrix for it is computed by taking the (row) Hermite normal form of the $(n+m) \times m$ matrix

$$\begin{pmatrix} A^T \\ qI_m \end{pmatrix}$$

where I_m is an $m \times m$ identity matrix. One then tries to find an element $\underline{v}$ of L that is close to $\underline{c}$. Hopefully, $\underline{v} = \underline{c} - \underline{e} \equiv \underline{s}A^T \pmod{q}$. For usual LWE parameters we have that there is a unique $\underline{v} \in L$ that is very close to $\underline{c}$, and so the problem matches the bounded distance decoding problem.

One can perform lattice basis reduction and apply the nearest plane algorithm. For improved methods and experimental results see Lindner and Peikert [390]. As in Example 19.7.5 one can work with a subset of m' rows of A; see Section 5.1 of [390] for details.

19.8 Further Applications of Lattice Reduction

There are a number of other applications of lattices in cryptography. We briefly list some of them.

- The improvement by Boneh and Durfee of Wiener's attack on small private exponent RSA. This is briefly mentioned in Section 24.5.1.
- Solving the hidden number problem in finite fields and its applications to bit security of Diffie-Hellman key exchange. See Section 21.7.1.
- The attack by Howgrave-Graham and Smart on digital signature schemes in finite fields when there is partial information available about the random nonces. See Section 22.3.
- The deterministic reduction by Coron and May from knowing $\varphi(N)$ to factoring N. This is briefly mentioned in Section 24.1.3.

Cryptosystems Based on Lattices

We present some cryptosystems whose common feature is that they all rely on computational problems in lattices for their security. The subject of lattice based cryptography is very active and there have recently been new ideas that revolutionised the field. It is beyond the scope of this book to survey these recent developments.

19.9 The Goldreich-Goldwasser-Halevi Cryptosystem and Variants

The Goldreich-Goldwasser-Halevi (GGH) cryptosystem relies on the difficulty of the closest vector problem (CVP) in a lattice. The system is reminiscent of the McEliece cryptosystem, which we briefly recall in the next paragraph. Encryption for both systems is randomised.

In the McEliece cryptosystem one chooses an error correcting code (some references for error correcting codes are van Lint [391] and Chapter 18 of [609]) over a finite field $\mathbb{F}_q$ (typically $\mathbb{F}_2$) given by a $k \times n$ generator matrix G (where $k < n$) and publishes a "disguised" version $G' = SGP$ where S and P are suitable invertible matrices (we refer to Section 8.5 of Menezes, van Oorschot and Vanstone [418] for details). The public key is G' and the private key is (S, G, P). To encrypt a message $\underline{m} \in \mathbb{F}_q^k$ one computes $\underline{c} = \underline{m}G' + \underline{e}$ where $\underline{e} \in \mathbb{F}_q^n$ is a randomly chosen error vector of low Hamming weight; note that this computation is over $\mathbb{F}_q$. To decrypt one uses the decoding algorithm for the error correcting code.

The basic GGH public key encryption scheme is similar; we give an informal sketch of the idea now. One chooses a "nice" basis B for a full rank lattice $L \subset \mathbb{Z}^n$ and publishes a "disguised" basis $B' = UB$ for L where U is "random" unimodular matrix. A message $\underline{m} \in \mathbb{Z}^n$ is encrypted as $\underline{c} = \underline{m}B' + \underline{e}$ where $\underline{e}$ is a randomly chosen short error vector; note that this computation is over $\mathbb{Z}$. To decrypt one solves the closest vector problem, using the nice basis B, to obtain the lattice point $\underline{m}B'$ close to $\underline{c}$; one can then obtain $\underline{m}$.

While encryption is superficially the same for the McEliece and GGH cryptosystems, there are significant differences between the security analysis of these schemes. An advantage of the lattice approach is that the error vector is required to have less structure: it is only required to be short, compared with McEliece where the error vector must have low Hamming weight. Both schemes have ciphertexts larger than the messages but an advantage of McEliece is that ciphertexts have a fixed size whereas for GGH the coefficients are integers whose size can vary significantly.

Exercise 19.9.1. Show that any cryptosystem based on the McEliece or GGH idea does not have indistinguishability security under passive attack.

Exercise 19.9.2. A variant of the McEliece or GGH proposal is to swap the roles of the message and the randomness. In other words one encodes the message as a valid error vector $\underline{m}$, chooses a random $\underline{e} \in \mathbb{F}_q^k$ (respectively, $\underline{e} \in \mathbb{Z}^k$) and computes $\underline{c} = \underline{e}G' + \underline{m}$ (resp., $c = \underline{e}B' + \underline{m}$). Show that this variant also does not have indistinguishability security under passive attacks.

Exercise 19.9.3. Show that any cryptosystem based on the McEliece or GGH idea (and without any padding scheme) does not have one way encryption security under a CCA attack.

Exercises 19.9.1 and 19.9.3 show that the 'textbook' (i.e., without a padding scheme) McEliece and GGH cryptosystems should not be used in practice. Using techniques similar to those presented later for Elgamal and RSA one can prevent such attacks as long as the basic scheme is OWE-CPA secure (see Section 1.3.1 for the definition of this security notion). Hence, for the rest of this chapter we focus purely on the textbook versions and mainly consider security under passive attacks.

Exercise 19.9.4. Given a GGH public key B' show that there is more than one private basis matrix B that is suitable for decryption. Show that one can efficiently determine whether a guess B for a GGH private basis matrix can correspond to a given public basis B'.

To give a precise definition of the GGH cryptosystem it is necessary to give the following details:

1. What dimension n should be used?
2. How does one choose the "nice" lattice basis B and what properties should it have?
3. How does one choose the "random" unimodular matrix U?
4. What is the message space and how does one encode information into a vector $\underline{m}$?
5. How does one choose the error vector $\underline{e}$ and in what space does it lie?

We briefly sketch the proposal of Goldreich, Goldwasser and Halevi; the reader should refer to the original paper [256] for complete details. It is suggested to take $n \geq 200$. Two methods to generate the "nice" basis B are given: one is to choose a random matrix B with entries in, say, $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ (so that all vectors are relatively short); another is to choose $B = kI_n + E$ where I_n is the $n \times n$ identity matrix, $k > 1$ is a "medium sized" integer and E is a random matrix with small entries as in the first case above. Two methods to generate U are also given; in both cases the issue is to ensure that the coefficients of $B' = UB$ do not explode in size (we refer to Section 3.2 of [256] for details). The message space is the set of vectors of length n with entries in

$\{-M, -(M-1), \ldots, -1, 0, 1, \ldots, M-1, M\}$ for some $M \in \mathbb{N}$ ([256] actually suggests $M = n$). Finally, the error vector is chosen to be a random vector of length n with entries in $\{-\sigma, \sigma\}$ for some $\sigma \in \mathbb{N}$ (typically, $\sigma = 3$).

As mentioned above, to encrypt a message $\underline{m}$ one computes the ciphertext $\underline{c} = \underline{m}B' + \underline{e}$. To decrypt $\underline{c}$ one uses the Babai rounding technique with respect to the nice basis B for the lattice. More precisely, multiply $\underline{c}$ by B^{-1} to obtain

$$\underline{c}B^{-1} = (\underline{m}B' + \underline{e})B^{-1} = \underline{m}UBB^{-1} + \underline{e}B^{-1} = \underline{m}U + \underline{e}B^{-1} \in \mathbb{Q}^n.$$

The Babai rounding will remove the term $\underline{e}B^{-1}$ as long as it is small enough. One then multiplies by U^{-1} to get the message $\underline{m}$.

Exercise 19.9.5. Write down algorithms for KeyGen, Encrypt and Decrypt.

Example 19.9.6. Let $L \subset \mathbb{R}^2$ be the lattice with basis matrix

$$B = \begin{pmatrix} 17 & 0 \\ 0 & 19 \end{pmatrix}.$$

Let

$$U = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \quad \text{giving} \quad B' = UB = \begin{pmatrix} 34 & 57 \\ 51 & 95 \end{pmatrix}.$$

Let the message be $\underline{m} = (2, -5)$ and take $\underline{e} = (1, -1)$ (this is GGH encryption with $\sigma = 1$). Then

$$\underline{c} = \underline{m}B' + \underline{e} = (-186, -362).$$

To decrypt one computes

$$\underline{c}B^{-1} \approx (-10.94, -19.05)$$

(note that $\underline{m}U = (-11, -19)$ and $\underline{e}B^{-1} \approx (0.06, -0.05)$). We round the above to $(-11, -19)$ and recover the message as $\underline{m} = (-11, -19)U^{-1} = (2, -5)$.

Exercise 19.9.7. Show that GGH decryption gives the correct result as long as the entries of $\underline{e}B^{-1}$ are real numbers of absolute value $< 1/2$. Let ρ be the maximum, in the ℓ_1-norm, of the columns of B^{-1}. Show that if $\sigma < 1/(2\rho)$ then decryption gives the correct result.

Exercise 19.9.8. For the public key in Example 19.9.6 decrypt the ciphertext $\underline{c} = (220, 400)$.

As mentioned, the ciphertext in GGH encryption is considerably larger than the message. A precise analysis of this depends on the sizes of entries in B' (which in turns depends on the specific choices for B and U). We do not give any estimates for the ciphertext expansion.

Micciancio [421] proposed a variant of the GGH cryptosystem. The first idea is, instead of choosing the public basis to be $B' = UB$ for a random matrix $U \in \mathrm{SL}_2(\mathbb{Z})$, one can choose B' to be the Hermite normal form (HNF) of B. There is no loss of security by doing this, since anyone can compute the HNF of UB, and get the same result. The second idea is to encode the message in the error vector rather than in the lattice point (this is the same idea as discussed in Exercise 19.9.2) and to reduce it to the orthogonalized parallelepiped (see Exercise 19.9.9). This results in significantly shorter ciphertexts than the original GGH system and makes the encryption process deterministic. We refer to [421] for further details.

Exercise 19.9.9. Let $\underline{b}_1, \ldots, \underline{b}_n$ be an ordered basis for a lattice L and let $\underline{b}_1^*, \ldots, \underline{b}_n^*$ be the corresponding Gram-Schmidt vectors. Define the **orthogonalized parallelepiped**

$$\mathcal{P} = \left\{ \sum_{i=1}^{n} x_i \underline{b}_i^* : 0 \leq x_i \leq 1 \right\}.$$

Given $\underline{v} \in \mathbb{R}^n$ show how to compute $\underline{w} \in \mathcal{P}$ such that $\underline{v} - \underline{w} \in L$. This is called reducing to the orthogonalized parallelepiped.

19.10 Cryptanalysis of GGH Encryption

We now discuss the one-way encryption (OWE) security of the GGH cryptosystem under passive attacks. There are three natural ways to attack the GGH cryptosystem:

1. Try to obtain the private key B from the public key B'.
2. Try to obtain information about the message from the ciphertext, given that the error vector is small.
3. Try to solve the CVP of $\underline{c}$ with respect to the lattice L defined by B'.

We also present a fourth attack, due to Nguyen, which exploits the particular format of the error vectors in the GGH cryptosystem. Lattice basis reduction algorithms have a role to play in the first and third of these attacks.

Computing a Private Key

For the first attack, we simply run a lattice basis reduction algorithm (such as LLL) on the public basis matrix B'. If we are lucky then it will output a basis B'' that is good enough to allow the efficient solution of the required closest vector instances.

Example 19.10.1. Let

$$B = \begin{pmatrix} 7 & 0 & 0 \\ 0 & 23 & 0 \\ 0 & 0 & 99 \end{pmatrix}$$

and define $B' = UB$ where

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ -11 & 5 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 3 & -10 \\ 0 & 1 & -6 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then B' is the public basis matrix

$$B' = \begin{pmatrix} 7 & 69 & -990 \\ 56 & 575 & -8514 \\ -77 & -644 & 8019 \end{pmatrix}.$$

Let $\underline{m} = (2, -1, 3)$ be a message and $\underline{e} = (-1, 1, 1)$ an error vector and define $\underline{c} = \underline{m}B' + \underline{e} = (-274, -2368, 30592)$. Running LLL on B' does yield (up to sign) the matrix B (and hence $U = B'B^{-1}$). From this one can recover $\underline{m}$.

To prevent such an attack it is necessary that the dimension of the lattice be sufficiently large.

Computing Information about the Message

For the second attack we exploit the fact that $\underline{c} = \underline{m}B' + \underline{e}$ where $\underline{e}$ is a vector with small entries. A naive attack is to try all values of the error vector $\underline{e}$ until $\underline{c} - \underline{e}$ lies in the image of $\mathbb{Z}^n B'$. A more subtle idea is to compute $\underline{c}(B')^{-1} = \underline{m} + \underline{e}(B')^{-1}$ and try to deduce possible values for some entries of $\underline{e}(B')^{-1}$. For example, if the j-th column of $(B')^{-1}$ has particularly small norm then one can deduce that the j-th entry of $\underline{e}(B')^{-1}$ is always small and hence get an accurate estimate for the j-th entry of $\underline{m}$. We refer to Section 4.2 of [256] for further discussion. To defeat this attack one should not naively encode the message as a vector $\underline{m} \in \mathbb{Z}^n$. Instead, one should only use some low-order bits of some entries of $\underline{m}$ to carry information, or use an appropriate randomised padding scheme.

Solving the CVP Directly

For the third attack one can consider any of the algorithms listed in Chapter 18 for solving the CVP. For example, one can use the Babai nearest plane algorithm or the embedding technique.

Example 19.10.2. We use the public key and ciphertext from Example 19.10.1 and recover the message using the embedding technique. Construct

$$A = \begin{pmatrix} 7 & 69 & -990 & 0 \\ 56 & 575 & -8514 & 0 \\ -77 & -644 & 8019 & 0 \\ -274 & -2368 & 30592 & 1 \end{pmatrix}.$$

Running LLL on A yields the matrix

$$\begin{pmatrix} -1 & 1 & 1 & 1 \\ 5 & 2 & 2 & 2 \\ -1 & -15 & 8 & 8 \\ -1 & -2 & 51 & -48 \end{pmatrix}.$$

As desired, the first row is $(-1, 1, 1, 1) = (\underline{e}, 1)$. From this one can compute the message as $\underline{m} = (\underline{c} - \underline{e})(B')^{-1}$.

Exercise 19.10.3. For the public key from Example 19.10.1 use the embedding technique to decrypt the ciphertexts $\underline{c} = (120, 1220, -18017)$ and $\underline{c} = (-83, -714, 9010)$.

To defeat such attacks it is necessary that the lattice dimension is sufficiently large and that the solution to the CVP instance is not too special. In particular, the error vector should not be too short compared with the vectors the lattice.

Nguyen's Attack

Nguyen noted that the choice of the error vector in the original GGH cryptosystem made it extremely vulnerable to attack. Write $\underline{\sigma} = (\sigma, \sigma, \ldots, \sigma) \in \mathbb{Z}^n$. The crucial observation is that if $\underline{c}$ is a GGH ciphertext then $\underline{c} + \underline{\sigma} \equiv \underline{m}B' \pmod{2\sigma}$. If B' is invertible modulo 2σ (or even modulo a factor of 2σ) then one can already extract significant information about the message $\underline{m}$. Furthermore, if one successfully computes $\underline{m}_0 \equiv \underline{m} \pmod{2\sigma}$, then one obtains the simpler closest vector instance

$$\frac{\underline{c} - \underline{m}_0 B'}{2\sigma} = \underline{m}' B' + \frac{\underline{e}}{2\sigma}$$

where $\underline{m} = \underline{m}_0 + 2\sigma\underline{m}'$. Since $\underline{e}/(2\sigma)$ is a much shorter vector than $\underline{e}$ it is possible that algorithms for the closest vector problem that were not successful on the original instance can succeed on the new instance.

Example 19.10.4. Consider the lattice L and ciphertext c from Example 19.9.6. Since $\sigma = 1$ we can add $(1,1)$ to c and solve

$$c + (1,1) = (-185, -361) \equiv \underline{m}_0 B' \pmod 2$$

(note that B' is invertible over $\mathbb{F}_2$). One finds $\underline{m}_0 = (0,1) \equiv (2,-5) \pmod 2$ as expected.

Exercise 19.10.5. Perform Nguyen's attack for the ciphertexts of Exercise 19.10.3.

The natural approach to resist Nguyen's attack is to choose error vectors with a more general range of entries (e.g., $e_j \in \{-\sigma, -(\sigma-1), \ldots, -1, 0, 1, \ldots, \sigma\}$ for $1 \leq j \leq n$). It is then necessary to re-evaluate all the other attacks and parameter choices.

Finally, we remark that none of the above techniques gives an attack with polynomial asymptotic complexity as the dimension n grows. Hence, the GGH encryption scheme and its variants are not broken. On the other hand, in practice one needs to use lattices of rather large dimension and this limits the practicality of the GGH system.

19.11 GGH Signatures

Let B' be a GGH public key corresponding to a lattice L in $\mathbb{Z}^n$. The natural signature scheme is as follows: Given a message m hash it to a "random" element $H(m) \in \mathbb{Z}^n$. Then, using the private key, compute a lattice vector $\underline{s}$ close to $H(m)$. The signature on message m is then $\underline{s}$. To verify the signature one checks that $\underline{s}$ lies in the lattice (i.e., $\underline{s}(B')^{-1} \in \mathbb{Z}^n$) and that $\|\underline{s} - H(m)\|$ is smaller than some threshold that is specified as part of the signature verification key.

We remark that signatures for lattice schemes are somewhat easier than for the McEliece cryptosystem since CVP algorithms work for any point in $\mathbb{R}^n$ whereas decoding algorithms may fail for words that are not within the minimum distance of a code-word (however, see Courtois, Finiasz and Sendrier [451] for a study of McEliece signatures).

To analyse the security (namely, resistance to forgery) of such a signature scheme one must consider all the attacks mentioned above on the encryption scheme. One therefore is required to use lattices of large dimension $n \geq 200$.

Furthermore, as usual with signatures, one must also consider the fact that an adversary could obtain signatures on messages and that this might leak information about the private key. For the GGH signature scheme one sees that $\underline{s} - H(m)$ is a short vector in $\mathbb{R}^n$. Indeed, if the CVP algorithm used by the signer is perfect for the basis B then $\underline{s} - H(m)$ always lies in the parallelepiped

$$\mathcal{P}_{1/2}(B) = \{\underline{x}B : \underline{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n, -1/2 \leq x_i \leq 1/2 \text{ for all } 1 \leq i \leq n\},$$

which is called a **fundamental domain** for the lattice (i.e., for every point $\underline{x} \in \mathbb{R}^n$ there is some $\underline{y}$ in the lattice such that $\underline{x} - \underline{y} \in \mathcal{P}_{1/2}(B)$). The fundamental domain of a lattice is a simplex whose sides are determined by the basis vectors in B. Hence, it is natural to wonder whether seeing a number of random entries in $\mathcal{P}_{1/2}(B)$ allows one to learn something about the vectors in B. Nguyen and Regev [457, 458] have explored this idea and shown that such an approach can be used to cryptanalyse signatures. Adding a "perturbation" to the signature seems to prevent the attack of Nguyen and Regev (see Section 1.3 of [458]). Gentry, Peikert and Vaikuntanathan [253] give a method to sample

from a lattice (when given a sufficiently good basis) such that the output is statistically close to a Gaussian distribution. Hence, their paper gives[3] a secure implementation of the GGH signature concept.

19.12 NTRU

The NTRU[4] cryptosystem was invented by Hoffstein, Pipher and Silverman. The original proposal is phrased in terms of polynomial rings. We refer to Hoffstein, Pipher and Silverman [288], Section 6.10 of [289] or Section 17.4 of [609] for a description of the system in these terms.

The NTRU encryption scheme can also be described as a special case of Micciancio's variant of the GGH encryption scheme. The public key is a $2n \times 2n$ matrix

$$B = \begin{pmatrix} qI_n & 0 \\ H & I_n \end{pmatrix}$$

in Hermite normal form, where I_n is the $n \times n$ identity matrix, q is an integer (typically $q = 2^8$ or 2^{10}) and H is an $n \times n$ matrix with entries in $\{0, 1, \ldots, q-1\}$. The crucial property of NTRU is that the matrix H is a **circulant matrix**, in other words, the rows of H are just cyclic rotations of the first row of H. This means that to specify the NTRU public key one only needs to specify q and the first row of H; the public key requires $O(n \log_2(q))$ bits.

The matrix H is constructed by the user in a special way so that they know a basis for the lattice generated by B consisting of short vectors. Encryption proceeds as in the Micciancio scheme. We refer to Section 5.2 of Micciancio and Regev [423] for further details.

The details of the NTRU scheme have evolved over time. In particular, earlier parameter choices for NTRU had a noticeable probability of decryption failures, and this property was used to develop active (i.e., not passive) attacks [298]. Hence, the currently recommended parameters for NTRU have negligible probability of decryption failures.

The security of the NTRU cryptosystem relies on the difficulty of computing short vectors in the NTRU lattice. One remark is that the NTRU lattice has a number of special properties that can be used to improve the standard algorithms for finding short vectors. In particular, if $\underline{v}$ is a short vector in the NTRU lattice then so are the n "cyclic rotations" of $\underline{v}$. As a sample of the literature on special properties of the NTRU lattice we refer to May and Silverman [412], Gama, Howgrave-Graham and Nguyen [234] and Gentry [251].

19.13 Knapsack Cryptosystems

Knapsack cryptosystems were proposed by Merkle and Hellman in 1978. As with NTRU, the original description of knapsack cryptosystems made no reference to lattices. However there is a general attack on knapsacks using lattices (indeed, this was the first application of lattice basis reduction to public key cryptanalysis) and so it is natural to consider them as a lattice-based cryptosystem. Though not used in practice, we briefly present knapsack cryptosystems as they are an excellent source of exercises in cryptanalysis.

[3] This is only one of the many contributions of [253].

[4] The meaning of the acronym NTRU is not explained in the original paper. One interpretation is that it stands for "Number Theorists are Us". After various successful attacks were discovered on the corresponding signature scheme some individuals in the cryptography community started to refer to it as "Not True".

Definition 19.13.1. Let $b_1, \ldots, b_n$ be distinct positive (i.e., $b_i \geq 1$) integers (sometimes called **weights**). The **subset sum problem** is, given an integer s obtained as a sum of elements b_i, to find $x_i \in \{0, 1\}$ for $i = 1, \ldots, n$ such that

$$s = \sum_{i=1}^{n} x_i b_i.$$

The name **knapsack** is a mis-use of subset sum. It comes from the idea of finding out what is in a knapsack (a type of bag) just from its weight. The subset sum problem is $\mathcal{NP}$-complete.

Exercise 19.13.2. A decisional variant of Definition 19.13.1 is, given $\{b_1, \ldots, b_n\}$ and $s \in \mathbb{N}$ to decide whether or not there are $x_i \in \{0, 1\}$ such that $s = \sum_{i=1}^{n} x_i b_i$. Prove that these two computational problems are equivalent.

Exercise 19.13.3. Let notation be as in Definition 19.13.1 and let $B = \sum_{i=1}^{n} b_i$. Give a time-memory tradeoff algorithm to find the solution $x_i \in \{0, 1\}$, or show none exists, in $O(n2^{n/2} \log(B)^2)$ bit operations and with $O(n2^{n/2} \log(B))$ bits of storage.

The attack of Exercise 19.13.3 has been greatly improved by Shamir and Schroeppel (we do not have space for the details; see Section 8.1.2 of Joux [317]). A further improvement has been given by Howgrave-Graham and Joux [300]. Wagner's algorithm (see Section 13.8) does not seem to be directly applicable to the subset sum problem, though has been used to solve the modular subset sum problem (i.e., given $\{b_i\}$, s and m to find $x_i \in \{0, 1\}$ such that $\sum_{i=1}^{n} x_i b_i \equiv s \pmod{m}$) by Wagner (also see the work of Lyubashevsky and Shallue).

Exercise 19.13.4. Show that every subset sum instance can be reduced to an instance where the weights satisfy $\gcd(b_1, \ldots, b_n) = 1$.

The motivating idea of a knapsack cryptosystem is that computing $s = \sum_{i=1}^{n} x_i b_i$ is a one-way function. The remaining problem is to design subset sum instances that can be efficiently solved using a private key. To do this one first considers easy instances of the subset sum problem.

Definition 19.13.5. A sequence $b_1, \ldots, b_n$ in $\mathbb{N}$ is **superincreasing** if, for each $2 \leq i \leq n$

$$b_i > \sum_{j=1}^{i-1} b_j.$$

There is an efficient greedy algorithm to solve the subset sum problem if the b_i are a superincreasing sequence: Just subtract the largest possible value from s and repeat.

Example 19.13.6. The sequence

$$1, 2, 4, 8, \ldots, 2^{n-1}$$

is a superincreasing sequence. Decomposing an integer s with respect to this sequence is the same as writing it in binary.

Exercise 19.13.7. Consider the superincreasing sequence

$$1,\ 5,\ 7,\ 20,\ 35,\ 80,\ 170.$$

Decompose $s = 112$ with respect to this sequence.

Exercise 19.13.8. Show that if $b_1, \ldots, b_n$ is a superincreasing sequence then $b_i \geq 2^{i-1}$ and $b_{i+j} > 2^{j-1} b_i$ for $1 \leq i \leq n$ and $1 \leq j$.

The following definition gives a rough estimate for the "information rate" of a knapsack cryptosystem (in other words, the ratio of the number of bits to represent the solution of a subset sum instance versus the number of bits in sum itself). This quantity arises in the cryptanalysis of knapsack cryptosystems.

Definition 19.13.9. The **density** of a sequence $b_1, \ldots, b_n$ is

$$d = n / \log_2 \max\{b_i\}.$$

Exercise 19.13.10. What is the density of $1, 2, 4, 8, \ldots, 2^{n-1}$?

Exercise 19.13.11. What is the density of $3, 7, 11, 27, 50, 107, 210, 430$?

Exercise 19.13.12. Show that the density of a superincreasing sequence is at most $1 + 1/(n-1)$.

19.13.1 Public Key Encryption Using Knapsacks

The idea of the Merkle-Hellman knapsack cryptosystem is to have a superincreasing sequence as the private key but to 'disguise' this for the public key. We briefly sketch the algorithms for the "textbook" Merkle-Hellman knapsack cryptosystem (for more details see Section 8.6 of [418]). The length n of the sequence is a security parameter.

- KeyGen(n): Generate a superincreasing sequence $b_1, \ldots, b_n$ in $\mathbb{N}$. Choose a modulus $M > \sum_{i=1}^{n} b_i$ and a random integer W coprime to M. Select a random permutation π of the integers $\{1, \ldots, n\}$. Define $a_i = W b_{\pi(i)} \pmod{M}$. The public key is $\underline{a} = (a_1, \ldots, a_n)$ and the private key is $\pi, W, M, \underline{b} = (b_1, \ldots, b_n)$.
- The message space is $M_n = \{0,1\}^n$ (i.e., binary strings of length n).
- To Encrypt a message $\underline{m} = (m_1, \ldots, m_n)$ where $m_i \in \{0,1\}$ a user computes the integer
$$c = \underline{m} \cdot \underline{a} = \sum_{i=1}^{n} m_i a_i$$
and transmits this.
- To Decrypt, the user with the private key multiplies c by $W^{-1} \pmod{M}$ to obtain $0 \leq s < M$. The user can solve the subset sum problem for s with respect to the superincreasing sequence. (If there is no solution then the decryption algorithm outputs the invalid ciphertext symbol $\perp$.) The message is then obtained by permuting the sequence x_i using π^{-1}.

Exercise 19.13.13. Show that decryption does recover the message.

Example 19.13.14. Consider the superincreasing sequence from Exercise 19.13.7

$$1,\ 5,\ 7,\ 20,\ 35,\ 80,\ 170.$$

We disguise using modulus 503 and multiplier 430 (and taking π to be the identity permutation for simplicity) to get the public key

$$430,\ 138,\ 495,\ 49,\ 463,\ 196,\ 165.$$

Let the message be the binary sequence 1001100. The ciphertext is

$$c = 430 + 49 + 463 = 942.$$

To decrypt we compute $430^{-1}c \equiv 56 \pmod{503}$, which is then easily decomposed as $35 + 20 + 1$ giving the message 1001100.

Exercise 19.13.15. Consider the Merkle-Hellman public and private key from Example 19.13.14. Decrypt the ciphertext 829.

Exercise 19.13.16. What is the density of the public key in Example 19.13.14.

Exercise 19.13.17. Consider the Merkle-Hellman private key $M = 201$, $W = 77$ and $\underline{b} = (2, 5, 11, 27, 46, 100)$. What is the public key? What is the encryption of 101011?

Exercise 19.13.18. Show that the "textbook" Merkle-Hellman knapsack does not have IND-CPA security.

Exercise 19.13.19. Show that the "textbook" Merkle-Hellman knapsack does not have OWE-CCA security.

Example 19.13.20. One can compute a single bit of information about the message from the ciphertext in the the "textbook" Merkle-Hellman system. Suppose that not all $a_1, \ldots, a_n$ in the public key are even (if so, divide all a_i and the challenge ciphertext c by 2 and try again). Then $c \equiv \sum_{i=1}^{n} x_i a_i \pmod 2$ and so one obtains

$$\sum_{i=1, a_i \text{ odd}}^{n} x_i \pmod 2.$$

In general one prefers the cipertext to have a similar size to n. Exercise 19.13.21 shows that it is impossible to have a ciphertext of exactly the same bit-length as the message when using knapsacks.

Exercise 19.13.21. Show that a ciphertext in the "textbook" Merkle-Hellman scheme is expected to require at least $n + \log_2(n) - 2$ bits.

Exercise 19.13.22. It is sometimes stated in the literature that a Merkle-Hellman public key must have density less than 1. Show that this is not the case.

To avoid attacks (to be described in the next section) it was proposed to iterate the Merkle-Hellman procedure t times. In other words, first choose a superincreasing sequence $b_1, \ldots, b_n$, choose (M_1, W_1) such that $M_1 > \sum_{i=1}^{n} b_n$ and compute $a_{1,i} = Wb_i \pmod{M_1}$ for $1 \leq i \leq n$. Then choose (M_2, W_2) such that $M_2 > \sum_{i=1}^{n} a_{1,i}$ and compute $a_{2,i} = Wa_{1,i} \pmod{M_2}$ for $1 \leq i \leq n$ and so on. The public key is $a_{t,1}, \ldots, a_{t,n}$. One can then apply a permutation to the public key if necessary. The original Merkle-Hellman cryptosystem is the case $t = 1$, which is sometimes given the anachronistic name "single-iterated Merkle-Hellman".

Exercise 19.13.23. Give the decryption algorithm for the iterated Merkle-Hellman system.

Exercise 19.13.24. Show that in iterated Merkle-Hellman one expects $M_{i+1} > (n/2)M_i$ for $1 \leq i < n$. Hence, show that the ciphertext in an iterated Merkle-Hellman system is at least $t(\log_2(n) - 1) + n + \log_2(n) - 2$ bits. Determine the expected density of the public key.

It follows that one cannot iterate the Merkle-Hellman construction too many times.

In the next section we will sometimes assume that $b_1 b_2 < M$. Exercise 19.13.25 shows that if this is not the case then ciphertexts are roughly double the length of the message, and hence are less desirable for practical applications.

Exercise 19.13.25. Let $b_1, \ldots, b_n$ be a superincreasing sequence and suppose $M > \sum_{i=1}^{n} b_i$ is such that $b_1 b_2 > M$. Show that the average ciphertext size is at least $2n + \log_2(n) - 6$ bits.

19.13.2 Cryptanalysis of Knapsack Cryptosystems

We now give a number of attacks on the knapsack cryptosystem, some of which are easy exercises. For a thorough discussion of the history of these attacks see Brickell and Odlyzko [104] and Odlyzko [470].

We remark that there is not necessarily a unique private key for a given Merkle-Hellman knapsack public key since $\{W^{-1} a_i \pmod{M} : 1 \leq i \leq n\}$ might be a superincreasing sequence for more than one choice of (M, W).

Exercise 19.13.26. Show that, given a Merkle-Hellman knapsack public key $(a_1, \ldots, a_n)$, one can efficiently determine whether a guess for (M, W) provides a useful private key.

We now show that the scheme is insecure if the first elements of the superincreasing sequence are known.

Example 19.13.27. Let $a_1, \ldots, a_n$ be a Merkle-Hellman knapsack public key. Suppose one knows the first two elements b_1 and b_2 of the superincreasing sequence. We show how to recover the private key.

First, suppose no permutation is used. Then $a_1 \equiv W b_1 \pmod{M}$ and $a_2 \equiv W b_2 \pmod{M}$. It follows that $a_1 b_2 \equiv a_2 b_1 \pmod{M}$ and so M is a factor of $(a_1 b_2 - a_2 b_1)$. Since b_1 and b_2 are small, $a_i \approx 2^n$ (perhaps $n = 256$) and $(a_1 b_2 - a_2 b_1)$ is not expected to have any special form, it is natural to assume that this factoring problem is fairly easy. Furthermore, since $\max\{a_i : 1 \leq i \leq n\} < M$ and we expect $M < 2 \max\{a_i : 1 \leq i \leq n\}$ (i.e., not all $a_i < M/2$) there are few possible values for M.

For each possible value of M one can compute $W = a_1 b_1^{-1} \pmod{M}$ and then test whether the values $W^{-1} a_i \pmod{M}$ look like a superincreasing sequence.

To deal with the permutation just repeat the attack for all triples (a_i, a_j) with $1 \leq i, j \leq n$ distinct. If (i, j) does not correspond to the correct permutation of $(1, 2)$ then probably either $(a_i b_2 - a_j b_1)$ does not have a factor of the right size, or the corresponding W do not yield superincreasing sequences.

Exercise 19.13.28. Perform the attack of Example 19.13.27 for the Merkle-Hellman public key

$$8391588,\ 471287,\ 8625204,\ 906027,\ 8328886$$

given that $b_1 = 44899$ and $b_2 = 1048697$ (with no permutation used).

In practice, due to Example 19.13.27, one would take b_1 and b_2 to have around $2^{\kappa/2}$ bits each for security parameter κ.

We now show why M must be kept secret.

Example 19.13.29. Suppose M is known to the attacker, who wants to compute W and hence the superincreasing sequence $b_1, \ldots, b_n$.

First, assume no permutation is used. Since

$$a_i \equiv b_i W \pmod{M}$$

for $1 \leq i \leq n$ one has $b_2 \equiv b_1(a_2 a_1^{-1}) \pmod{M}$. Let $0 \leq c < M$ be such that $c \equiv a_2 a_1^{-1} \pmod{M}$. Then

$$b_2 = b_1 c + zM$$

where $z < b_1$. Running the extended Euclidean algorithm on (c, M) computes all triples (b_1, z, b_2) such that $b_1 b_2 < M$ in polynomial-time (following Exercise 19.13.25 we assume that the desired solution satisfies this condition). For each candiate pair (b_1, b_2) one checks whether $a_1 b_1^{-1} \equiv a_2 b_2^{-1} \pmod{M}$ and, if so, calls this value W and tests whether $W^{-1} b_i \pmod{N}$ is "small" (at most $M/2$, and usually much smaller) for a few randomly chosen indices i. One expects to easily find the right pair (b_1, b_2) and hence the correct value for W.

When the permutation is used one repeats the above attack for all pairs (a_i, a_j) for distinct $1 \leq i, j \leq n$.

Exercise 19.13.30. Show that W must be kept secret.

Shamir's Attack

We now present an attack using lattices to compute both M and W together (actually, to compute M and $U = W^{-1} \pmod{M}$ where $1 \leq U < M$). This approach originates with Shamir [546] although we follow the presentation of Lagarias [360]. For clarity, we first assume that no permutation is used. The starting point is to note that for $1 \leq i \leq n$ there are integers k_i such that

$$a_i U - k_i M = b_i$$

and $0 \leq k_i < a_i$. Hence,

$$0 \leq \frac{U}{M} - \frac{k_i}{a_i} = \frac{b_i}{a_i M}. \tag{19.7}$$

Since the b_i are superincreasing we have $b_i < M/2^{n-i}$ and so $0 \leq U/M - k_i/a_i < 1/(a_i 2^{n-i})$. In particular, $U/M - k_1/a_1 < 1/(a_1 2^{n-1})$ is very small.

We now observe that to break the Merkle-Hellman knapsack it is sufficient to find any pair (u, m) of positive integers such that $ua_i \pmod{m}$ is a superincreasing sequence (or at least is similar enough to such a sequence that one can solve the subset sum problem). We show in the next paragraph that if k_1/a_1 is close enough to U/M then taking $(u, m) = (k_1, a_1)$ will suffice.

Subtracting the case $i = 1$ of equation (19.7) from the i-th gives

$$\frac{k_1}{a_1} - \frac{k_i}{a_i} = \frac{b_i}{a_i M} - \frac{b_1}{a_1 M} = \frac{a_1 b_i - a_i b_1}{a_1 a_i M}$$

and so, for $2 \leq i \leq n$,

$$|a_i k_1 - a_1 k_i| = |a_1 b_i - a_i b_1|/M < 2Mb_i/M = 2b_i < M/2^{n-i-1}. \tag{19.8}$$

Taking $m = a_1$ and $u = k_1$ we have $ua_i \pmod{m}$ being very close to a superincreasing sequence (in the sense that the numbers grow in a very controlled way).

It remains to compute the integer k_1 such that equation (19.8) holds, given only the integers $a_1, \ldots, a_n$. Another way to write equation (19.8) is $|a_i/a_1 - k_i/k_1| < M/(a_1 k_1 2^{n-i-1})$ and one sees that the problem is precisely simultaneous Diophantine approximation as considered in Section 19.5. We apply the method of Section 19.5.

Hence, consider the following basis matrix (where $0 < \lambda < 1$ is a parameter analogous to ϵ/Q in equation (19.5) and where $1 < l \leq n$)

$$\begin{pmatrix} \lambda & a_2 & a_3 & \cdots & a_l \\ 0 & -a_1 & 0 & \cdots & 0 \\ 0 & 0 & -a_1 & & \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & & \cdots & -a_1 \end{pmatrix}. \tag{19.9}$$

This lattice contains the vector $(\lambda k_1, k_1 a_2 - k_2 a_1, k_1 a_3 - k_3 a_1, \ldots, k_1 a_d - k_d a_1)$. Perfoming lattice basis reduction one obtains a guess for k_1. One now sets $u = k_1$ and $m = a_1$ and computes $ua_i \pmod m$ for $2 \leq i \leq n$. Hopefully this is a superincreasing sequence (or, is at least close enough to one to allow efficient decryption). One then computes $uc \pmod n$ where c is any challenge ciphertext, decrypts using the superincreasing sequence, and therefore recovers the message. One might expect to have to take $l = n$, but the attack actually works for rather small values of l (see below for more discussion).

Example 19.13.31. Consider the superincreasing sequence

$$b_1 = 7, b_2 = 20, b_3 = 35, b_4 = 71, b_5 = 140, b_6 = 307, b_7 = 651, b_8 = 1301.$$

Choose $M = 2609$ and $W = 2525$ (giving $U = 528$). The Merkle-Hellman public key is

$$(2021, 929, 2278, 1863, 1285, 302, 105, 294).$$

The encryption of 10101011 is 5983.

The sequence of values k_i such that $a_i U - k_i M = b_i$ are

$$409, 188, 461, 377, 260, 61, 21, 59$$

and the values of $a_i k_1 - a_1 k_i$ for $i = 2, 3, 4$ are 13, 21 and 50.

Take $\lambda = 1/32$ and $l = 4$ and consider the lattice basis as in equation (19.9). LLL reduction gives

$$\begin{pmatrix} 409/32 & 13 & 21 & 50 \\ 2021/32 & 0 & 0 & 0 \\ -755/32 & -108 & -19 & 51 \\ 205/8 & -137 & 556 & -216 \end{pmatrix}.$$

One recovers $k_1 = 409$ (and the first few values $a_i k_1 - a_1 k_i$). One can even get the result using $\lambda = 1/8$ and $l = 3$. The LLL-reduced basis is

$$\begin{pmatrix} -409/8 & -13 & -21 \\ 63/8 & -82 & 23 \\ 385/8 & -52 & -84 \end{pmatrix}.$$

To complete the cryptanalysis take $u = k_1 = 409$ and $m = a_1 = 2021$. The sequence $a_i u \pmod m$ for $1 \leq i \leq 8$ is $(0, 13, 21, 50, 105, 237, 504, 1007)$, which is a superincreasing sequence. One then computes $5983u \equiv 1637 \pmod m$, which decomposes with respect to the superincreasing sequence as $1637 = 1007 + 504 + 105 + 21$. The corresponding message is $x_1 0101011$ where $x_1 \in \{0, 1\}$. Using the original public key one can determine that $x_1 = 1$ and confirm that the message does encrypt to the given ciphertext.

Exercise 19.13.32. Using the same public key as Example 19.13.31 decrypt the ciphertext 5522 using the key (u, m) determined by the cryptanalysis.

Exercise 19.13.33. Consider the Merkle-Hellman public key 1994, 1966, 1889, 822, 640, 1224, 1402, 1492 and ciphertext 6569. Deduce the message using Shamir's attack.

A formal analysis of this method is given by Lagarias [360]. As with other attacks on knapsack cryptosystems, the results are heuristic in the sense that they are proved by considering a "random" knapsack instance. The first issue is the size of l. Shamir [546] and Lagarias [360] both suggest that one can take $l > 1/d + 1$, where d is the density of the instance. In practice, $l = 4$ seems to be acceptable. This means the computation is only for lattices of very small dimensions and is certainly polynomial-time. So far we have ignored the permutation; in practice the attack is repeated for the $n(n-1)\cdots(n-(l-1))$ choices of l values from $(a_1, \ldots, a_n)$. Since l is constant this still gives a polynomial-time attack. For these reasons the Merkle-Hellman knapsack cryptosystem is considered to be totally broken.

The iterated Merkle-Hellman system is designed to avoid the above attacks, though Lagarias [360] showed how to attack the double iterated knapsack (i.e., the case $t = 2$) and discussed how to generalise the attack to larger t using exactly the same methods. Brickell [103] also discusses a heuristic method to attack the general iterated Merkle-Hellman system.

Direct Lattice Attack on Subset Sum

We now discuss a more direct way to use lattices to solve the subset sum problem and hence break knapsack cryptosystems. This idea originates in the work of Lagarias and Odlyzko [362]. These methods do not rely on any properties of the subset sum instance and so can be applied to iterated Merkle-Hellman. However, they only work when the density is sufficiently small.

Let $(a_1, \ldots, a_n)$ be a sequence of weights and let $s = \sum_{i=1}^{n} x_i a_i$ be a subset sum instance. Note that $s' = \sum_{i=1}^{n} a_i - s$ is the subset sum instance of the complement $\bar{x_1} \cdots \bar{x_n}$ (where $\bar{0} = 1$ and $\bar{1} = 0$). Since one can repeat any attack on s and s' in turn we may always assume that at most half the entries of the solution are non-zero.

The basic method is to consider the lattice L with basis

$$\begin{pmatrix} I_n & \underline{a} \\ \underline{0} & -s \end{pmatrix} \tag{19.10}$$

where I_n is an $n \times n$ identity matrix and $\underline{a}$ is the list of weights represented as a column vector. Then

$$\underline{v} = (x_1, x_2, \ldots, x_n, 0)$$

is a vector in the lattice. Since $\|v\| \leq \sqrt{n}$ this vector is very short and so one could hope to find it using lattice basis reduction.

Example 19.13.34. Consider the subset sum instance from Example 19.13.14. Reducing the basis

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 430 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 138 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 495 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 49 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 463 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 196 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 165 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -942 \end{pmatrix}$$

using LLL gives

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & -1 & 1 & 1 \\ 1 & 0 & 1 & 0 & -2 & 0 & 0 & -1 \\ 0 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ -1 & 1 & 2 & 1 & 0 & 1 & 0 & 1 \\ 0 & -2 & 1 & 1 & -1 & 1 & 0 & 1 \\ -1 & 0 & 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 0 & 1 & 0 & 0 & 0 & -3 & 0 \end{pmatrix}.$$

One sees that the message $(1, 0, 0, 1, 1, 0, 0, 0)$ appears as the first row (smallest vector) in the lattice.

Exercise 19.13.35. Consider the knapsack public key

$$2381, 1094, 2188, 2442, 2280, 1129, 1803, 2259, 1665$$

and ciphertext 7598. Determine the message using the direct lattice method.

Lagarias and Odlyzko analysed the method for "random" subset sum instances of a given size. They showed (Theorem 3.3 of [362], also see Section 2 of [154]) that for randomly chosen weights a_i of size $2^{\beta n}$ with $\beta > 1.54725$ (i.e., random subset sum instances of density at most 0.6463) then with overwhelming probability (as n tends to infinity) the desired solution vector $\underline{x}$ is the shortest non-zero vector in the lattice. If one can solve the shortest vector problem then one therefore can break the cryptosystem.

There are therefore two problems to overcome. First, the statement only holds for randomly generated weights of a given size and so does not say anything concrete about specific instances. Second, there is no known efficient algorithm to solve SVP exactly. This latter point is a serious problem: as seen in Example 19.13.34 there are many very small vectors in the lattice that do not have entries only in $\{0, 1\}$ (these are often called **parasitic solutions** to the subset sum instance). Hence, for large n, it is quite possible that LLL outputs a short basis that does not include the desired solution vector. Nevertheless, the LLL algorithm does work well in practice and can be used to solve subset sum instances when the density is not too high.

Theorem 3.5 of Lagarias and Odlyzko [362] shows (for randomly chosen weights a_i of size $2^{(1/2+\beta)n^2}$ with $\beta > 0$) that with overwhelming probability (as n tends to infinity) the desired solution vector $\underline{x}$ is computed using the LLL algorithm. This is done by showing that the parasitic solutions all have significantly larger size. The problem with this result is that it only applies when the density satisfies $d \leq (1/2 + \beta)^{-1} 1/n$, which is extremely low.

Coster, Joux, LaMacchia, Odlyzko, Schnorr and Stern [154] improved the method by replacing the last row of the lattice in equation (19.10) by $(1/2, 1/2, \ldots, 1/2, s)$. Under the same simplifying assumptions as used by Lagarias and Odlyzko they showed the attack could be applied for instances with density $d < 0.9408$. Again, although their method officially requires an efficient algorithm for SVP, solving the approximate SVP using LLL works well in practice as long as n is not too large. An alternative formulation of this method is given in Section 3.2 of Nguyen and Stern [463].

The direct lattice attacks require lattices of dimension n so can be defeated by choosing n sufficiently large. Hence, the high-density subset sum problem remains hard in general. The problem with knapsack cryptosystems is that one needs to iterate the basic Merkle-Hellman construction sufficiently many times to avoid the attacks presented earlier. Iterating the Merkle-Hellman method lowers the lattice density and this can make

the system vulnerable to the direct lattice attack unless n is rather large. To conclude, it seems that iterated knapsack cryptosystems are completely broken.

Part V

Cryptography Related to Discrete Logarithms

Chapter 20

The Diffie-Hellman Problem and Cryptographic Applications

This chapter introduces some basic applications of the discrete logarithm problem in cryptography, such as Diffie-Hellman key exchange and "textbook" Elgamal encryption. A brief security analysis of these systems is given. This motivates the computational and decisional Diffie-Hellman problems (CDH and DDH). A thorough discussion of these computational problems will be given in Chapter 21.

20.1 The Discrete Logarithm Assumption

The discrete logarithm problem (DLP) was defined in Definition 13.0.1. Our main interest is the DLP in an algebraic group or algebraic group quotient over a finite field $\mathbb{F}_q$ (for example, elliptic curves, the multiplicative group of a finite fields, tori etc). We always use multiplicative notation for groups in this chapter. As discussed in Section 13.2, in practice we usually restrict to groups of prime order r.

Recall that the difficulty of the DLP is defined with respect to an instance generator that runs on input a security parameter κ. An algorithm to solve the DLP with respect to a given instance generator is only required to succeed with a noticeable probability. The **discrete logarithm assumption** is that there exist instance generators that, on input κ, output instances of the DLP such that no algorithm A running in polynomial-time in κ can solve the DLP apart from with negligible (in κ) probability. The cryptosystems in this chapter rely on the discrete logarithm assumption (and other assumptions).

20.2 Key Exchange

20.2.1 Diffie-Hellman Key Exchange

The starting point of discrete logarithms (indeed, of public key cryptography) is the seminal paper of Diffie and Hellman [179] from 1976 (more recently it became known that this idea was also found by Williamson at GCHQ in 1974).

Suppose Alice and Bob want to agree on a random key K. Assume they both know an algebraic group or algebraic group quotient G and some element $g \in G$ of prime order r (everyone in the world could use the same g). They perform the following protocol:

- Alice chooses a random integer $0 < a < r$ and sends $\mathsf{c}_1 = g^a$ to Bob.
- Bob chooses a random integer $0 < b < r$ and sends $\mathsf{c}_2 = g^b$ to Alice.
- On receiving c_2 Alice computes $K = \mathsf{c}_2^a$.
- On receiving c_1 Bob computes $K = \mathsf{c}_1^b$.

Hence, both players share the key $K = g^{ab}$. One can derive (see Definition 20.2.10 below) a bitstring from the group element K for use as the key of a symmetric encryption scheme. Hence, encryption of data or other functionalities can be implemented using traditional symmetric cryptography. The key K is called the **session key** and the values $\mathsf{c}_1, \mathsf{c}_2$ in the protocol are called **messages** or **ephemeral keys**.

We discuss the security of key exchange protocols (in particular, person-in-the-middle attacks and authenticated key exchange) in Section 20.5. For the remainder of this section we consider the simplest possible attacker. A **passive attacker** or **eavesdropper** (i.e., an attacker who learns g, c_1 and c_2, but does not actively interfere with the protocol) cannot determine K unless they can solve the following computational problem.

Definition 20.2.1. The **Computational Diffie-Hellman problem (CDH)**[1] is: given the triple (g, g^a, g^b) of elements of G to compute g^{ab}.

An extensive discussion of the computational Diffie-Hellman problem will be given in Chapter 21.

Exercise 20.2.2. What is the solution to the CDH instance $(2, 4, 7)$ in the group $\mathbb{F}_{11}^*$?

Suppose one is an eavesdropper on a Diffie-Hellman session and tries to guess the session key K shared by Alice and Bob. The following computational problem is precisely the problem of determining whether the guess for K is correct. This problem arises again later in the chapter in the context of Elgamal encryption.

Definition 20.2.3. Let G be a group and $g \in G$. The **Decisional Diffie-Hellman problem (DDH)** is, given a quadruple (g, g^a, g^b, g^c) of elements in $\langle g \rangle$ to determine whether or not $g^c = g^{ab}$.

Saying that a computational problem such as DDH is hard is slightly less straightforward than with problems like DLP or CDH, since if (g, g^a, g^b, g^c) are chosen uniformly at random in G^4 then the solution to the DDH problem is "no" with overwhelming probability. Clearly, an algorithm that says "no" all the time is not solving the DDH problem,

[1] This assumption comes in two flavours, depending on whether g is fixed or variable. We discuss this issue in more detail later. But, as is the convention in this book, whenever we write "Given...compute..." one should understand that all of the inputs are considered as variables.

so our notion of success must capture this. The correct approach is to define a DDH solver to be an algorithm that can distinguish two distributions on G^4, namely the distribution of **Diffie-Hellman tuples** (i.e., the uniform distribution on tuples of the form $(g, g^a, g^b, g^{ab}) \in G^4$) and the uniform distribution on G^4.

Definition 20.2.4. Let (G_n, r_n) be a family of cyclic groups G_n of order r_n, for $n \in \mathbb{N}$. A **DDH algorithm** for the family G_n is an algorithm A that takes as input a quadruple in G_n^4 and outputs "yes" or "no". The **advantage** of the DDH algorithm A is

$$\begin{aligned}\mathrm{Adv}(A) &= \big|\Pr\left(A\left(g, g^a, g^b, g^{ab}\right) = \text{“}yes\text{”} : g \leftarrow G_n,\ a, b \leftarrow \mathbb{Z}/r\mathbb{Z}\right) \\ &\quad - \Pr\left(A\left(g, g^a, g^b, g^c\right) = \text{“}yes\text{”} : g \leftarrow G_n,\ a, b, c \leftarrow \mathbb{Z}/r\mathbb{Z}\right)\big|.\end{aligned}$$

A DDH algorithm is called **successful** if the advantage is noticeable. The **DDH assumption** for the family of groups is that all polynomial-time (i.e., running time $O(\log(r_n)^c)$ for some constant c) DDH algorithms have negligible advantage.

Lemma 20.2.5. *DDH* $\leq_R$ *CDH* $\leq_R$ *DLP.*

Exercise 20.2.6. Prove Lemma 20.2.5.

Exercise 20.2.7. Definition 20.2.3 states that r is prime. Show that if (g, g^a, g^b, g^c) is a quadruple of elements such that the order of g is n for some integer n where n has some small factors (e.g., factors $l \mid n$ such that $l \leq \log_2(n)$) then one can eliminate some quadruples $(g, g^a, g^b, g^c) \in G^4$ that are not valid DDH tuples by reducing to DDH instances in subgroups of prime order. Show that this is enough to obtain a successful DDH algorithm according to Definition 20.2.4.

20.2.2 Burmester-Desmedt Key Exchange

In the case of $n > 2$ participants there is a generalisation of Diffie-Hellman key exchange due to Burmester and Desmedt [114] that requires two rounds of broadcast. Let the participants in the protocol be numbered as player 0 to player $n-1$. In the first round, player i (for $0 \leq i < n$) chooses a random $1 \leq a_i < r$ and sends $\mathsf{c}_i = g^{a_i}$ to the other players (or, at least, to player $i-1 \pmod n$ and $i+1 \pmod n$). In the second round player i computes

$$\mathsf{t}_i = \left(\mathsf{c}_{i+1 \pmod n}\mathsf{c}_{i-1 \pmod n}^{-1}\right)^{a_i}$$

and sends it to all other players. Finally, player i computes

$$K = \mathsf{c}_{i+1 \pmod n}^{na_i}\mathsf{t}_{i+1 \pmod n}^{n-1}\mathsf{t}_{i+2 \pmod n}^{n-2}\cdots\mathsf{t}_{i+n-1 \pmod n}.$$

Lemma 20.2.8. *Each participant in the Burmester-Desmedt protocol computes*

$$K = g^{a_0a_1 + a_1a_2 + \cdots a_{n-2}a_{n-1} + a_{n-1}a_0}.$$

Exercise 20.2.9. Prove Lemma 20.2.8.

20.2.3 Key Derivation Functions

The result of Diffie-Hellman key exchange is a group element g^{ab}. Typically this should be transformed into an l-bit string for use as a symmetric key (where $l < \log_2(r)$).

Definition 20.2.10. Let G be an algebraic group (or algebraic group quotient) and let l be an integer. A **key derivation function** is a function $\mathsf{kdf} : G \to \{0,1\}^l$. The **output distribution** of a key derivation function is the probability distribution on $\{0,1\}^l$ induced by $\mathsf{kdf}(g)$ over uniformly distributed $g \in G$. A key derivation function is **preimage-resistant** if there is no polynomial-time algorithm known that, on input $x \in \{0,1\}^l$, computes $g \in G$ such that $\mathsf{kdf}(g) = x$.

In general, a key derivation function should have output distribution statistically very close to the uniform distribution on $\{0,1\}^l$. For many applications it is also necessary that kdf be preimage-resistant.

A typical instantiation for kdf is to take a binary representation of $K \in G$, apply a cryptographic hash function (see Chapter 3) to obtain a bit string, and concatenate/truncate as required. See the IEEE P1363 or ANSI X9.42 standards, Section 8 of Cramer and Shoup [161] or Section 6.1 of Raymond and Stiglic [495] for more details; also see Section 3 of [46] for a specific key derivation function for elliptic curves.

20.3 Textbook Elgamal Encryption

In this section we present **textbook Elgamal public key encryption**.[2] This is historically the first public key encryption scheme based on the discrete logarithm problem. As we will see, the scheme has a number of security weaknesses and so is not recommended for practical use. In Chapter 23 we will present secure methods for public key encryption based on computational problems in cyclic groups.

We actually present two "textbook" versions of Elgamal. The first we call "classic textbook Elgamal" as it is essentially the version that appears in [192]. It requires G to be a group (i.e., we cannot use algebraic group quotients) and requires the message m to be encoded as an element of G. Encoding messages as group elements is not difficult, but it is un-natural and inconvenient. The second version, which we call "semi-textbook Elgamal", is more practical as it treats messages as bitstrings. As we will see, the security properties of the two versions are slightly different.

For both schemes, κ denotes a security parameter (so that all attacks should require at least 2^κ bit operations). Figure 20.1 gives classic textbook Elgamal and Figure 20.2 gives semi-textbook Elgamal. We call the sender Bob and the recipient Alice. Messages in the former scheme are group elements and in the latter are l-bit strings, where l depends on the security parameter. Semi-textbook Elgamal also requires a cryptographic hash function $H : G \to \{0,1\}^l$ where G is the group.

Remarks

1. Both versions of textbook Elgamal encryption are best understood as a **static Diffie-Hellman key exchange** followed by symmetric encryption. By this we mean that the sender (Bob) is essentially doing a Diffie-Hellman key exchange with the recipient (Alice): he sends g^k and Alice's component is her fixed (i.e., static) public key g^a. Hence the shared key is g^{ak}, which can then be used as a key for any symmetric encryption scheme (this general approach is known as **hybrid encryption**). The two variants of textbook Elgamal vary in the choice of symmetric encryption scheme: the first uses the map $\mathsf{m} \mapsto \mathsf{m}g^{ak}$ from G to itself while the second uses the map $\mathsf{m} \mapsto \mathsf{m} \oplus H(g^{ak})$ from $\{0,1\}^l$ to itself.

[2] Some authors write "ElGamal" and others write "El Gamal". Reference [192] uses "ElGamal", but we follow the format apparently used nowadays by Elgamal himself.

KeyGen(κ): Run a parameter generation algorithm on security parameter κ that outputs an algebraic group G over a finite field $\mathbb{F}_q$ such that $\#G(\mathbb{F}_q)$ has a prime divisor r and all known algorithms for the discrete logarithm problem in a subgroup of $G(\mathbb{F}_q)$ of order r require at least 2^κ bit operations.

Compute $g \in G$ of prime order r.
Choose a random integer $0 < a < r$ and set $h = g^a$. The public key is (G, g, h) and the private key is a.

The message space is $\mathsf{M}_\kappa = G$.
The ciphertext space is $\mathsf{C}_\kappa = G \times G$.

Encrypt(m): (where $\mathsf{m} \in G$).

- Obtain the public key h of the recipient, Alice.
- Choose a random $0 < k < r$ and set $\mathsf{c}_1 = g^k$.
- Set $\mathsf{c}_2 = \mathsf{m}h^k$.
- Transmit the ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$.

Decrypt($\mathsf{c}_1, \mathsf{c}_2$): Check that $\mathsf{c}_1, \mathsf{c}_2 \in G$. If so, compute and output

$$\mathsf{m} = \mathsf{c}_2\mathsf{c}_1^{-a}.$$

Figure 20.1: Classic Textbook Elgamal Encryption.

2. Elgamal encryption requires two exponentiations in G and decryption requires one. Hence encryption and decryption are polynomial-time and efficient.

3. Elgamal encryption is randomised, so encrypting the same message with the same public key twice will yield two different ciphertexts in general.

4. Unlike RSA, all users in a system can share the same group G. So typically G and g are fixed for all users, and only the value $h = g^a$ changes. Values that are shared by all users are usually called **system parameters**.

20.4 Security of Textbook Elgamal Encryption

We now briefly review the security properties for the textbook Elgamal cryptosystem. First, note that the encryption algorithm should use a good pseudorandom number generator to compute the values for k. A simple attack when this is not the case is given in Exercise 20.4.1.

Exercise 20.4.1. Suppose the random values k used by a signer are generated using the linear congruential generator $k_{i+1} = Ak_i + B \pmod r$ for some $1 \leq A, B < r$. Suppose an adversary knows A and B and sees two classic textbook Elgamal ciphertexts $(\mathsf{c}_1, \mathsf{c}_2)$ and $(\mathsf{c}'_1, \mathsf{c}'_2)$, for the same public key, generated using consecutive outputs k_i and k_{i+1} of the generator. If both ciphertexts are encryptions of the same message then show how the adversary can compute the message. If both ciphertexts are encryptions of different messages then show how to decrypt both ciphertexts using one query to a decryption oracle.

KeyGen(κ): Generate an algebraic group or algebraic group quotient G as in Figure 20.1. Choose a random $g \in G$ of prime order r.
Choose a message size l and a cryptographic hash function $H : G \to \{0,1\}^l$.
Choose a random integer $0 < a < r$ and set $h = g^a$. The public key is (G, H, g, h) and the private key is a.

The message space is $\mathsf{M}_\kappa = \{0,1\}^l$.
The ciphertext space is $\mathsf{C}_\kappa = G \times \{0,1\}^l$.

Encrypt(m): (where $\mathsf{m} \in \{0,1\}^l$).

- Obtain the public key of the recipient, Alice.
- Choose a random $0 < k < r$ and set $\mathsf{c}_1 = g^k$.
- Set $\mathsf{c}_2 = \mathsf{m} \oplus H(h^k)$.
- Transmit the ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$.

Decrypt($\mathsf{c}_1, \mathsf{c}_2$): Check that $\mathsf{c}_1 \in G$ and $\mathsf{c}_2 \in \{0,1\}^l$. If so, compute and output

$$\mathsf{m} = \mathsf{c}_2 \oplus H(\mathsf{c}_1^a).$$

Figure 20.2: Semi-Textbook Elgamal Encryption.

20.4.1 OWE Against Passive Attacks

Theorem 20.4.2. *The computational problem of breaking OWE security of classic textbook Elgamal under passive attack is equivalent to CDH in $\langle g \rangle$.*

Proof: We prove the result only for perfect oracles. To prove OWE-CPA $\leq_R$ CDH, let A be a perfect oracle that solves CDH in the subgroup of order r in G. Call $A(g, h_A, \mathsf{c}_2)$ to get u and set $\mathsf{m} = \mathsf{c}_2 u^{-1}$.

To prove CDH $\leq_R$ OWE-CPA let A be a perfect adversary that takes an Elgamal public key (g, h_A) and an Elgamal ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$ and returns the corresponding message m. We will use this to solve CDH. Let the CDH instance be (g, g_1, g_2). Then choose a random element $\mathsf{c}_2 \in \langle g \rangle$ and call $A(g, g_1, g_2, \mathsf{c}_2)$ to get m. Return $\mathsf{c}_2 \mathsf{m}^{-1}$ as the solution to the CDH instance. □

One can also consider a non-perfect adversary (for example, maybe an adversary can only decrypt some proportion of the possible ciphertexts). It might be possible to develop methods to "self-correct" the adversary using random self-reductions, but this is considered to be the adversary's job. Instead, it is traditional to simply give a formula for the success probability of the algorithm that breaks the computational assumption in terms of the success probability of the adversary. In the context of Theorem 20.4.2, if the adversary can decrypt with noticeable probability ϵ then we obtain a CDH algorithm that is correct with probability ϵ.

Exercise 20.4.3. Prove OWE-CPA $\leq_R$ CDH for semi-textbook Elgamal. Explain why the proof CDH $\leq_R$ OWE-CPA cannot be applied in this case.

20.4.2 OWE Security Under CCA Attacks

We now show that both variants of textbook Elgamal do not have OWE security against an adaptive (CCA) attacker (and hence not IND-CCA security either). Recall that such

an attacker has access to a decryption oracle that will decrypt every ciphertext except the challenge.

Lemma 20.4.4. *Let* $(\mathsf{c}_1, \mathsf{c}_2)$ *be a ciphertext for classic textbook Elgamal with respect to the public key* (G, g, h)*. Suppose* A *is a decryption oracle. Then under a CCA attack one can compute the message corresponding to* $(\mathsf{c}_1, \mathsf{c}_2)$*.*

Proof: Assume that A is perfect. Call A on the ciphertext $(\mathsf{c}_1, \mathsf{c}_2 g) \neq (\mathsf{c}_1, \mathsf{c}_2)$ to obtain a message m'. Then the message corresponding to the original ciphertext is $\mathsf{m} = \mathsf{m}' g^{-1}$.

More generally if A succeeds only with noticeable probability ϵ then we have a CCA2 attack that succeeds with noticeable probability ϵ. □

Another version of this attack follows from Exercises 23.3.3 and 23.3.2.

Exercise 20.4.5. Show that semi-textbook Elgamal encryption does not have the OWE security property under a CCA attack.

We have seen how a CCA attack can lead to an adversary learning the contents of a message. Exercise 20.4.6 gives an example of a general class of attacks called **small subgroup attacks** or **invalid parameter attacks** that can allow a CCA (even a CCA1) adversary to obtain the private key of a user. Such attacks can be performed in many scenarios. One example is when working in a prime order subgroup of $\mathbb{F}_p^*$ where $p-1$ has many small factors. Another example is when using elliptic curves $E : y^2 = x^3 + a_4 x + a_6$; since the addition formula does not feature the value a_6 one can pass an honest user a point of small order on some curve $E'(\mathbb{F}_p)$. A related example is when using x-coordinate only arithmetic on elliptic curves one can choose an x-coordinate corresponding to a point that lies on the quadratic twist. For further discussion is given in Section 4.3 of [274] and a summary of the history of these results is given in Section 4.7 of [274]. We stress that such attacks do not only arise in encryption, but also in authenticated key exchange protocols, undeniable signatures, etc. The general way to avoid such attacks is for all parties to test membership of group elements in every step of the protocol (see Section 11.6).

Exercise 20.4.6. Show how a CCA1 attacker on classic textbook Elgamal can compute u^a for a group element u of their choice where a is the private key of a user. Show that if this attack can be repeated for sufficiently many elements u of coprime small orders then the private key a can be computed.

20.4.3 Semantic Security Under Passive Attacks

A serious problem with the classic textbook Elgamal cryptosystem is that, even though encryption is randomised, it does not necessarily provide semantic security under passive attacks.

Example 20.4.7. Consider the case $G = \mathbb{F}_p^*$, $\mathsf{M} = G$. Let $g \in G$ have prime order r. Then the Legendre symbol of g is $(\frac{g}{p}) = 1$. Hence, the Legendre symbol of the message m satisfies

$$(\tfrac{\mathsf{m}}{p}) = (\tfrac{\mathsf{c}_2}{p})$$

and so can be computed in polynomial-time from the public key and the ciphertext.

To prevent the attack in Example 20.4.7 one can restrict the message space to elements of $\mathbb{F}_p^*$ with Legendre symbol 1. However, this attack is just a special case of a more general phenomenon. The Legendre symbol is a homomorphism $\mathbb{F}_p^* \to G_1$ where $G_1 = \{-1, 1\} \subset \mathbb{F}_p^*$ is the subgroup of order 2. The attack can be performed for any homomorphism onto a subgroup of order coprime to r (this is a slightly different application of the ideas of Section 13.2).

Example 20.4.8. (Boneh, Joux and Nguyen [82]) Let p be a 3072-bit prime and let $r \mid (p-1)$ be a 256-bit prime. Let $g \in \mathbb{F}_p^*$ have order r. Suppose, in violation of the description of classic textbook Elgamal in Section 20.3, one chooses the message space to be

$$\mathsf{M} = \{1, 2, \ldots, 2^{32} - 1\}$$

interpreted as a subset of $\mathbb{F}_p^*$. We identify M with $\{0,1\}^{32} - \{0\}$. Let $(\mathsf{c}_1 = g^k, \mathsf{c}_2 = \mathsf{m}h^k)$ be a challenge ciphertext for classic textbook Elgamal encryption, where $\mathsf{m} \in \mathsf{M}$. Then

$$\mathsf{c}_2^r = \mathsf{m}^r.$$

One expects that, with overwhelming probability, the 2^{32} values m^r are distinct, and hence one can obtain m with at most 2^{32} exponentiations in $\mathbb{F}_p^*$.

Exercise 20.4.9. (Boneh, Joux and Nguyen [82]) Let p and $r \mid (p-1)$ be prime and let $g \in \mathbb{F}_p^*$ have order r. Suppose one uses classic textbook Elgamal with restricted message space $\mathsf{M} = \{0,1\}^m - \{0\}$ as in Example 20.4.8 where $\#\mathsf{M} = 2^m - 1 < p/r$. Extend the attack of Example 20.4.8 using the baby-step-giant-step method, so that it requires $O(2^{m/2+\epsilon})$ exponentiations in G to find m with noticeable probability, for $\epsilon > 0$.

One way to avoid these attacks is to restrict the message space to $\langle g \rangle$. It is then intuitively clear that IND security under passive attacks depends on the decisional Diffie-Hellman problem.

Theorem 20.4.10. *Classic textbook Elgamal with $\mathsf{M} = \langle g \rangle$ has IND-CPA security if and only if the DDH problem is hard.*

Proof: (For perfect oracles.) First we show IND-CPA $\leq_R$ DDH: Let A be an oracle to solve DDH. Let $(\mathsf{c}_1, \mathsf{c}_2)$ be a ciphertext that is an encryption of either m_0 or m_1. Call $A(g, \mathsf{c}_1, h_A, \mathsf{c}_2\mathsf{m}_0^{-1})$ and if the answer is 'yes' then the message is m_0 and if the answer is 'no' then the message is m_1.

For the converse (i.e., DDH $\leq_R$ IND-CPA of Elgamal): Let A be an oracle that breaks indistinguishability of Elgamal. Then A takes as input a public key (g, h), a pair of messages $\mathsf{m}_0, \mathsf{m}_1$ and a ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$ and outputs either 0 or 1. (We assume that A outputs either 0 or 1 even if the ciphertext corresponds to neither message.) Given a DDH instance (g, g_1, g_2, g_3) we repeatedly do the following: choose two random messages m_0 and m_1 in $\langle g \rangle$, choose a random $i \in \{0,1\}$, and call A on the input $(g, g_1, \mathsf{m}_0, \mathsf{m}_1, g_2, \mathsf{m}_i g_3)$. If A outputs i every time then we return 'yes' as the answer to the DDH. If A only outputs the correct answer i about half of the time, then we return 'no'. To be sure the decryption oracle is not just being lucky one should repeat the experiment $\Omega(\log(r))$ times. □

If the hash function is sufficiently good then one does not have to make as strong an assumption as DDH to show that semi-textbook Elgamal encryption has IND security. Instead, the IND security intuitively only depends on CDH. Theorem 20.4.11 is a basic example of a security proof in the random oracle model (see Section 3.7 for background on this model). We give the proof as it illustrates one of the ways the random oracle model is used in theoretical cryptography.

Theorem 20.4.11. *In the random oracle model, semi-textbook Elgamal encryption has IND-CPA security if CDH is hard.*

Proof: (Sketch) Let A be an adversary for the IND-CPA game on semi-textbook Elgamal encryption. Let g, g^a, g^b be a CDH instance. We will describe a simulator S that will solve the CDH problem using A as a subroutine.

First S runs the adversary A with public key (g, g^a).

The simulator must handle the queries made by A to the random oracle. To do this it stores a list of hash values, initially empty. Let g_i be the input for the $i-$th hash query. If $g_i = g_j$ for some $1 \leq j < i$ then we respond with the same value as used earlier. If not then the simulator chooses uniformly at random an element $H_i \in \{0,1\}^l$, stores (g_i, H_i) in the list, and answers the query $H(g_i)$ with H_i. This is a perfect simulation of a random oracle, at least until the challenge ciphertext is issued below.

At some time A outputs a pair of messages m_0 and m_1. The simulator sets $\mathsf{c}_1 = g^b$, chooses c_2 uniformly at random in $\{0,1\}^l$ and responds with the challenge ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$. The adversary A may make further hash function queries (which are answered using the algorithm above) and eventually A outputs $b \in \{0,1\}$ (of course A may crash, or run for longer than its specified running time, in which case S treats this as the output 0).

The logic of the proof is as follows: If A never queries the random oracle H on g^{ab} then A has no information on $H(g^{ab})$ and so cannot determine whether the answer should be 0 or 1. Hence, for A to succeed then one of the queries on H must have been on g^{ab}. Once this query is made then the simulator is seen to be fake as the adversary can check that c_2 is not equal to $\mathsf{m}_b \oplus H(g^{ab})$ for $b \in \{0,1\}$. However, the simulator is not concerned with this issue since it knows that g^{ab} occurs somewhere in the list of hash queries.

The simulator therefore chooses a random index i and responds with g_i as its solution to the CDH instance. □

Exercise 20.4.12. Fill the gaps in the proof of Theorem 20.4.11 and determine the exact probability of success in terms of the success of the adversary and the number of queries to the random oracle.

The power of the random oracle model is clear: we have been able to "look inside" the adversary's computation.

Exercise 20.4.13. Prove the converse to Theorem 20.4.11.

Indeed, the same technique leads to a much stronger result.

Theorem 20.4.14. *In the Random Oracle Model, semi-textbook Elgamal encryption has OWE-CPA security if CDH is hard.*

Exercise 20.4.15. Prove Theorem 20.4.14.

20.5 Security of Diffie-Hellman Key Exchange

A discussion of security models for key exchange is beyond the scope of this book. We refer to Bellare and Rogway [39], Bellare, Pointcheval and Rogaway [37], Bellare, Canetti and Krawczyk [32], Canetti and Krawczyk [116], Shoup [554], Boyd and Mathuria [94] and Menezes, van Oorschot and Vanstone [418] for details. However, as a rough approximation we can consider three types of adversary:

- Passive adversary (also called "benign" in [39]). This attacker obtains all messages sent during executions of the key exchange protocol but does not modify or delete any messages. This attacker is also called an eavesdropper.
- Weak[3] active adversary. This attacker obtains all messages sent during executions of the key exchange protocol and can modify or delete messages. This attacker can also initiate protocol executions with any player.

[3]This use of the word "weak" is non-standard.

- Active adversary. This is as above, but the attacker is allowed to corrupt any honest player who has completed an execution of the protocol and thus obtain the agreed key.

There are two possible goals of an adversary:

- To obtain the shared session key.

- To distinguish the session key from a random key. To make this notion more precise consider a game between an adversary and a challenger. The challenger performs one or more executions of the key exchange protocol and obtains a key K. The challenger also chooses uniformly at random a key K' from the space of possible session keys. The challenger gives the adversary either K or K' (with probability $1/2$). The adversary has to decide whether the received key is K or not. This is called **real or random security**.

The Diffie-Hellman key exchange protocol is vulnerable to a person-in-the-middle attack. Unlike similar attacks on public key encryption, the attacker in this case does not need to replace any users' public keys.

Imagine that an adversary Eve can intercept all communication between Alice and Bob. When Alice sends $\mathsf{c}_1 = g^a$ to Bob, Eve stores c_1 and sends g^e to Bob, for some random integer e known to Eve. Similarly, when Bob sends $\mathsf{c}_2 = g^b$ to Alice, Eve stores c_2 and sends g^e to Alice. Alice computes the key g^{ae} and Bob computes the key g^{be}. Eve can compute both keys. If Alice later sends an encrypted message to Bob using the key g^{ae} then Eve can decrypt it, read it, re-encrypt using the key g^{be}, and forward to Bob. Hence Alice and Bob might never learn that their security has been compromised.

One way to overcome person-in-the-middle attacks is for Alice to send a digital signature on her value g^a (and similarly for Bob). As long as Alice and Bob each hold authentic copies of the other's public keys then this attack fails. Note that this solution does not prevent all attacks on the Diffie-Hellman key exchange protocol.

Another solution is given by authenticated key exchange protocols such as STS, KEA, MTI, MQV, etc (see Chapter 11 of Stinson [592] and the references listed earlier).

We illustrate the basic idea behind most protocols of this type using the **MTI/A0 protocol**: Alice and Bob have public keys $h_A = g^a$ and $h_B = g^b$. We assume that Alice and Bob have authentic copies of each others public keys. They perform Diffie-Hellman key exchange in the usual way (Alice sends g^x and Bob sends g^y). Then the value agreed by both players is

$$g^{ay+bx}.$$

Exercise 20.5.1. Explain why the person-in-the-middle attack fails for this protocol (assuming the public key authentication process is robust).

Exercise 20.5.2. Consider a key exchange protocol where Alice and Bob have public keys $h_A = g^a$ and $h_B = g^b$, where Alice sends g^x and Bob sends g^y and where the shared key is g^{ab+xy}. Show that if corrupt queries are allowed then this key exchange protocol does not provide authentication.

Exercise 20.5.3. Give a person-in-the-middle attack on the Burmester-Desmedt protocol.

20.6 Efficiency Considerations for Discrete Logarithm Cryptography

All cryptographic protocols whose security is related to the DLP involve computations of the form g^a at some stage, and this is usually the most demanding computation in terms of time and computing resources. To make the cryptosystem fast it is natural to try to speed up exponentiation. One could try working in a smaller group, however it is important to ensure that the security of the system is maintained. Indeed, many of the main topics in this book (e.g., tori, elliptic curves and hyperelliptic curves) are attempts to get the "most efficient" group for a given security level.

A number of methods to speed up exponentiation in certain groups have already been presented. Section 11.1 discussed signed expansions, which are suitable for groups (such as elliptic and hyperelliptic curves or tori) where inversion is very efficient. Section 11.3 presented Frobenius expansions and the GLV method, which are suitable for elliptic curves. Those methods all assume that the exponent a takes any value.

One can also consider methods that do not correspond to values a chosen uniformly at random. Such methods can be much faster than the general methods already mentioned, but understanding the security implications can be more complicated. We do not have space to describe any of these methods in detail, but we briefly mention some of them.

1. Choose a to have low Hamming weight. This is mentioned by Agnew, Mullin, Onyszchuk and Vanstone [5] and Schnorr [523].

2. Choose a to be a random Frobenius expansion of low Hamming weight. This is credited to H. W. Lenstra Jr. in Section 6 of Koblitz [347].

3. Choose a to be given by a random addition chain (or addition-subtraction chain). This is proposed in Section 3.3 of Schroeppel, Orman, O'Malley and Spatscheck [532].

4. Choose a to be a product of integers of low Hamming weight. This was proposed and analysed by Hoffstein and Silverman [290].

5. Choosing a to be a random element in GLV representation, possibly with smaller than typical coefficients.

6. Generate random elements using large amounts of precomputation. A solution that can be used in any group is given by Boyko, Peinado and Venkatesan [96]. The method requires precomputing and storing random powers $g_j = g^{a_j}$. One generates a random pair (a, g^a) by taking the product of a random subset of the g^{a_j} and setting $a = \sum a_j \pmod r$. This method is presented as the "simple solution" in [152].

   A more sophisticated method for Koblitz curves is given by Coron, M'Raïhi and Tymen [152]. They use repeated application of sparse Frobenius expansions on elements of the precomputed table. They also give a security analysis.

Chapter 21

The Diffie-Hellman Problem

This chapter gives a thorough discussion of the computational Diffie-Hellman problem (CDH) and related computational problems. We give a number of reductions between computational problems, most significantly reductions from DLP to CDH. We explain self-correction of CDH oracles, study the static Diffie-Hellman problem, and study hard bits of the DLP and CDH. We always use multiplicative notation for groups in this chapter (except for in the Maurer reduction where some operations are specific to elliptic curves).

21.1 Variants of the Diffie-Hellman Problem

We present some computational problems related to CDH, and prove reductions among them. The main result is to prove that CDH and Fixed-CDH are equivalent. Most of the results in this section apply to both algebraic groups (AG) and algebraic group quotients (AGQ) of prime order r (some exceptions are Lemma 21.1.9, Lemma 21.1.16 and, later, Lemma 21.3.1). For the algebraic group quotients G considered in this book then one can obtain all the results by lifting from the quotient to the covering group G' and applying the results there.

A subtle distinction is whether the base element $g \in G$ is considered fixed or variable in a CDH instance. To a cryptographer it is most natural to assume the generator is fixed, since that corresponds to the usage of cryptosystems in the real world (the group G and element $g \in G$ are fixed for all users). Hence, an adversary against a cryptosystem leads to an oracle for a fixed generator problem. To a computational number theorist it is most natural to assume the generator is variable, since algorithms in computational number theory usually apply to all problem instances. Hence both problems are studied in the literature and when an author writes CDH it is sometimes not explicit which of the variants is meant. Definition 20.2.1 was for the case when g varies. Definition 21.1.1 below is the case when g is fixed. This issue is discussed in Section 5 of Shoup [554] and in Sadeghi and Steiner [508] (where it is called "granularity").

Definition 21.1.1. Let G be an algebraic group (AG) or algebraic group quotient (AGQ) and let $g \in G$. The **Fixed-base computational Diffie-Hellman problem (Fixed-CDH)** with respect to g is: Given (g^a, g^b) to compute g^{ab}.

In this book the acronym CDH will always refer to the case where g is allowed to vary. Hence, an algorithm for CDH will always take three inputs (formally we should also include a description of the underlying group G, but we assume this is implicit in the specification of g) while an algorithm for Fixed-CDH will always take two inputs.

It is trivial that Fixed-CDH $\leq_R$ CDH, but the reverse implication is less obvious; see Corollary 21.1.18 below.

Analogously, given $g \in G$ one can define Fixed-DLP (namely, given h to find a such that $h = g^a$) and Fixed-DDH (given (g^a, g^b, g^c) determine whether $g^c = g^{ab}$). Though Fixed-DLP is equivalent to DLP (see Exercise 21.1.2) it is not expected that DDH is equivalent to Fixed-DDH (see Section 5.3.4 of [554]).

Exercise 21.1.2. Prove that Fixed-DLP is equivalent to DLP.

Exercise 21.1.3. Let G be a cyclic group of prime order r. Let $h_1, h_2, h_3 \in G$ such that $h_j \neq 1$ for $j = 1, 2, 3$. Show there exists some $g \in G$ such that (g, h_1, h_2, h_3) is a Diffie-Hellman tuple.

We now introduce some other variants of CDH. These are interesting in their own right, but are also discussed as they play a role in the proof of equivalence between CDH and Fixed-CDH.

Definition 21.1.4. Let G be a group or algebraic group quotient of prime order r. The computational problem **Inverse-DH** is: given a pair $g, g^a \in G - \{1\}$ of elements of prime order r in G to compute $g^{a^{-1} \pmod r}$. (Clearly, we must exclude the case $a = 0$ from the set of instances.)

Lemma 21.1.5. *Inverse-DH $\leq_R$ CDH.*

Proof: Suppose O is a perfect oracle for solving CDH. Let $(g, g_1 = g^a)$ be the given Inverse-DH instance. Then

$$g = g_1^{a^{-1}}.$$

Calling $O(g_1, g, g) = O(g_1, g_1^{a^{-1}}, g_1^{a^{-1}})$ gives $g_1^{a^{-2}}$. Finally,

$$g_1^{a^{-2}} = (g^a)^{a^{-2}} = g^{a^{-1}}$$

as required. □

Definition 21.1.6. Let G be an AG or AGQ. The computational problem **Square-DH** is: given (g, g^a) where $g \in G$ has prime order r to compute g^{a^2}.

Exercise 21.1.7. Show that Square-DH $\leq_R$ CDH.

Lemma 21.1.8. *Square-DH $\leq_R$ Inverse-DH.*

Proof: Let O be a perfect oracle that solves Inverse-DH and let $(g, g_1 = g^a)$ be given. If $g_1 = 1$ then return 1. Otherwise, we have

$$O(g_1, g) = O(g_1, g_1^{a^{-1}}) = g_1^a = (g^a)^a = g^{a^2}.$$

□

Hence Square-DH $\leq_R$ Inverse-DH $\leq_R$ CDH. Finally we show CDH $\leq_R$ Square-DH and so all these problems are equivalent.

Lemma 21.1.9. *Let G be a group of odd order. Then CDH $\leq_R$ Square-DH.*

Proof: Let (g, g^a, g^b) be a CDH instance. Let O be a perfect oracle for Square-DH. Call $O(g, g^a)$ to get $g_1 = g^{a^2}$, $O(g, g^b)$ to get $g_2 = g^{b^2}$ and $O(g, g^a g^b)$ to get $g_3 = g^{a^2+2ab+b^2}$.

Now compute

$$(g_3/(g_1 g_2))^{2^{-1} \pmod r},$$

which is g^{ab} as required. □

Exercise 21.1.10. Let G be a group of prime order r. Show that Inverse-DH and Square-DH are random self-reducible. Hence give a self-corrector for Square-DH. Finally, show that Lemma 21.1.9 holds for non-perfect oracles. (Note that it seems to be hard to give a self-corrector for Inverse-DH directly, though one can do this via Lemma 21.1.8.)

Note that the proofs of Lemmas 21.1.5 and 21.1.8 require oracle queries where the first group element in the input is not g. Hence, these proofs do not apply to variants of these problems where g is fixed. We now define the analogous problems for fixed g and give reductions between them.

Definition 21.1.11. Let g have prime order r and let $G = \langle g \rangle$. The computational problem **Fixed-Inverse-DH** is: given $g^a \neq 1$ to compute $g^{a^{-1} \pmod r}$. Similarly, the computational problem **Fixed-Square-DH** is: given g^a to compute g^{a^2}.

Exercise 21.1.12. Show that Fixed-Inverse-DH and Fixed-Square-DH are random self-reducible.

Lemma 21.1.13. *Let $g \in G$. Let A be a perfect Fixed-CDH oracle. Let $h = g^a$ and let $n \in \mathbb{N}$. Then one can compute $g^{a^n \pmod r}$ using $\leq 2\log_2(n)$ queries to A.*

Proof: Assume A is a perfect Fixed-CDH oracle. Define $h_i = g^{a^i \pmod r}$ so that $h_1 = h$. One has $h_{2i} = A(h_i, h_i)$ and $h_{i+1} = A(h_i, h)$. Hence one can compute h_n by performing the standard square-and-multiply algorithm for efficient exponentiation. □

Note that the number of oracle queries in Lemma 21.1.13 can be reduced by using window methods or addition chains.

Exercise 21.1.14. Show that if the conjecture of Stolarsky (see Section 2.8) is true then one can compute g^{a^n} in $\log_2(n) + \log_2(\log_2(n))$ Fixed-CDH oracle queries.

Lemma 21.1.15. *Fixed-Inverse-DH $\leq_R$ Fixed-CDH.*

Proof: Fix $g \in G$. Let O be a perfect Fixed-CDH oracle. Let g^a be the given Fixed-Inverse-DH instance. Our task is to compute $g^{a^{-1}}$. The trick is to note that $a^{-1} = a^{r-2} \pmod r$. Hence, one computes $g^{a^{r-2}}$ using Lemma 21.1.13. The case of non-perfect oracles requires some care, although at least one can check the result using O since one should have $O(g^a, g^{a^{-1}}) = g$. □

Lemma 21.1.16. *Fixed-Square-DH $\leq_R$ Fixed-Inverse-DH.*

Proof: Let $h = g^a$ be the input Fixed-Square-DH instance and let A be a perfect oracle for the Fixed-Inverse-DH problem. Call $A(gh)$ to get $g^{(1+a)^{-1}}$ and call $A(gh^{-1})$ to get $g^{(1-a)^{-1}}$.

Multiplying these outputs gives

$$w = g^{(1+a)^{-1}} g^{(1-a)^{-1}} = g^{2(1-a^2)^{-1}}.$$

Calling $A(w^{2^{-1} \pmod r})$ gives g^{1-a^2} from which we compute g^{a^2} as required. □

We can now solve a non-fixed problem using an oracle for a fixed problem.

Lemma 21.1.17. *Square-DH $\leq_R$ Fixed-CDH.*

Proof: Let $g \in G$ be fixed of prime order r and let A be a perfect Fixed-CDH oracle. Let g_1, g_1^b be the input Square-DH problem. Write $g_1 = g^a$. We are required to compute $g_1^{b^2} = g^{ab^2}$.

Call $A(g_1^b, g_1^b)$ to compute $g^{a^2b^2}$. Use the perfect Fixed-CDH oracle as in Lemma 21.1.15 to compute $g^{a^{-1}}$. Then compute $A(g^{a^2b^2}, g^{a^{-1}})$ to get g^{ab^2}. □

Since CDH $\leq_R$ Square-DH we finally obtain the main result of this section.

Corollary 21.1.18. *Fixed-CDH and CDH are equivalent.*

Proof: We already showed Fixed-CDH $\leq_R$ CDH. Now, let A be a perfect Fixed-CDH oracle. Lemma 21.1.17 together with Lemma 21.1.9 gives CDH $\leq_R$ Square-DH $\leq_R$ Fixed-CDH as required.

Now suppose A only succeeds with noticeable probability $\epsilon > 1/\log(r)^c$ for some fixed c. The reductions CDH $\leq_R$ Square-DH $\leq_R$ Fixed-CDH require $O(\log(r))$ oracle queries. We perform self-correction (see Section 21.3) to obtain an oracle A for Fixed-CDH that is correct with probability $1 - 1/(\log(r)^{c'})$ for some constant c'; by Theorem 21.3.8 this requires $O(\log(r)^c \log\log(r))$ oracle queries. □

Exercise 21.1.19. It was assumed throughout this section that G has prime order r. Suppose instead that G has order $r_1 r_2$ where r_1 and r_2 are distinct odd primes and that g is a generator for G.

Prove that if one has a perfect CDH oracle O_1 that applies in the subgroup of order r_1, and a perfect CDH oracle O_2 that applies in the subgroup of order r_2, then one can solve CDH in G.

More generally in this context, which of the results in this section no longer necessarily hold? Is Fixed-CDH in $\langle g \rangle$ equivalent to Fixed-CDH in $\langle g^{r_1} \rangle$?

We end with a variant of the DDH problem.

Exercise 21.1.20. Let g have prime order r and let $\{x_1, \ldots, x_n\} \subset \mathbb{Z}/r\mathbb{Z}$. For a subset $A \subset \{1, \ldots, n\}$ define

$$g^A = g^{\prod_{i \in A} x_i}.$$

The **group decision Diffie-Hellman problem** (GDDH) is: Given g, g^A for all proper subsets $A \subsetneq \{1, \ldots, n\}$, and h, to distinguish $h = g^c$ (where $c \in \mathbb{Z}/r\mathbb{Z}$ is chosen uniformly at random) from $g^{x_1 x_2 \cdots x_n}$. Show that GDDH $\equiv$ DDH.

21.2 Lower Bound on the Complexity of CDH for Generic Algorithms

We have seen (Theorem 13.4.5) that a generic algorithm requires $\Omega(\sqrt{r})$ group operations to solve the DLP in a group of order r. Shoup proved an analogue of this result for CDH. As before, fix $t \in \mathbb{R}_{>0}$ and assume that all group elements are represented by bitstrings of length at most $t \log(r)$.

Theorem 21.2.1. *Let G be a cyclic group of prime order r. Let A be a generic algorithm for CDH in G that makes at most m oracle queries. Then the probability that $A(\sigma(g), \sigma(g^a), \sigma(g^b)) = \sigma(g^{ab})$ over $a, b \in \mathbb{Z}/r\mathbb{Z}$ and an encoding function $\sigma : G \to S \subseteq \{0,1\}^{\lceil t \log(r) \rceil}$ chosen uniformly at random is $O(m^2/r)$.*

Proof: The proof is almost identical to the proof of Theorem 13.4.5. Let $S = \{0,1\}^{\lceil t \log(r) \rceil}$. The simulator begins by uniformly choosing three distinct $\sigma_1, \sigma_2, \sigma_3$ in S and running $A(\sigma_1, \sigma_2, \sigma_3)$. The encoding function is then specifed at the two points $\sigma_1 = \sigma(g)$ and $\sigma_2 = \sigma(h)$. From the point of view of A, g and h are independent distinct elements of G.

It is necessary to ensure that the encodings are consistent with the group operations. This cannot be done perfectly without knowledge of a and b, but using polynomials as previously ensures there are no "trivial" inconsistencies. The simulator maintains a list of pairs (σ_i, F_i) where $\sigma_i \in S$ and $F_i \in \mathbb{F}_r[x,y]$ (indeed, the $F_i(x,y)$ will always be linear). The initial values are $(\sigma_1, 1)$, (σ_2, x) and (σ_3, y). Whenever A makes an oracle query on (σ_i, σ_j) the simulator computes $F = F_i - F_j$. If F appears as F_k in the list of pairs then the simulator replies with σ_k and does not change the list. Otherwise, an element $\sigma \in S$, distinct from the previously used values, is chosen uniformly at random, (σ, F) is added to the simulator's list, and σ is returned to A.

After making at most m oracle queries, A outputs $\sigma_4 \in \mathbb{Z}/r\mathbb{Z}$. The simulator now chooses a and b uniformly at random in $\mathbb{Z}/r\mathbb{Z}$. Algorithm A wins if $\sigma_4 = \sigma(g^{ab})$. Note that if σ_4 is not σ_1, σ_2 or one of the strings output by the oracle then the probability of success is at most $1/(2^{\lceil t \log(r) \rceil} - m - 2)$. Hence we assume that σ_4 is on the simulator's list.

Let the simulator's list contain precisely k polynomials $\{F_1(x,y), \ldots, F_k(x,y)\}$ for some $k \leq m+3$. Let E be the event that $F_i(a,b) = F_j(a,b)$ for some pair $1 \leq i < j \leq k$ or $F_i(a,b) = ab$. The probability that A wins is

$$\Pr(A \text{ wins } | E) \Pr(E) + \Pr(A \text{ wins } | \neg E) \Pr(\neg E). \tag{21.1}$$

For each pair $1 \leq i < j \leq k$ the probability that $(F_i - F_j)(a,b) = 0$ is $1/r$ by Lemma 13.4.4. Similarly, the probability that $F_i(a,b) - ab = 0$ is $2/r$. Hence, the probability of event E is at most $k(k+1)/2r + 2k/r = O(m^2/r)$. On the other hand, if event E does not occur then all A "knows" about (a,b) is that it lies in the set

$$\mathcal{X} = \{(a,b) \in (\mathbb{Z}/r\mathbb{Z})^2 : F_i(a,b) \neq F_j(a,b) \text{ for all } 1 \leq i < j \leq k \text{ and } F_i(a,b) \neq ab \text{ for all } 1 \leq i \leq k\}.$$

Let $N = \#\mathcal{X} \approx r^2 - m^2/2$ Then $\Pr(\neg E) = N/r^2$ and $\Pr(A \text{ wins } | \neg E) = 1/N$.

Hence, the probability that A wins is $O(m^2/r)$. □

21.3 Random Self-Reducibility and Self-Correction of CDH

We defined random self-reducibility in Section 2.1.4. Lemma 2.1.19 showed that the DLP in a group G of prime order r is random self-reducible. Lemma 2.1.20 showed how to obtain an algorithm with arbitrarily high success probability for the DLP from an algorithm with noticeable success probability.

Lemma 21.3.1. *Let g have order r and let $G = \langle g \rangle$. Then CDH in G is random self-reducible.*

Proof: Let $\mathcal{X} = (G - \{1\}) \times G^2$ Let $(g, h_1, h_2) = (g, g^a, g^b) \in \mathcal{X}$ be the CDH instance. Choose uniformly at random $1 \leq u < r$ and $0 \leq v, w < r$ and consider the triple $(g^u, h_1^u g^{uv}, h_2^u g^{uw}) = (g^u, (g^u)^{a+v}, (g^u)^{b+w}) \in \mathcal{X}$. Then every triple in $\mathcal{X}$ arises from exactly one triple (u,v,w). Hence, the new triples are uniformly distributed in $\mathcal{X}$. If $Z = (g^u)^{(a+v)(b+w)}$ is the solution to the new CDH instance then the solution to the original CDH instance is

$$Z^{u^{-1} \pmod r} h_1^{-w} h_2^{-v} g^{-vw}.$$

□

Exercise 21.3.2. Show that Fixed-CDH is random self-reducible in a group of prime order r.

The following problem[1] is another cousin of the computational Diffie-Hellman problem. It arises in some cryptographic protocols.

Definition 21.3.3. Fix g of prime order r and $h = g^a$ for some $1 \leq a < r$. The **static Diffie-Hellman problem** (**Static-DH**) is: Given $h_1 \in \langle g \rangle$ to compute h_1^a.

Exercise 21.3.4. Show that the static Diffie-Hellman problem is random self-reducible.

One can also consider the decision version of static Diffie-Hellman.

Definition 21.3.5. Fix g of prime order r and $h = g^a$ for some $1 \leq a < r$. The **decision static Diffie-Hellman problem** (**DStatic-DH**) is: Given $h_1, h_2 \in \langle g \rangle$ to determine whether $h_2 = h_1^a$.

We now show that DStatic-DH is random-self-reducible. This is a useful preliminary to showing how to deal with DDH.

Lemma 21.3.6. *Fix g of prime order r and $h = g^a$ for some $1 \leq a < r$. Then the decision static Diffie-Hellman problem is random self-reducible.*

Proof: Write $G = \langle g \rangle$. Choose $1 \leq w < r$ and $0 \leq x < r$ uniformly at random. Given (h_1, h_2) compute $(Z_1, Z_2) = (h_1^w g^x, h_2^w h^x)$. We must show that if (h_1, h_2) is (respectively, is not) a valid Static-DH pair then (Z_1, Z_2) is uniformly distributed over the set of all valid (resp. invalid) Static-DH pairs.

First we deal with the case of valid Static-DH pairs. It is easy to check that if $h_2 = h_1^a$ then $Z_2 = Z_1^a$. Furthermore, for any pair $Z_1, Z_2 \in G$ such that $Z_2 = Z_1^a$ then one can find exactly $(r-1)$ pairs (w, x) such that $Z_1 = h_1^w g^x$.

On the other hand, if $h_2 \neq h_1^a$ then write $h_1 = g^b$ and $h_2 = g^c$ with $c \not\equiv ab \pmod{r}$. For any pair $(Z_1, Z_2) = (g^y, g^z) \in G^2$ such that $z \not\equiv ay \pmod{r}$ we must show that (Z_1, Z_2) can arise from precisely one choice (w, x) above. Indeed,

$$\begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} b & 1 \\ c & a \end{pmatrix} \begin{pmatrix} w \\ x \end{pmatrix}$$

and, since the matrix has determinant $ab - c \not\equiv 0 \pmod{r}$ one can show that there is a unique solution for (w, x) and that $w \not\equiv 0 \pmod{r}$. □

We now tackle the general case of decision Diffie-Hellman.

Lemma 21.3.7. *Let g have prime order r and let $G = \langle g \rangle$. Then DDH in G is random self-reducible.*

Proof: Choose $1 \leq u, w < r$ and $0 \leq v, x < r$ uniformly at random. Given $(g, h_1, h_2, h_3) = (g, g^a, g^b, g^c)$ define the new tuple $(g^u, h_1^u g^{uv}, h_2^{uw} g^{ux}, h_3^{uw} h_1^{ux} h_2^{vw} g^{uvx})$. One can verify that the new tuple is a valid Diffie-Hellman tuple if and only if the original input is a valid Diffie-Hellman tuple (i.e., $c = ab$). If the original tuple is a valid Diffie-Hellman tuple then the new tuple is uniformly distributed among all Diffie-Hellman tuples. Finally, we show that if the original tuple is not a valid Diffie-Hellman tuple then the new tuple is uniformly distributed among the set of all invalid Diffie-Hellman tuples. To see this think

[1] The Static-DH problem seems to have been first studied by Brown and Gallant [111].

of (h_2, h_3) as a DStatic-DH instance with respect to the pair (g, h_1). Since $(g^u, h_1^u g^{uv})$ is chosen uniformly at random from $(G - \{1\}) \times G$ we have a uniformly random DStatic-DH instance with respect to a uniformly random static pair. The result then follows from Lemma 21.3.6. □

It is easy to turn a DLP oracle that succeeds with noticeable probability ϵ into one that succeeds with probability arbitrarily close to 1, since one can check whether a solution to the DLP is correct. It is less easy to amplify the success probability for a non-perfect CDH oracle.

A natural (but flawed) approach is just to run the CDH oracle on random self-reduced instances of CDH until the same value appears twice. We now explain why this approach will not work in general. Consider a Fixed-CDH oracle that, on input (g^a, g^b), returns $g^{ab+\xi}$ where $\xi \in \mathbb{Z}$ is uniformly chosen between $-1/\log(r)$ and $1/\log(r)$. Calling the oracle on instances arising from the random self-reduction of Exercise 21.3.2 one gets a sequence of values $g^{ab+\xi}$. Eventually the correct value g^{ab} will occur twice, but it is quite likely that some other value will occur twice before that time.

We present Shoup's self-corrector for CDH or Fixed-CDH from [553].[2] Also see Cash, Kiltz and Shoup [120].

Theorem 21.3.8. *Fix $l \in \mathbb{N}$. Let g have prime order r. Let A be a CDH (resp. Fixed-CDH) oracle with success probability at least $\epsilon > \log(r)^{-l}$. Let (g, g^a, g^b) be a CDH instance. Let $1 > \epsilon' > 1/r$. Then one can obtain an oracle that solves the CDH (resp. Fixed-CDH) with probability at least $1 - \epsilon' - \log(2r)^2/(r\epsilon^2)$ and that makes at most $2\lceil \log(2/\epsilon')/\epsilon \rceil$ queries to A (where* log *is the natural logarithm).*

Proof: Define $c = \log(2/\epsilon') \in \mathbb{R}$ so that $e^{-c} = \epsilon'/2$. First call the oracle $n = \lceil c/\epsilon \rceil$ times on random-self-reduced instances (if the oracle is a CDH oracle then use Lemma 21.3.1 and if the oracle is a Fixed-CDH oracle then use Exercise 21.3.2) of the input problem (g, g^a, g^b) and store the resulting guesses $Z_1, \ldots, Z_n$ for g^{ab} in a list L_1. Note that $n = O(\log(r)^{l+1})$. The probability that L_1 contains at least one copy of g^{ab} is $\geq 1 - (1-\epsilon)^{c/\epsilon} \geq 1 - e^{-c} = 1 - \epsilon'/2$.

Now choose uniformly at random integers $1 \leq s_1, s_2 < r$ and define $X_2 = g^{s_1}/(g^a)^{s_2}$. One can show that X_2 is uniformly distributed in $G = \langle g \rangle$ and is independent of $X_1 = g^a$.

Call the oracle another n times on random-self-reduced versions of the CDH instance (g, X_2, g^b) and store the results $Z'_1, \ldots, Z'_n$ in a list L_2.

Hence, with probability $\geq (1 - \epsilon'/2)^2 \geq 1 - \epsilon'$ there is some $Z_i \in L_1$ and some $Z'_j \in L_2$ such that $Z_i = g^{ab}$ and $Z'_j = g^{b(s_1 - as_2)}$. For each $1 \leq i, j \leq n$ test whether

$$Z_i^{s_2} = (g^b)^{s_1}/Z'_j. \tag{21.2}$$

If there is a unique solution (Z_i, Z'_j) then output Z_i, otherwise output $\perp$. Finding Z_i can be done efficiently by sorting L_1 and then, for each $Z'_j \in L_2$, checking whether the value of the right hand side of equation (21.2) lies in L_1.

We now analyse the probability that the algorithm fails. The probability there is no pair (Z_i, Z'_j) satisfying equation (21.2), or that there are such pairs but none of them have $Z_i = g^{ab}$, is at most ϵ'. Hence, we now assume that a good pair (Z_i, Z'_j) exists and we want to bound the probability that there is a bad pair (i.e., a solution to equation (21.2) for which $Z_i \neq g^{ab}$). Write $X_1 = g^a$, $X_2 = g^{a'}$ (where $a' = s_1 - as_2$) and $Y = g^b$. Suppose (Z, Z') is a pair such that

$$Z^{s_2} Z' = Y^{s_1}. \tag{21.3}$$

[2] Maurer and Wolf [405] were the first to give a self-corrector for CDH, but Shoup's method is more efficient.

We claim that $Z = Y^a$ and $Z' = Y^{a'}$ with probability at least $1 - 1/q$. Note that if equation (21.3) holds then

$$(Z/Y^a)^{s_1} = Y^{a'}/Z'. \tag{21.4}$$

If precisely one of $Z = Y^a$ or $Z' = Y^{a'}$ holds then this equation does not hold. Hence, $Z \neq Y^a$ and $Z' \neq Y^{a'}$, in which case there is precisely one value for s_1 for which equation (21.4) holds. Considering all n^2 pairs $(Z, Z') \in L_1 \times L_2$ it follows there are at most n^2 values for s_1, which would lead to an incorrect output for the self-corrector. Since s_1 is chosen uniformly at random the probability of an incorrect output is at most n^2/r. Since $n \leq \log(2r)/\epsilon$ one gets the result. Note that $\log(2r)^2/(r\epsilon^2) = O(\log(r)^{2+2l}/r)$. □

Exercise 21.3.9. Extend Lemma 21.1.13 to the case of a non-perfect Fixed-CDH oracle. What is the number of oracle queries required?

21.4 The den Boer and Maurer Reductions

The goal of this section is to discuss reductions from DLP to CDH or Fixed-CDH in groups of prime order r. Despite having proved that Fixed-CDH and CDH are equivalent, we prefer to treat them separately in this section. The first such reduction (assuming a perfect Fixed-CDH oracle) was given by den Boer [169] in 1988. Essentially den Boer's method involves solving a DLP in $\mathbb{F}_r^*$, and so it requires $r - 1$ to be sufficiently smooth. Hence there is no hope of this approach giving an equivalence between Fixed-CDH and DLP for all groups of prime order.

The idea was generalised by Maurer [402] in 1994, by replacing the multiplicative group $\mathbb{F}_r^*$ by an elliptic curve group $E(\mathbb{F}_r)$. Maurer and Wolf [405, 406, 408] extended the result to non-perfect oracles. If $\#E(\mathbb{F}_r)$ is sufficiently smooth then the reduction is efficient. Unfortunately, there is no known algorithm to efficiently generate such smooth elliptic curves. Hence Maurer's result also does not prove equivalence between Fixed-CDH and DLP for all groups. A subexponential-time reduction that conjecturally applies to all groups was given by Boneh and Lipton [83]. An exponential-time reduction (but still faster than known algorithms to solve DLP) that applies to all groups was given by Muzereau, Smart and Vercauteren [448], and Bentahar [42, 43].

21.4.1 Implicit Representations

Definition 21.4.1. Let G be a group and let $g \in G$ have prime order r. For $a \in \mathbb{Z}/r\mathbb{Z}$ we call $h = g^a$ an **implicit representation** of a.

In this section we call the usual representation of $a \in \mathbb{Z}/r\mathbb{Z}$ the **explicit representation** of a.

Lemma 21.4.2. *There is an efficient (i.e., computable in polynomial-time) mapping from $\mathbb{Z}/r\mathbb{Z}$ to the implicit representations of $\mathbb{Z}/r\mathbb{Z}$. One can test equality of elements in $\mathbb{Z}/r\mathbb{Z}$ given in implicit representation. If h_1 is an implicit representation of a and h_2 is an implicit representation of b then h_1h_2 is an implicit representation of $a+b$ and h_1^{-1} is an implicit representation of $-a$.*

In other words, we can compute in the additive group $\mathbb{Z}/r\mathbb{Z}$ using implicit representations.

Lemma 21.4.3. *If h is an implicit representation of a and $b \in \mathbb{Z}/r\mathbb{Z}$ is known explicitly, then h^b is an implicit representation of ab.*

Let O be a perfect Fixed-CDH oracle with respect to g. Suppose h_1 is an implicit representation of a and h_2 is an implicit representation of b. Then $h = O(h_1, h_2)$ is an implicit representation of ab.

In other words, if one can solve Fixed-CDH then one can compute multiplication modulo r using implicit representatives.

Exercise 21.4.4. Prove Lemmas 21.4.2 and 21.4.3.

Lemma 21.4.5. *Let g have order r. Let h_1 be an implicit representation of a such that $h_1 \neq 1$ (in other words, $a \not\equiv 0 \pmod r$).*

1. *Given a perfect CDH oracle one can compute an implicit representation for $a^{-1} \pmod r$ using one oracle query.*
2. *Given a perfect Fixed-CDH oracle with respect to g one can compute an implicit representation for $a^{-1} \pmod r$ using $\leq 2\log_2(r)$ oracle queries.*

Proof: Given a perfect CDH oracle A one calls $A(g^a, g, g) = g^{a^{-1} \pmod r}$. Given a perfect Fixed-CDH oracle one computes $g^{a^{r-2} \pmod r}$ as was done in Lemma 21.1.15. □

To summarise, since $\mathbb{Z}/r\mathbb{Z} \cong \mathbb{F}_r$, given a perfect CDH or Fixed-CDH oracle then one can perform all field operations in $\mathbb{F}_r$ using implicit representations. Boneh and Lipton [83] call the set of implicit representations for $\mathbb{Z}/r\mathbb{Z}$ a **black box field**.

21.4.2 The den Boer Reduction

We now present the **den Boer reduction** [169], which applies when $r-1$ is smooth. The crucial idea is that the Pohlig-Hellman and baby-step-giant-step methods only require the ability to add, multiply and compare group elements. Hence, if a perfect CDH oracle is given then these algorithms can be performed using implicit representations.

Theorem 21.4.6. *Let $g \in G$ have prime order r. Suppose l is the largest prime factor of $r-1$. Let A be a perfect oracle for the Fixed-CDH problem with respect to g. Then one can solve the DLP in $\langle g \rangle$ using $O(\log(r)\log(\log(r)))$ oracle queries, $O(\log(r)(\sqrt{l}/\log(l) + \log(r))$ multiplications in $\mathbb{F}_r$ and $O(\sqrt{l}\log(r)^2/\log(l))$ operations in G (where the constant implicit in the $O(\cdot)$ does not depend on l).*

Proof: Let the challenge DLP instance be $g, h = g^a$. If $h = 1$ then return $a = 0$. Hence, we now assume $1 \leq a < r$. We can compute a primitive root $\gamma \in \mathbb{F}_r^*$ in $O(\log(r)\log(\log(r)))$ operations in $\mathbb{F}_r$ (see Section 2.15). The (unknown) logarithm of h satisfies

$$a \equiv \gamma^u \pmod r \tag{21.5}$$

for some integer u. To compute a it is sufficient to compute u.[3] The idea is to solve the DLP in equation (21.5) using the implicit representation of a. Since $r-1$ is assumed to be smooth then we can use the Pohlig-Hellman (PH) method, followed by the baby-step-giant-step (BSGS) method in each subgroup. We briefly sketch the details.

Write $r - 1 = \prod_{i=1}^{n} l_i^{e_i}$ where the l_i are prime. The PH method involves projecting a and γ into the subgroup of $\mathbb{F}_r^*$ of order $l_i^{e_i}$. In other words, we must compute

$$h_i = g^{a^{(r-1)/l_i^{e_i}}}$$

[3] It may seem crazy to try to work out u without knowing a, but it works!

for $1 \leq i \leq n$. Using the Fixed-CDH oracle to perform computations in implicit representation, Algorithm 4 computes all the h_i together in $O(\log(r)\log\log(r))$ oracle queries.[4] A further $O(\log(r))$ oracle queries are required to compute all $g^{a^{(r-1)/l_i^f}}$ where $0 \leq f < e_i$. Similarly one computes all $x_i = \gamma^{(r-1)/l_i^{e_i}}$ in $O(\log(r)\log\log(r))$ multiplications in $\mathbb{F}_r$. We then have

$$h_i = g^{x_i^{u \pmod{l_i^{e_i}}}}.$$

Following Section 13.2 one reduces these problems to $\sum_{i=1}^{n} e_i$ instances of the DLP in groups of prime order l_i. This requires $O(\log(r)^2)$ group operations and field operations overall (corresponding to the computations in line 6 of Algorithm 13).

For the baby-step-giant-step algorithm, suppose we wish to solve $g^a = g^{\gamma^u}$ (where, for simplicity, we redefine a and γ so that they now have order l modulo r). Set $m = \lceil \sqrt{l} \rceil$ and write $u = u_0 + mu_1$ where $0 \leq u_0, u_1 < m$. From

$$g^a = g^{\gamma^u} = g^{\gamma^{u_0+mu_1}} = g^{\gamma^{u_0}(\gamma^m)^{u_1}} \tag{21.6}$$

one has

$$(g^a)^{(\gamma^{-m})^{u_1}} = g^{\gamma^{u_0}}. \tag{21.7}$$

We compute and store (in a sorted structure) the baby steps g^{γ^i} for $i = 0, 1, 2, \ldots, m-1$ (this involves computing one exponentiation in G at each step, as $g^{\gamma^{i+1}} = (g^{\gamma^i})^{\gamma}$, which is at most $2\log_2(r)$ operations in G).

We then compute the giant steps $(g^a)^{\gamma^{-mj}}$. This involves computing $w_0 = \gamma^{-m} \pmod{r}$ and then the sequence $w_j = \gamma^{-mj} \pmod{r}$ as $w_{j+1} = w_i w_0 \pmod{r}$; this requires $O(\log(m) + m)$ multiplications in $\mathbb{F}_r$. We also must compute $(g^a)^{w_j}$, each of which requires $\leq 2\log_2(r)$ operations in G.

When we find a match then we have solved the DLP in the subgroup of order l. The BSGS algorithm for each prime l requires $O(\sqrt{l}\log(r))$ group operations and $O(\sqrt{l} + \log(r))$ operations in $\mathbb{F}_r$. There are $O(\log(r))$ primes l for which the BSGS must be run, but a careful analysis of the cost (using the result of Exercise 13.2.7) gives an overall running time of $O(\log(r)^2\sqrt{l}/\log(l))$ group operations and $O(\log(r)^2 + \log(r)\sqrt{l}/\log(l))$ multiplications in $\mathbb{F}_r$. Note that the CDH oracle is not required for the BSGS algorithm.

Once u is determined modulo all prime powers $l^e \mid (r-1)$ one uses the Chinese remainder theorem to compute $u \in \mathbb{Z}/(r-1)\mathbb{Z}$. Finally, one computes $a = \gamma^u \pmod{r}$. These final steps require $O(\log(r))$ operations in $\mathbb{F}_r$. □

Corollary 21.4.7. *Let $A(\kappa)$ be an algorithm that outputs triples (g, h, r) such that r is a κ-bit prime, g has order r, $r-1$ is $O(\log(r)^2)$-smooth, and $h \in \langle g \rangle$. Then DLP $\leq_R$ Fixed-CDH for the problem instances output by A.*

Proof: Suppose one has a perfect Fixed-CDH oracle. Putting $l = O(\log(r)^2)$ into Theorem 21.4.6 gives a reduction with $O(\log(r)\log\log(r))$ oracle queries and $O(\log(r)^3)$ group and field operations. □

The same results trivially hold if one has a perfect CDH oracle.

Exercise 21.4.8.★ Determine the complexity in Theorem 21.4.6 if one has a Fixed-CDH oracle that only succeeds with probability ϵ.

[4] Remark 2.15.9 does not lead to a better bound, since the value n (which is m in the notation of that remark) is not necessarily large.

Cherepnev [135] iterates the den Boer reduction to show that if one has an efficient CDH algorithm for arbitrary groups then one can solve DLP in a given group in subexponential time. This result is of a very different flavour to the other reductions in this chapter (which all use an oracle for a group G to solve a computational problem in the same group G) so we do not discuss it further.

21.4.3 The Maurer Reduction

The den Boer reduction can be seen as solving the DLP in the algebraic group $G_m(\mathbb{F}_r)$, performing all computations using implicit representation. Maurer's idea was to replace $G_m(\mathbb{F}_r)$ by any algebraic group $G(\mathbb{F}_r)$, in particular the group of points on an elliptic curve $E(\mathbb{F}_r)$. As with Lenstra's elliptic curve factoring method, even when $r-1$ is not smooth then there might be an elliptic curve E such that $E(\mathbb{F}_r)$ is smooth.

When one uses a general algebraic group G there are two significant issues that did not arise in the den Boer reduction.

- The computation of the group operation in G may require inversions. This is true for elliptic curve arithmetic using affine coordinates.
- Given $h = g^a$ one must be able to compute an element $P \in G(\mathbb{F}_r)$, in implicit representation, such that once P has been determined in explicit representation one can compute a. For an elliptic curve E one could hope that $P = (a, b) \in E(\mathbb{F}_r)$ for some $b \in \mathbb{F}_r$.

Before giving the main result we address the second of these issues. In other words, we show how to embed a DLP instance into an elliptic curve point.

Lemma 21.4.9. *Let g have prime order r and let $h = g^a$. Let $E : y^2 = x^3 + Ax + B$ be an affine elliptic curve over $\mathbb{F}_r$. Given a perfect Fixed-CDH oracle there is an algorithm that outputs an implicit representation (g^X, g^Y) of a point $(X, Y) \in E(\mathbb{F}_r)$ and some extra data, and makes an expected $O(\log(r))$ oracle queries and performs an expected $O(\log(r))$ group operations in $\langle g \rangle$. Furthermore, given the explicit value of X and the extra data one can compute a.*

Proof: The idea is to choose uniformly at random $0 \leq \alpha < r$ and set $X = a + \alpha$. An implicit representation of X can be computed as $h_1 = hg^\alpha$ using $O(\log(r))$ group operations. If we store α then, given X, we can compute a. Hence, the extra data is α.

Given the implicit representation for X one determines an implicit representation for $\beta = X^3 + AX + B$ using two oracle queries. Given g^β one can compute (here $(\frac{\beta}{r}) \in \{-1, 1\}$ is the Legendre symbol)

$$h_2 = g^{(\frac{\beta}{r})} = g^{\beta^{(r-1)/2}} \tag{21.8}$$

using $O(\log(r))$ oracle queries. If $h_2 = g$ then β is a square and so X is an x-coordinate of a point of $E(\mathbb{F}_r)$.

Since there are at least $(r - 2\sqrt{r})/2$ possible x-coordinates of points in $E(\mathbb{F}_r)$ it follows that if one chooses X uniformly at random in $\mathbb{F}_r$ then the expected number of trials until X is the x-coordinate of a point in $E(\mathbb{F}_r)$ is approximately two.

Once β is a square modulo r then one can compute an implicit representation for $Y = \sqrt{\beta} \pmod r$ using the Tonelli-Shanks algorithm with implicit representations. We use the notation of Algorithm 3. The computation of the non-residue n is expected to require $O(\log(r))$ operations in $\mathbb{F}_r$ and can be done explicitly. The computation of the terms w and b requires $O(\log(r))$ oracle queries, some of which can be avoided by storing intermediate

values from the computation in equation (21.8). The computation of i using a Pohlig-Hellman-style algorithm is done as follows. First compute the sequence $b, b^2, \ldots, b^{2^{e-1}}$ using $O(\log(r))$ oracle queries and the sequence $y, y^2, \ldots, y^{2^{e-1}}$ using $O(\log(r))$ group operations. With a further $O(\log(r))$ group operations one can determine the bits of i. □

Theorem 21.4.10. *Let $B \in \mathbb{N}$. Let $g \in G$ have order r. Let E be an elliptic curve over $\mathbb{F}_r$ such that $E(\mathbb{F}_r)$ is a cyclic group. Suppose that the order of $E(\mathbb{F}_r)$ is known and is B-smooth. Given a perfect Fixed-CDH oracle with respect to g one can solve the DLP in $\langle g \rangle$ using an expected $O(\log(r)^2 \log(\log(r)))$ oracle queries.*[5]

Indeed, there are two variants of the reduction, one using exhaustive search and one using the baby-step-giant-step algorithm. One can also consider the case of a perfect CDH oracle. The following table gives the full expected complexities (where the constant implicit in the $O(\cdot)$ is independent of B). We use the abbreviation $l(x) = \log(x)$, so that $l(l(r)) = \log(\log(r))$.

Oracle	*Reduction*	*Oracle queries*	*Group operations*	*$\mathbb{F}_r$ operations*
Fixed-CDH	*PH only*	$O(l(r)^2 l(l(r)))$	$O(Bl(r)^2/l(B))$	$O(Bl(r)^2/l(B))$
Fixed-CDH	*PH+BSGS*	$O(\sqrt{B}l(r)^2/l(B) + l(r)^2 l(l(r)))$	$O(\sqrt{B}l(r)^2/l(B))$	$O(\sqrt{B}l(r)^2/l(B))$
CDH	*PH only*	$O(l(r)l(l(r)))$	$O(Bl(r)^2/l(B))$	$O(Bl(r)^2/l(B))$
CDH	*PH+BSGS*	$O(\sqrt{B}l(r)/l(B) + l(r)l(l(r)))$	$O(\sqrt{B}l(r)^2/l(B))$	$O(\sqrt{B}l(r)^2/l(B))$

Proof: Let the discrete logarithm instance be $(g, h = g^a)$. Write $N = \#E(\mathbb{F}_r) = \prod_{i=1}^{k} l_i^{e_i}$. We assume that affine coordinates are used for arithmetic in $E(\mathbb{F}_r)$. Let P be a generator of $E(\mathbb{F}_r)$.

The reduction is conceptually the same as the den Boer reduction. One difference is that elliptic curve arithmetic requires inversions (which are performed using the method of Lemma 21.1.13 and Lemma 21.1.15), hence the number of Fixed-CDH oracle queries must increase. A sketch of the reduction in the case of exhaustive search is given in Algorithm 27.

The first step is to use Lemma 21.4.9 to associate with h the implicit representations of a point $Q \in E(\mathbb{F}_r)$. This requires an expected $O(\log(r))$ oracle queries and $O(\log(r))$ group operations for all four variants. Then $Q \in \langle P \rangle$ where P is the generator of the cyclic group $E(\mathbb{F}_r)$.

The idea is again to use Pohlig-Hellman (PH) and baby-step-giant-step (BSGS) to solve the discrete logarithm of Q with respect to P in $E(\mathbb{F}_r)$. If we can compute an integer u such that $Q = [u]P$ (with computations done in implicit representation) then computing $[u]P$ and using Lemma 21.4.9 gives the value a explicitly.

First we consider the PH algorithm. As with the den Boer reduction, one needs to compute explicit representations (i.e., standard affine coordinates) for $[N/l_i^{e_i}]P$ and implicit representations for $[N/l_i^{e_i}]Q$. It is possible that $[N/l_i^{e_i}]Q = \mathcal{O}_E$ so this case must be handled. As in Section 2.15.1, computing these points requires $O(\log(r)\log\log(r))$ elliptic curve operations. Hence, for the multiples of P we need $O(\log(r)\log\log(r))$ operations in $\mathbb{F}_r$ while for the multiples of Q we need $O(\log(r)^2 \log\log(r))$ Fixed-CDH oracle queries and $O(\log(r)\log\log(r))$ group operations. (If a CDH oracle is available then this stage only requires $O(\log(r)\log\log(r))$ oracle queries, as an inversion in implicit representation can be done with a single CDH oracle query.) Computing the points $[N/l_i^f]P$ for $1 \leq f < e_i$ and all i requires at most a further $2\sum_{i=1}^{k} e_i \log_2(l_i) = 2\log_2(N) = O(\log(r))$ group operations. Similarly, computing the implicit representations of the remaining $[N/l_i^f]Q$ requires $O(\log(r)^2)$ Fixed-CDH oracle queries and $O(\log(r))$ group operations.

[5] This is improved to $O(\log(r)\log\log(r))$ in Remark 21.4.11.

The computation of $u_i P_0$ in line 8 of Algorithm 27 requires $O(\log(r))$ operations in $\mathbb{F}_r$ followed by $O(1)$ operations in G and oracle queries.

The exhaustive search algorithm for the solution to the DLP in a subgroup of prime order l_i is given in lines 9 to 16 of Algorithm 27. The point P_0 in line 8 has already been computed, and computing Q_0 requries only one elliptic curve addition (i.e., $O(\log(r))$ Fixed-CDH oracle queries). The while loop in line 12 runs for $\leq B$ iterations, each iteration involves a constant number of field operations to compute $T + P_0$ followed by two exponentiations in the group to compute g^{x_T} and g^{y_T} (an obvious improvement is to use g^{x_T} only). The complexity of lines 9 to 16 is therefore $O(B \log(r))$ group operations, and $O(B)$ field operations.

If one uses BSGS the results are similar. Suppose Q and P are points of order l, where P is known explicitly while we only have an implicit representation (g^{x_Q}, g^{y_Q}) for Q. Let $m = \lceil \sqrt{l} \rceil$ and $P_1 = [m]P$ so that $Q = [u_0]P + [u_1]P_1$ for $0 \leq u_0, u_1 < m$. One computes a list of baby steps $[u_0]P$ in implicit representation using $O(\sqrt{B})$ field operations and $O(\sqrt{B}\log(r))$ group operations as above. For the giant steps $Q - [u_1]P_1$ one is required to perform elliptic curve arithmetic with the implicit point Q and the explicit point $[u_1]P_1$, which requires an inversion of an implicit element. Hence the giant steps require $O(\sqrt{B})$ field operations, $O(\sqrt{B}\log(r))$ group operations and $O(\sqrt{B}\log(r))$ Fixed-CDH oracle queries.

Since $\sum_{i=1}^{k} e_i \leq \log_2(N)$ the exhaustive search or BSGS subroutine is performed $O(\log(r))$ times. A more careful analysis using Exercise 13.2.7 means the complexity is multiplied by $\log(r)/\log(B)$. The Chinese remainder theorem and later stages are negligible. The result follows. □

Algorithm 27 Maurer reduction

INPUT: $g, h = g^a$, $E(\mathbb{F}_r)$
OUTPUT: a

1: Associate to h an implicit representation for a point $Q = (X, Y) \in E(\mathbb{F}_r)$ using Lemma 21.4.9
2: Compute a point $P \in E(\mathbb{F}_r)$ that generates $E(\mathbb{F}_r)$. Let $N = \#E(\mathbb{F}_r) = \prod_{i=1}^{k} l_i^{e_i}$
3: Compute explicit representations of $\{[N/l_i^j]P : 1 \leq i \leq k, 1 \leq j \leq e_i\}$
4: Compute implicit representations of $\{[N/l_i^j]Q : 1 \leq i \leq k, 1 \leq j \leq e_i\}$
5: **for** $i = 1$ to k **do**
6: $\quad u_i = 0$
7: $\quad$ **for** $j = 1$ to e_i **do** ▷ Reducing DLP of order $l_i^{e_i}$ to cyclic groups
8: $\quad\quad$ Let $P_0 = [N/l_i^j]P$ and $Q_0 = [N/l_i^j]Q - u_i P_0$
9: $\quad\quad$ **if** $Q_0 \neq \mathcal{O}_E$ **then**
10: $\quad\quad\quad$ Let $(h_{0,x}, h_{0,y})$ be the implicit representation of Q_0
11: $\quad\quad\quad$ $P_0 = [N/l_i]P_0$, $n = 1$, $T = P_0 = (x_T, y_T)$
12: $\quad\quad\quad$ **while** $h_{0,x} \neq g^{x_T}$ or $h_{0,y} \neq g^{y_T}$ **do** ▷ Exhaustive search
13: $\quad\quad\quad\quad$ $n = n + 1$, $T = T + P_0$
14: $\quad\quad\quad$ **end while**
15: $\quad\quad\quad$ $u_i = u_i + n l^{j-1}$
16: $\quad\quad$ **end if**
17: $\quad$ **end for**
18: **end for**
19: Use Chinese remainder theorem to compute $u \equiv u_i \pmod{l_i^{e_i}}$ for $1 \leq i \leq k$
20: Compute $(X, Y) = [u]P$ and hence compute a
21: **return** a

Remark 21.4.11. We have seen that reductions involving a Fixed-CDH oracle are less efficient (i.e., require more oracle queries) than reductions using a CDH oracle. A solution[6] to this is to work with projective coordinates for elliptic curves. Line 12 of Algorithm 27 tests whether the point Q_0 given in implicit representation is equal to the point (x_T, y_T) given in affine representation. When $Q_0 = (x_0 : y_0 : z_0)$ then the test $h_{0,x} = g^{x_T}$ in line 12 is replaced with the comparison

$$g^{x_0} = (g^{z_0})^{x_T} .$$

Hence the number of oracle queries in the first line of the table in Theorem 21.4.10 can be reduced to $O(\log(r) \log\log(r))$. As mentioned in Remark 13.3.2, one cannot use the BSGS algorithm with projective coordinates, as the non-uniqueness of the representation means one can't efficiently detect a match between two lists.

Exercise 21.4.12. ★ Generalise the Maurer algorithm to the case where the group of points on the elliptic curve is not necessarily cyclic. Determine the complexity if l_1 is the largest prime for which $E(\mathbb{F}_r)[l_1]$ is not cyclic and l_2 is the largest prime dividing $\#E(\mathbb{F}_r)$ for which $E(\mathbb{F}_r)[l_2]$ is cyclic.

Exercise 21.4.13. If $r+1$ is smooth then one can use the algebraic group $G_{2,r} \cong \mathbb{T}_2(\mathbb{F}_r)$ (see Section 6.3) instead of $G_m(\mathbb{F}_r)$ or $E(\mathbb{F}_r)$. There are two approaches: the first is to use the usual representation $\{a + b\theta \in \mathbb{F}_{r^2} : \mathrm{N}_{\mathbb{F}_{r^2}/\mathbb{F}_r}(a + b\theta) = 1\}$ for $G_{2,r}$ and the second is to use the representation $\mathbb{A}^1(\mathbb{F}_r)$ for $\mathbb{T}_2(\mathbb{F}_r) - \{1\}$ corresponding to the map decomp_2 from Definition 6.3.7. Determine the number of (perfect) oracle queries in the reductions from Fixed-CDH to DLP for these two representations. Which is better? Repeat the exercise when one has a CDH oracle.

Corollary 21.4.14. *Let $c \in \mathbb{R}_{>1}$. Let (G_n, g_n, r_n) be a family of groups for $n \in \mathbb{N}$ where $g_n \in G_n$ has order r_n and r_n is an n-bit prime. Suppose we are given **auxiliary elliptic curves** (E_n, N_n) for the family, where E_n is an elliptic curve over $\mathbb{F}_{r_n}$ such that $\#E_n(\mathbb{F}_{r_n}) = N_n$ and N_n is $O(\log(r_n)^c)$-smooth. Then the DLP in $\langle g_n \rangle$ is equivalent to the Fixed-CDH problem in $\langle g_n \rangle$.*

Exercise 21.4.15. Prove Corollary 21.4.14.

We now state the conjecture of Maurer and Wolf that all Hasse intervals contain a polynomially smooth integer. Define $\nu(r)$ to be the minimum, over all integers $n \in [r + 1 - 2\sqrt{r}, r + 1 + 2\sqrt{r}]$, of the largest prime divisor of n. Conjecture 1 of [407] states that

$$\nu(r) = \log(r)^{O(1)}. \tag{21.9}$$

See Remark 15.3.5 for discussion of this. Muzereau, Smart and Vercauteren [448] note that if r is a pseudo-Mersenne prime (as is often used in elliptic curve cryptography) then the Hasse interval usually contains a power of 2. Similarly, as noted by Maurer and Wolf in [405], one can first choose a random smooth integer n and then search for a prime r close to n and work with a group G of order r.

Exercise 21.4.16. ★ Show how to use the algorithm of Section 19.4.4 to construct a smooth integer in the Hasse interval. Construct a 2^{40}-smooth integer (not equal to 2^{255}) close to $p = 2^{255} - 19$ using this method.

[6] This idea is briefly mentioned in Section 3 of [402], but was explored in detail by Bentahar [42].

Remark 21.4.17. There are two possible interpretations of Corollary 21.4.14. The first interpretation is: if there exists an efficient algorithm for CDH or Fixed-CDH in a group $G = \langle g \rangle$ of prime order r and if there exists an auxiliary elliptic curve over $\mathbb{F}_r$ with sufficiently smooth order then there exists an efficient algorithm to solve the DLP in G. Maurer and Wolf [408] (also see Section 3.5 of [409]) claim this gives a non-uniform reduction from DLP to CDH, however the validity of this claim depends on the DLP instance generator.[7]

In other words, if one believes that there does not exist a non-uniform polynomial-time algorithm for DLP in G (for certain instance generators) and if one believes the conjecture that the Hasse interval around r contains a polynomially smooth integer, then one must believe there is no polynomial-time algorithm for CDH or Fixed-CDH in G. Hence, one can use the results to justify the assumption that CDH is hard. We stress that this is purely a statement of existence of algorithms; it is independent of the issue of whether or not it is feasible to write the algorithms down.

A second interpretation is that CDH might be easy and that this reduction yields the best algorithm for solving the DLP. If this were the case (or if one wants a uniform reduction) then, in order to solve a DLP instance, the issue of how to implement the DLP algorithm becomes important. The problem is that there is no known polynomial-time algorithm to construct auxiliary elliptic curves $E(\mathbb{F}_r)$ of smooth order. An algorithm to construct smooth curves (based on the CM method) is given in Section 4 of [405] but it has exponential complexity. Hence, if one can write down an efficient algorithm for CDH then the above ideas alone do not allow one to write down an efficient algorithm for DLP.

Boneh and Lipton [83] handle the issue of auxiliary elliptic curves by giving a subexponential-time reduction between Fixed-CDH and DLP. They make the natural assumption (essentially Conjecture 15.3.1; as used to show that the elliptic curve factoring method is subexponential-time) that, for sufficiently large primes, the probability that a randomly chosen integer in the Hasse interval $[r + 1 - 2\sqrt{r}, r + 1 + 2\sqrt{r}]$ is $L_r(1/2, c)$-smooth is $1/L_r(1/2, c')$ for some constants $c, c' > 0$ (see Section 15.3 for further discussion of these issues). By randomly choosing $L_r(1/2, c')$ elliptic curves over $\mathbb{F}_r$ one therefore expects to find one that has $L_r(1/2, c)$-smooth order. One can then perform Algorithm 27 to solve an instance of the DLP in subexponential-time and using polynomially many oracle queries. We refer to [83] for the details.

Maurer and Wolf extend the Boneh-Lipton idea to genus 2 curves and use results of Lenstra, Pila and Pomerance (Theorem 1.3 of [380]) to obtain a reduction with proven complexity $L_r(2/3, c)$ for some constant c (see Section 3.6 of [409]). This is the only reduction from DLP to CDH that does not rely on any conjectures or heuristics. Unfortunately it is currently impractical to construct suitable genus 2 curves in practice (despite being theoretically polynomial-time).

Muzereau, Smart and Vercauteren [448] go even further than Boneh and Lipton. They allow an exponential-time reduction, with the aim of minimising the number of CDH or Fixed-CDH oracle queries. The motivation for this approach is to give tight reductions between CDH and DLP (i.e., to give a lower bound on the running time for an algorithm

[7] An instance generator for the DLP (see Example 2.1.9) outputs a quadruple (G, r, g, h) where G is a description of a group, $g \in G$ has order r, $h \in \langle g \rangle$ and r is prime. The size of the instance depends on the representation of G and g, but is at least $2 \log_2(r)$ bits since one must represent r and h. If one considers the DLP with respect to an instance generator for which r is constant over all instances of a given size n, then a single auxiliary curve is needed for all DLP instances of size n and so Corollary 21.4.14 gives a non-uniform reduction. On the other hand, if there are superpolynomially many r among the outputs of size n of the instance generator (this would be conjecturally true for the instance generator of Example 2.1.9) then the amount of auxiliary data is not polynomially bounded and hence the reduction is not non-uniform.

for CDH in terms of conjectured lower bounds for the running time of an algorithm for DLP). Their results were improved by Bentahar [42, 43]. It turns out to be desirable to have an auxiliary elliptic curve such that $\#E(\mathbb{F}_r)$ is a product of three coprime integers of roughly equal size $r^{1/3}$. The reduction then requires $O(\log(r))$ oracle queries but $O(r^{1/3}\log(r))$ field operations. Islam [306] has proved that such an elliptic curve exists for each prime r. One can construct auxiliary curves by choosing random curves, counting points and factoring; one expects only polynomially many trials, but the factoring computation is subexponential. We refer to [448, 42, 43] for further details.

Exercise 21.4.18. Write down the algorithm for the Muzereau-Smart-Vercauteren reduction using projective coordinates. Prove that the algorithm has the claimed complexity.

Exercise 21.4.19. Show how to generate in heuristic expected polynomial-time primes $r, p \equiv 2 \pmod 3$ such that $r \mid (p+1)$, $r+1$ is κ-smooth, and $2^{\kappa-1} \leq r < p \leq 2^{\kappa+3}$. Hence, by Exercise 9.10.4, taking $E : y^2 = x^3 + 1$ then $E(\mathbb{F}_p)$ is a group of order divisible by r and $E(\mathbb{F}_r)$ has κ-smooth order and is a suitable auxiliary elliptic curve for the Maurer reduction.

Finally, we remark that the den Boer and Maurer reductions cannot be applied to relate CDH and DLP in groups of unknown order. For example, let N be composite and $g \in (\mathbb{Z}/N\mathbb{Z})^*$ of unknown order M. Given a perfect Fixed-CDH oracle with respect to g one can still compute with the algebraic group $G_m(\mathbb{Z}/M\mathbb{Z})$ in implicit representation (or projective equations for $E(\mathbb{Z}/M\mathbb{Z})$), but if M is not known then the order of $G = G_m(\mathbb{Z}/M\mathbb{Z})$ (respectively, $G = E(\mathbb{Z}/M\mathbb{Z})$) is also not known and so one cannot perform the Pohlig-Hellman algorithm in G. Later we will mention how a CDH oracle in $(\mathbb{Z}/N\mathbb{Z})^*$ can be used to factor N (see Exercise 24.2.23) and hence avoid this problem in that group.

21.5 Algorithms for Static Diffie-Hellman

Brown and Gallant [111] studied the relationship between Static-DH and DLP. Their main result is an algorithm to solve an instance of the DLP using a perfect Static-DH oracle. Cheon [131] independently discovered this algorithm in a different context, showing that a variant of the DLP (namely, the problem of computing a given g, g^a and g^{a^d}; we call this **Cheon's variant of the DLP**) can be significantly easier than the DLP. We now present the algorithm of Brown-Gallant and Cheon, and discuss some of its applications.

Theorem 21.5.1. *Let g have prime order r and let $d \mid (r-1)$. Given $h_1 = g^a$ and $h_d = g^{a^d}$ then one can compute a in $O((\sqrt{(r-1)/d} + \sqrt{d})\log(r))$ group operations, $O(\sqrt{(r-1)/d} + \sqrt{d})$ group elements of storage and $O(\sqrt{(r-1)/d} + \sqrt{d})$ multiplications in $\mathbb{F}_r$.*[8]

Proof: First, the case $a \equiv 0 \pmod r$ is easy, so we assume $a \not\equiv 0 \pmod r$. The idea is essentially the same as the den Boer reduction. Let γ be a primitive root modulo r. Then $a = \gamma^u \pmod r$ for some $0 \leq u < r-1$ and it suffices to compute u. The den Boer reduction works by projecting the unknown a into prime order subgroups of $\mathbb{F}_r^*$ using a Diffie-Hellman oracle. In our setting, we already have an implicit representation of the projection a^d into the subgroup of $\mathbb{F}_r^*$ of order $(r-1)/d$.

[8] As usual, we are being careless with the $O(\cdot)$-notation. What we mean is that there is a constant c independent of r, d, g and a such that the algorithm requires $\leq c(\sqrt{(r-1)/d}+\sqrt{d})\log(r)$ group operations.

The first step is to solve $h_d = g^{a^d} = g^{\gamma^{du}}$ for some $0 \leq u \leq (r-1)/d$. Let $m = \lceil \sqrt{(r-1)/d} \rceil$ and write $u = u_0 + mu_1$ with $0 \leq u_0, u_1 < m$. This is exactly the setting of equations (21.6) and (21.7) and hence one can compute (u_0, u_1) using a baby-step-giant-step algorithm. This requires $\leq m$ multiplications in $\mathbb{F}_r$ and $\leq 2m$ exponentiations in the group. Thus the total complexity is $O(\sqrt{(r-1)/d}\log(r))$ group operations and $O(\sqrt{(r-1)/d})$ field operations.

We now have $a^d = \gamma^{du}$ and so $a = \gamma^{u+v(r-1)/d}$ for some $0 \leq v < d$. It remains to compute v. Let

$$h = h_1^{\gamma^{-u}} = g^{a\gamma^{-u}} = g^{\gamma^{v(r-1)/d}}.$$

Set $m = \lceil \sqrt{d} \rceil$ and write $v = v_0 + mv_1$ where $0 \leq v_0, v_1 < m$. Using the same ideas as above (since γ is known explicitly the powers are computed efficiently) one can compute (v_0, v_1) using a baby-step-giant-step algorithm in $O(\sqrt{d}\log(r))$ group operations. Finally, we compute $a = \gamma^{u+v(r-1)/d} \pmod r$. □

Kozaki, Kutsuma and Matsuo [353] show how to reduce the complexity in the above result to $O(\sqrt{(r-1)/d} + \sqrt{d})$ group operations by using precomputation to speed up the exponentiations to constant time. Note that this trick requires exponential storage and is not applicable when low-storage discrete logarithm algorithms are used (as in Exercise 21.5.5).

The first observation is that if $r-1$ has a suitable factorisation then Cheon's variant of the DLP can be much easier than the DLP.

Corollary 21.5.2. *Let g have prime order r and suppose $r-1$ has a factor d such that $d \approx r^{1/2}$. Given $h_1 = g^a$ and $h_d = g^{a^d}$ then one can compute a in $O(r^{1/4}\log(r))$ group operations.*

Corollary 21.5.3. *Let g have prime order r and suppose $r - 1 = \prod_{i=1}^n d_i$ where the d_i are coprime. Given $h_1 = g^a$ and $h_{d_i} = g^{a^{d_i}}$ for $1 \leq i \leq n$ then one can compute a in $O((\sum_{i=1}^n \sqrt{d_i})\log(r))$ group operations.*

Exercise 21.5.4. Prove Corollaries 21.5.2 and 21.5.3.

As noted in [111] and [131] one can replace the baby-step-giant-step algorithms by Pollard methods. Brown and Gallant[9] suggest a variant of the Pollard rho method, but with several non-standard features: one needs to find the precise location of the collision (i.e., steps $x_i \neq x_j$ in the walk such that $x_{i+1} = x_{j+1}$) and there is only a (heuristic) 0.5 probability that a collision leads to a solution of the DLP. Cheon [131] suggests using the Kangaroo method, which is a more natural choice for this application.

Exercise 21.5.5. Design a pseudorandom walk for the Pollard kangaroo method to solve the DLP in implicit representation arising in the proof of Theorem 21.5.1.

Brown and Gallant use Theorem 21.5.1 to obtain the following result.

Theorem 21.5.6. *Let g have prime order r and let $d \mid (r-1)$. Let $h = g^a$ and suppose A is a perfect oracle for the static Diffie-Hellman problem with respect to (g, h) (i.e., $A(h_1) = h_1^a$). Then one can compute a using d oracle queries, $O((\sqrt{(r-1)/d} + \sqrt{d})\log(r))$ group operations and $O((\sqrt{(r-1)/d} + \sqrt{d})\log(r))$ multiplications in $\mathbb{F}_r$.*

Proof: Write $h_1 = h = g^a$ and compute the sequence $h_{i+1} = O(h_i) = g^{a^i}$ until g^{a^d} is computed. Then apply Theorem 21.5.1. □

[9] See Appendix B.2 of the first version of [111]. This does not appear in the June 2005 version.

Note that the reduction uses a Static-DH oracle with respect to g^a to compute a. The reduction does not solve a general instance of the DLP using a specific Static-DH oracle, hence it is not a reduction from DLP to Static-DH. Also recall that Exercise 20.4.6 showed how one can potentially compute a efficiently given access to a Static-DH oracle (with respect to a) that does not check that the inputs are group elements of the correct order. Hence, the Brown-Gallant result is primarily interesting in the case where the Static-DH oracle does perform these checks.

Corollary 21.5.7. *Let g have prime order r and suppose $r-1$ has a factor d such that $d \approx r^{1/3}$. Given $h = g^a$ and a perfect Static-DH oracle with respect to (g, h) then one can compute a in $O(r^{1/3})$ oracle queries and $O(r^{1/3}\log(r))$ group operations.*

Exercise 21.5.8. Prove Corollary 21.5.7.

Brown and Gallant use Theorem 21.5.6 to give a lower bound on the difficulty of Static-DH under the assumption that the DLP is hard.

Exercise 21.5.9. Let g have order r. Assume that the best algorithm to compute a, given $h = g^a$, requires $\sqrt{r}$ group operations. Suppose that $r-1$ has a factor $d = c_1\log(r)^2$ for some constant c_1. Prove that the best algorithm to solve Static-DH with respect to (g, h) requires at least $c_2\sqrt{r}/\log(r)^2$ group operations for some constant c_2.

All the above results are predicated on the existence of a suitable factor d of $r-1$. Of course, $r-1$ may not have a factor of the correct size; for example if $r-1 = 2l$ where l is prime then we have shown that given (g, g^a, g^{a^2}) one can compute a in $O(\sqrt{r/2}\log(r))$ group operations, which is no better than general methods for the DLP. To increase the applicability of these ideas, Cheon also gives a method for when there is a suitable factor d of $r+1$. The method in this case is not as efficient as the $r-1$ case, and requires more auxiliary data.

Theorem 21.5.10. *Let g have prime order r and let $d \mid (r+1)$. Given $h_i = g^{a^i}$ for $1 \leq i \leq 2d$ then one can compute a in $O((\sqrt{(r+1)/d} + d)\log(r))$ group operations, $O(\sqrt{(r+1)/d} + \sqrt{d})$ group elements storage and $O((\sqrt{(r+1)/d} + \sqrt{d})\log(r))$ multiplications in $\mathbb{F}_r$.*

Proof: As in Exercise 21.4.13 the idea is to work in the algebraic group $G_{2,r}$, which has order $r+1$. Write $\mathbb{F}_{r^2} = \mathbb{F}_r(\theta)$ where $\theta^2 = t \in \mathbb{F}_r$. By Lemma 6.3.10 each element $\alpha \in G_{2,r} - \{1\} \subseteq \mathbb{F}_{r^2}^*$ is of the form $\alpha_0 + \alpha_1\theta$ where

$$\alpha_0 = \frac{a^2 - t}{a^2 + t}, \qquad \alpha_1 = \frac{2a}{a^2 + t}$$

for some $a \in \mathbb{F}_r$. For each $d \in \mathbb{N}$ there exist polynomials $f_{d,0}(x), f_{d,1}(x) \in \mathbb{F}_r[x]$ of degree $2d$ such that, for α as above, one has

$$\alpha^d = \frac{f_{d,0}(a) + \theta f_{d,1}(a)}{(a^2 + t)^d}.$$

The idea is to encode the DLP instance g^a into the element $\beta \in G_{2,r}$ as

$$\beta = \frac{a^2 - t}{a^2 + t} + \theta\frac{2a}{a^2 + t}.$$

We do not know β, but we can compute $(a^2 - t)$, $(a^2 + t)$ and $2a$ in implicit representation.

Let γ be a generator for $G_{2,r}$, known explicitly. Then $\beta = \gamma^u$ for some $0 \leq u < r+1$. It suffices to compute u.

The first step is to project into the subgroup of order $(r+1)/d$. We have $\beta^d = \gamma^{du}$ for some $0 \leq u < (r+1)/d$. Let $m = \lceil \sqrt{(r+1)/d} \rceil$ so that $u = u_0 + mu_1$ for $0 \leq u_0, u_1 < m$. Write $\gamma^i = \gamma_{i,0} + \theta\gamma_{i,1}$. Then $\beta^d\gamma^{-u_0} = \gamma^{du_1}$ and so $(f_{d,0}(a)+\theta f_{d,1}(a))(\gamma_{-u_0,0}+\theta\gamma_{-u_0,1}) = (a^2+t)^d(\gamma_{du_1,0} + \theta\gamma_{du_1,1})$. Hence

$$\left(g^{f_{d,0}(a)}\right)^{\gamma_{-u_0,0}} \left(g^{f_{d,1}(a)}\right)^{\gamma_{-u_0,1}} = \left(g^{(a^2+t)^d}\right)^{\gamma_{du_1,0}}$$

and similarly for the implicit representation of the coefficient of θ. It follows that one can perform the baby-step-giant-step algorithm in this setting to compute (u_0, u_1) and hence $u \pmod{(r+1)/d}$. Note that computing $g^{f_{d,0}(a)}, g^{f_{d,1}(a)}$ and $g^{(a^2+t)^d}$ requires $6d$ exponentiations. The stated complexity follows.

For the second stage, we have $\beta = \gamma^{u+v(r+1)/d}$ where $0 \leq v < d$. Giving a baby-step-giant-step algorithm here is straightforward and we leave the details as an exercise. □

One derives the following result. Note that it is not usually practical to consider a computational problem whose input is a $O(r^{1/3})$-tuple of group elements, hence this result is mainly of theoretical interest.

Corollary 21.5.11. *Let g have prime order r and suppose $r+1$ has a factor d such that $d \approx r^{1/3}$. Given $h_i = g^{a^i}$ for $1 \leq i \leq 2d$ then one can compute a in $O(r^{1/3}\log(r))$ group operations.*

Corollary 21.5.12. *Let g have prime order r and suppose $r+1$ has a factor d such that $d \approx r^{1/3}$. Given $h = g^a$ and a perfect Static-DH oracle with respect to (g, h) then one can compute a in $O(r^{1/3})$ oracle queries and $O(r^{1/3}\log(r))$ group operations.*

Exercise 21.5.13. Fill in the missing details in the proof of Theorem 21.5.10 and prove Corollaries 21.5.11 and 21.5.12.

Satoh [511] extends Cheon's algorithm to algebraic groups of order $\varphi_n(r)$ (essentially, to the groups $G_{n,r}$). He also improves Theorem 21.5.10 in the case of $d \mid (r+1)$ to only require $h_i = g^{a^i}$ for $1 \leq i \leq d$.

A natural problem is to generalise Theorem 21.5.10 to other algebraic groups, such as elliptic curves. The obvious approach does not seem to work (see Remark 1 of [131]), so it seems a new idea is needed to achieve this. Finally, Section 5.2 of [132] shows that, at least asymptotically, most primes r are such that $r-1$ or $r+1$ has a useful divisor.

Both [111] and [131] remark that a decryption oracle for classic textbook Elgamal leads to an Static-DH oracle: Given an Elgamal public key (g, g^a) and any $h_1 \in \langle g \rangle$ one can ask for the decryption of the ciphertext $(c_1, c_2) = (h_1, 1)$ (one can also make this less obvious using random self-reducibility of Elgamal ciphertexts) to get $c_2c_1^{-a} = h_1^{-a}$. From this one computes h_1^a. By performing this repeatedly one can compute a sequence $h_i = g^{a^i}$ as required. The papers [111, 131] contain further examples of cryptosystems that provide Static-DH oracles, or computational assumptions that contain values of the form $h_i = g^{a^i}$.

21.6 Hard Bits of Discrete Logarithms

Saying that a computational problem is hard is the same as saying that it is hard to write down a binary representation of the answer. Some bits of a representation of the

answer may be easy to compute (at least, up to a small probability of error) but if a computational problem is hard then there must be at least one bit of any representation of the answer that is hard to compute. In some cryptographic applications (such as key derivation or designing secure pseudorandom generators) it is important to be able to locate some of these "hard bits". Hence, the main challenge is to prove that a specific bit is hard. A potentially easier problem is to determine a small set of bits, at least one of which is hard. A harder problem is to prove that some set of bits are all simultaneously hard (for this concept see Definition 21.6.14).

The aim of this section is to give a rigorous definition for the concept of "hard bits" and to give some easy examples (hard bits of the solution to the DLP). In Section 21.7 we will consider related problems for the CDH problem. We first show that certain individual bits of the DLP, for any group, are as hard to compute as the whole solution.

Definition 21.6.1. Let $g \in G$ have prime order r. The computational problem **DL-LSB** is: given (g, g^a) where $0 \leq a < r$ to compute the least significant bit of a.

Exercise 21.6.2. Show that DL-LSB $\leq_R$ DLP.

Theorem 21.6.3. *Let G be a group of prime order r. Then DLP $\leq_R$ DL-LSB.*

Proof: Let A be a perfect oracle that, on input (g, g^a) outputs the least significant bit of $0 \leq a < r$. In other words, if the binary expansion of a is $\sum_{i=0}^{m} a_i 2^i$ then A outputs a_0. We will use A to compute a.

The first step is to call $A(g, h)$ to get a_0. Once this has been obtained we set $h' = hg^{-a_0}$. Then $h' = g^{2a_1+4a_2+\cdots}$. Let $u = 2^{-1} = (r+1)/2 \pmod r$ and define

$$h_1 = (h')^u.$$

Then $h_1 = g^{a_1+2a_2+\cdots}$ so calling $A(g, h_1)$ gives a_1. For $i = 2, 3, \ldots$ compute $h_i = (h_{i-1}g^{-a_{i-1}})^u$ and $a_i = A(g, h_i)$, which computes the binary expansion of a. This reduction runs in polynomial-time and requires polynomially many calls to the oracle A. □

Exercise 21.6.4. Give an alternative proof of Theorem 21.6.3 based on bounding the unknown a in the range

$$(l-1)r/2^j \leq a < lr/2^j.$$

Initially one sets $l = 1$ and $j = 0$. At step j, if one has $(l-1)r/2^j \leq a < lr/2^j$ and if a is even then $(l-1)r/2^{j+1} \leq a/2 < lr/2^{j+1}$ and if a is odd then $(2^j + l - 1)r/2^{j+1} \leq (a+r)/2 < (2^j + l)r/2^{j+1}$. Show that when $j = \lceil \log_2(r) \rceil$ one can compute $2^{-j}a \pmod r$ exactly and hence deduce a.

Exercise 21.6.5. Since one can correctly guess the least significant bit of the DLP with probability $1/2$, why does Theorem 21.6.3 not prove that DLP is easy?

One should also consider the case of a DL-LSB oracle that only works with some noticeable probability ϵ. It is then necessary to randomise the calls to the oracle, but the problem is to determine the LSB of a given the LSBs of some algebraically related values. The trick is to guess some $u = O(\log(1/\epsilon)) = O(\log(\log(r)))$ most significant bits of a and set them to zero (i.e., replace h by $h' = g^{a'}$ where the u most significant bits of a' are zero). One can then call the oracle on $h'g^y$ for random $0 \leq y \leq r - r/2^u$ and take a majority vote to get the result. For details of the argument see Blum and Micali [73].

We conclude that computing the LSB of the DLP is as hard as computing the whole DLP. Such bits are called **hardcore bits** since if DLP is hard then computing the LSB of the DLP is hard.

Definition 21.6.6. Let $f : \{0,1\}^* \to \{0,1\}^*$ be a function computable in polynomial-time (i.e., there is some polynomial $p(n)$ such that for $x \in \{0,1\}^n$ one can compute $f(x)$ in at most $p(n)$ bit operations). A function $b : \{0,1\}^* \to \{0,1\}$ is a **hardcore bit** or **hardcore predicate** for f if, for all probabilistic polynomial-time algorithms A, the **advantage**

$$\mathrm{Adv}_{x \in \{0,1\}^n}\big(A(f(x)) = b(x)\big)$$

is negligible as a function of n.

We now give some candidate hardcore predicates for the DLP. We also restate the meaning of hardcore bit for functions defined on $\{0,1,\ldots,r-1\}$ rather than $\{0,1\}^*$.

Definition 21.6.7. For all $n \in \mathbb{N}$ let (G_n, g_n, r_n) be such that G_n is a group and $g_n \in G_n$ is an element of order r_n where r_n is an n-bit prime. We call this a **family of groups**. For $n \in \mathbb{N}$ define the function $f_n : \{0,1,\ldots,r_n-1\} \to G_n$ by $f_n(a) = g_n^a$. For $n \in \mathbb{N}$ define $i(n) \in \{0,1,\ldots,n-1\}$. The predicate $b_{i(n)} : \{0,1,\ldots,r_n-1\} \to \{0,1\}$ is defined so that $b_{i(n)}(a)$ is bit $i(n)$ of a, when a is represented as an n-bit string. Then $b_{i(n)}$ is a **hardcore predicate for the DLP** (alternatively, bit $i(n)$ is a **hardcore bit for the DLP**) if, for all probabilistic polynomial-time algorithms A, the advantage

$$\mathrm{Adv}_{a \in \{0,1,\ldots,r_n-1\}}\big(A(f_n(a)) = b_{i(n)}(a)\big)$$

is negligible as a function of n.

The least significant bit (LSB) is the case $i(n) = 0$ in the above definition. If the DLP is hard then Theorem 21.6.3 shows that the LSB is a hardcore bit.

Example 21.6.8. Fix $m \in \mathbb{N}$. Let g have prime order $r > 2^m$. Suppose A is a perfect oracle such that, for $x \in \{0,1,\ldots,r-1\}$, $A(g^x)$ is the predicate $b_m(x)$ (i.e., bit m of x). One can use A to solve the DLP by guessing the $m-1$ LSBs of x and then using essentially the same argument as Theorem 21.6.3. Hence, if m is fixed and g varies in a family of groups as in Example 21.6.7 then $b_m(x)$ is a hardcore predicate for the DLP. A similar result holds if m is allowed to grow, but is bounded as $m = O(\log(\log(r)))$.

We now give an example of a hardcore predicate that is not just a bit of the DLP.

Exercise 21.6.9. Let g have prime order r. Let $f : \{0,1,\ldots,r-1\} \to G$ be $f(x) = g^x$. Define the predicate $b : \{0,1,\ldots,r-1\} \to \{0,1\}$ by $b(x) = x_1 \oplus x_0$ where x_0 and x_1 are the two least significant bits of x. Show that b is a hardcore predicate for f.

It is not true that any bit of the DLP is necessarily hardcore. For example, one can consider the most significant bit of a, which is $b_{n-1}(x)$ in Definition 21.6.7.

Example 21.6.10. Let $r = 2^l + u$ be a prime where $0 < u < 2^{l-\kappa}$. Let $0 \leq a < r$ be chosen uniformly at random and interpreted as an $(l+1)$-bit string. Then the most significant bit of a is equal to 1 with probability $u/r < u/2^l < 1/2^\kappa$ and is equal to 0 with probability at least $1 - 1/2^\kappa$. Hence, when $\kappa \leq 1$ then the most significant bit is not a hardcore bit for the DLP. Note that the function g^a is not used here; the result merely follows from the distribution of integers modulo r.

Exercise 21.6.11. Let $r = 2^l + 2^{l-1} + u$ where $0 < u < 2^{l/2}$. Let $0 \leq a < r$ be uniformly chosen and represented as an $(l+1)$-bit string. Show that neither the most significant bit (i.e., bit l) nor bit $l-1$ of a are hardcore for the DLP.

The above examples show that for some primes the most significant bit is easy to predict. For other primes the most significant bit can be hard.

Exercise 21.6.12. Suppose $r = 2^l - 1$ is a Mersenne prime and let g have order r. Fix $0 \leq i \leq l$. Show that if $O(g, h)$ is a perfect oracle that returns the i-th bit of the DLP of h with respect to g then one can compute the whole DLP.

To summarise, low order bits of the DLP are always as hard as the DLP, while high order bits may or may not be hard. However, our examples of cases where the high order bits are easy are due not to any weakness of the DLP, but rather to statistical properties of residues modulo r. One way to deal with this issue is to define a bit as being "hard" if it cannot be predicted better than the natural statistical bias (see, for example, Definition 6.1 of Håstad and Näslund [279]). However this approach is less satisfactory for cryptographic applications if one wants to use the DLP as a source of unpredictable bits. Hence, it is natural to introduce a more statistically balanced predicate to use in place of high order bits. In practice, it is often more efficient to compute the least significant bit than to evaluate this predicate.

Exercise 21.6.13. Let g have order r. Let $f : \{0, 1, \ldots, r-1\} \to G$ be $f(x) = g^x$. Define $b(x) = 0$ if $0 \leq x < r/2$ and $b(x) = 1$ if $r/2 \leq x < r$. Show, using the method of Exercise 21.6.4, that $b(x)$ is a hardcore bit for f.

We do not cover all results on hard bits for the DLP. See Section 9 of Håstad and Näslund [279] for a general result and further references.

So far we only discussed showing that single bits of the DLP are hard. There are several approaches to defining the notion of a set of k bits being simultaneously hard. One definition states that the bits are hard if, for every non-constant function $B : \{0,1\}^k \to \{0,1\}$, given an oracle that takes as input g^x and computes B on the k bits of x in question one can use the oracle to solve the DLP. Another definition, which seems to be more useful in practice, is in terms of distinguishing the bits from random.

Definition 21.6.14. Let $f : \{0,1\}^n \to \{0,1\}^m$ be a one way function and let $S \subset \{1, \ldots, n\}$. We say the bits labelled by S are **simultaneously hard** if there is no polynomial-time algorithm that given $f(x)$ can distinguish the sequence $(x_i : i \in S)$ from a random $\#S$-bit string.

Peralta [480] (using next-bit-predictability instead of hardcore predicates or Definition 21.6.14) proves that $O(\log(\log(r)))$ least significant bits of the DLP are hard. Schnorr [524] (using Definition 21.6.14) proves that essentially any $O(\log(\log(r)))$ bits of the DLP are simultaneously hard (using the "bits" of Exercise 21.6.13 for the most significant bits).

Patel and Sundaram [478] showed, under a stronger assumption, that many more bits are simultaneously hard. Let g be an element of prime order r, let $l \in \mathbb{N}$ and set $k = \lceil \log_2(r) \rceil - l$. The ideas of Patel and Sundaram lead to the following result. If, given g^x, the k least significant bits of x are not simultaneously hard then there is an efficient algorithm to solve the DLP in an interval of length 2^l (see Exercise 13.3.6 for the definition of this problem). Hence, under the assumption that the DLP in an interval of length 2^l is hard, then one can output many bits. Taking $l = \log(\log(p))^{1+\epsilon}$ gives an essentially optimal asymptotic bit security result for the DLP.

21.6.1 Hard Bits for DLP in Algebraic Group Quotients

One can consider hard bits for the DLP in algebraic group quotients. In other words, let O_i be a perfect oracle that on input the equivalence class of an element $[g^a]$ outputs bit i of a. The first problem is that there is more than one value a for each class $[g^a]$ and so the bit is not necessarily well-defined.

Section 7 of Li, Näslund and Shparlinski [387] considers this problem for LUC. To make the problem well-defined they consider an element $g \in \mathbb{F}_{p^2}$ of prime order r and an oracle A such that $A(t) = a_i$ where a_i is the i-th bit of a for the unique $0 \leq a < r/2$ such that $t = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(g^a)$. The idea of their method is, given t, to compute the two roots $h_1 = g^a$ and $h_2 = g^{r-a}$ of $X^2 - tX + 1$ in $\mathbb{F}_{p^2}$ then use previous methods (e.g., Theorem 21.6.3 or Exercise 21.6.4) on each of them to compute either a or $r-a$ (whichever is smaller).

Exercise 21.6.15. Work out the details of the Li, Näslund and Shparlinski result for the case of the least significant bit of the DLP in LUC.

Exercise 21.6.16. Consider the algebraic group quotient corresponding to elliptic curve arithmetic using x-coordinates only. Fix $P \in E(\mathbb{F}_q)$ of prime order r. Let A be an oracle that on input $u \in \mathbb{F}_q$ outputs a_0 where a_0 is the 0-th bit of a such that $0 \leq a < r/2$ and $x([a]P) = u$. Show that the method of Li, Näslund and Shparlinski can be applied to show that this bit is a hard bit for the DLP.

Li, Näslund and Shparlinski remark that it seems to be hard to obtain a similar result for XTR. Theorem 3 of Jiang, Xu and Wang [315] claims to be such a result, but it does not seem to be proved their paper.

21.7 Bit Security of Diffie-Hellman

We now consider which bits of the CDH problem are hard. Since the solution to a CDH instance is a group element it is natural to expect, in contrast with our discussion of the DLP, that the hardcore bits and the proof techniques will depend on which group is being studied.

We first consider the case $g \in \mathbb{F}_p^*$ where p is a large prime and g is a primitive root. Our presentation follows Boneh and Venkatesan [85]. We assume every element $x \in \mathbb{F}_p^*$ is represented as an element of the set $\{1, 2, \ldots, p-1\}$ and we interpret $x \pmod p$ as returning a value in this set.

Definition 21.7.1. Let p be odd. Let $x \in \{1, 2, \ldots, p-1\}$. Define

$$\mathrm{MSB}_1(x) = \begin{cases} 0 & \text{if } 1 \leq x < p/2 \\ 1 & \text{otherwise.} \end{cases}$$

For $k \in \mathbb{N}$ let $0 \leq t < 2^k$ be the integer such that

$$tp/2^k \leq x < (t+1)p/2^k$$

and define $\mathrm{MSB}_k(x) = t$.

An alternative definition, which is commonly used in the literature and sometimes used in this book, is $\mathrm{MSB}_k(x) = u \in \mathbb{Z}$ such that $|x - u| \leq p/2^{k+1}$ (e.g., $u = \lfloor tp/2^k + p/2^{k+1} \rfloor$). For this definition it is unnecessary to assume $k \in \mathbb{N}$ and so one can allow $k \in \mathbb{R}_{>0}$.

Note that these are not bits of the binary representation of x. Instead, as in Exercise 21.6.13, they correspond to membership of x in a certain partition of $\{1, 2, \ldots, p-1\}$.

Ideally we would like to show that, say, MSB_1 is a hardcore bit for CDH. This seems to be out of reach for $\mathbb{F}_p^*$. Instead, we will show that, for $k \approx \sqrt{\log_2(r)}$, if one can compute $\mathrm{MSB}_k(g^{ab} \pmod p)$ then one can compute $g^{ab} \pmod p$. A consequence of this result is that there exists some predicate defined on $\mathrm{MSB}_k(g^{ab} \pmod p)$ whose value is a hardcore bit for CDH.

The central idea of most results on the bit security of CDH is the following. Let p be an odd prime and let $g \in \mathbb{F}_p^*$ be a primitive root. Let $h_1 = g^a, h_2 = g^b$ be a CDH instance where b is coprime to $p-1$. For $k \in \mathbb{N}$ let A_k be a perfect oracle such that

$$A_k(g, g^a, g^b) = \mathrm{MSB}_k(g^{ab}).$$

Choose a random element $1 \leq x < p$ and set $u = A_k(g, h_1 g^x, h_2)$. One has

$$u = \mathrm{MSB}_k(g^{(a+x)b}) = \mathrm{MSB}_k(g^{ab}t) \quad \text{where} \quad t = h_2^x.$$

In other words, the oracle A_k gives the most significant bits of multiples of the unknown g^{ab} by uniformly random elements $t \in \mathbb{F}_p^*$. The problem of using this information to compute g^{ab} is (a special case of) the hidden number problem.

21.7.1 The Hidden Number Problem

Definition 21.7.2. Let p be an odd prime and $k \in \mathbb{R}_{>1}$. Let $\alpha \in \mathbb{F}_p^*$ and let $t_1, \ldots, t_n \in \mathbb{F}_p^*$ be chosen uniformly at random. The **hidden number problem** (**HNP**) is, given $(t_i, u_i = \mathrm{MSB}_k(\alpha t_i \pmod p))$ for $1 \leq i \leq n$ to compute α.

Throughout this section we will allow any $k \in \mathbb{R}_{>1}$ and define $\mathrm{MSB}_k(x)$ to be any integer u such that $|x - u| < p/2^{k+1}$.

Before giving the main results we discuss two easy variants of Definition 21.7.2 where the values t_i can be chosen adaptively.

Lemma 21.7.3. *Let p be an odd prime and $1 \leq \alpha < p$. Suppose one has a perfect oracle A_1 such that $A_1(t) = \mathrm{MSB}_1(\alpha t \pmod p)$. Then one can compute α using $O(\log(p))$ oracle queries.*

Exercise 21.7.4. Prove Lemma 21.7.3.

Lemma 21.7.5. *Let p be an odd prime and $1 \leq \alpha < p$. Suppose one has a perfect oracle A such that $A(t) = \mathrm{LSB}_1(\alpha t \pmod p)$, where $\mathrm{LSB}_1(x)$ is the least significant bit of the binary representation of $0 \leq x < p$. Then one can compute α using $O(\log_2(p))$ oracle queries.*

Exercise 21.7.6. Prove Lemma 21.7.5.

Lemmas 21.7.3 and 21.7.5 show that the hidden number problem can be easy if the values t_i in Definition 21.7.2 are chosen adaptively. However, it intuitively seems harder to solve the hidden number problem when the t_i are randomly chosen. On the other hand, as k grows the HNP becomes easier; the case $k = \log_2(p)$ being trivial. Hence, one could hope to be able to solve the HNP as long as k is sufficiently large. We now explain the method of Boneh and Venkatesan [85] to solve the HNP using lattices.

Definition 21.7.7. Let $(t_i, u_i = \mathrm{MSB}_k(\alpha t_i))$ for $1 \leq i \leq n$. Define a lattice $L \subseteq \mathbb{R}^{n+1}$ by the rows of the basis matrix

$$B = \begin{pmatrix} p & 0 & 0 & \cdots & 0 & 0 \\ 0 & p & 0 & & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & p & 0 \\ t_1 & t_2 & t_3 & \cdots & t_n & 1/2^{k+1} \end{pmatrix}.$$

Define the vector $\underline{u} = (u_1, u_2, \ldots, u_n, 0) \in \mathbb{R}^{n+1}$ where $|u_i - (\alpha t_i \pmod p)| < p/2^{k+1}$.

Lemma 21.7.8. *Let L, $\underline{u}$ and n be as in Definition 21.7.7. Then* $\det(L) = p^n/2^{k+1}$ *and there exists a vector* $\underline{v} \in L$ *such that* $\|\underline{u} - \underline{v}\| < \sqrt{n+1}p/2^{k+1}$.

Proof: The first statement is trivial. For the second, note that $u_i = \mathrm{MSB}_k(\alpha t_i \pmod p)$ is the same as saying $\alpha t_i = u_i + \epsilon_i + l_i p$ for some $\epsilon_i, l_i \in \mathbb{Z}$ such that $|\epsilon_i| \leq p/2^{k+1}$, for $1 \leq i \leq n$. Now define $\underline{v} \in L$ by

$$\begin{aligned} \underline{v} = (-l_1, -l_2, \ldots, -l_n, \alpha)B &= (\alpha t_1 - l_1 p, \ldots, \alpha t_n - l_n p, \alpha/2^{k+1}) \\ &= (u_1 + \epsilon_1, \ldots, u_n + \epsilon_n, \alpha/2^{k+1}). \end{aligned}$$

The result follows since $\alpha/2^{k+1} < p/2^{k+1}$. □

We now show that, for certain parameters, it is reasonable to expect that any vector in the lattice L that is close to $\underline{u}$ gives the solution α.

Theorem 21.7.9. *Let $p > 2^8$ be prime and let $\alpha \in \mathbb{F}_p^*$. Let $n = 2\lceil\sqrt{\log_2(p)}\rceil \in \mathbb{N}$ and let $k \in \mathbb{R}$ be such that $\log_2(p) - 1 \geq k > \mu = \frac{1}{2}\sqrt{\log_2(p)} + 3$. Suppose $t_1, \ldots, t_n$ are chosen uniformly and independently at random in $\mathbb{F}_p^*$ and set $u_i = \mathrm{MSB}_k(\alpha t_i)$ for $1 \leq i \leq n$. Construct the lattice L as above. Let $\underline{u} = (u_1, \ldots, u_n, 0)$. Then, with probability at least $1 - 1/2^n \geq 63/64$ over all choices for $t_1, \ldots, t_n$, any vector $\underline{v} \in L$ such that $\|\underline{v} - \underline{u}\| < p/2^{\mu+1}$ is of the form*

$$\underline{v} = (\beta t_1 \pmod p, \ldots, \beta t_n \pmod p, \beta/2^{k+1})$$

where $\beta \equiv \alpha \pmod p$.

Proof: In the first half of the proof we consider $t_1, \ldots, t_n$ as fixed values. Later in the proof we compute a probability over all choices for the t_i.

First, note that every vector in the lattice is of the form

$$\underline{v} = (\beta t_1 - l_1 p, \beta t_2 - l_2 p, \ldots, \beta t_n - l_n p, \beta/2^{k+1})$$

for some $\beta, l_1, \ldots, l_n \in \mathbb{Z}$. If $\beta \equiv \alpha \pmod p$ then we are done, so suppose now that $\beta \not\equiv \alpha \pmod p$. Suppose also that $\|\underline{v} - \underline{u}\| < p/2^{\mu+1}$, which implies $|(\beta t_i \pmod p) - u_i| < p/2^{\mu+1}$ for all $1 \leq i \leq n$. Note that

$$\begin{aligned} |(\beta - \alpha)t_i \pmod p| &= |(\beta t_i \pmod p) - u_i + u_i - (\alpha t_i \pmod p)| \\ &\leq |(\beta t_i \pmod p) - u_i| + |(\alpha t_i \pmod p) - u_i| \\ &< p/2^{\mu+1} + p/2^{\mu+1} = p/2^{\mu}. \end{aligned}$$

We now consider $\gamma = (\beta - \alpha)$ as a fixed non-zero element of $\mathbb{F}_p$ and denote by A the probability, over all $t \in \mathbb{F}_p^*$, that $\gamma t \equiv u \pmod p$ for some $u \in \mathbb{Z}$ such that $|u| < p/2^{\mu}$ and $u \neq 0$. Since γt is uniformly distributed over $\mathbb{F}_p^*$ it follows that

$$A \leq \frac{2(p/2^{\mu})}{p-1} \leq \frac{1}{p-1}\left(\frac{2(p-1)+2}{2^{\mu}}\right) < \frac{2}{2^{\mu}} + \frac{2}{p-1} < \frac{4}{2^{\mu}}.$$

Since there are n uniformly and independently chosen $t_1, \ldots, t_n \in \mathbb{F}_p^*$ the probability that $|\gamma t_i \pmod p| < p/2^{\mu}$ for all $1 \leq i \leq n$ is A^n. Finally, there are $p-1$ choices for $\beta \in \{0, 1, \ldots, p-1\}$ such that $\beta \not\equiv \alpha \pmod p$. Hence, the probability over all such β and all $t_1, \ldots, t_n$ that $\|\underline{v} - \underline{u}\| < p/2^{\mu+1}$ is at most

$$(p-1)A^n < \frac{(p-1)4^n}{2^{\mu n}} < \frac{2^{\log_2(p)+2n}}{2^{\mu n}}.$$

Now, $\mu n = (\frac{1}{2}\sqrt{\log_2(p)} + 3)2\lceil\sqrt{\log_2(p)}\rceil \geq \log_2(p) + 3n$ so $(p-1)A^n < 2^{-n}$. Since $n \geq 6$ the result follows. □

Corollary 21.7.10. *Let $p > 2^{32}$ be prime, let $n = 2\lceil\sqrt{\log_2(p)}\rceil$ and let $k = \lceil\sqrt{\log_2(p)}\rceil + \lceil\log_2(\log_2(p))\rceil$. Given $(t_i, u_i = \mathrm{MSB}_k(\alpha t_i))$ for $1 \leq i \leq n$ as in Definition 21.7.2 one can compute α in polynomial-time.*

Proof: One constructs the basis matrix B for the lattice L in polynomial-time. Note that $n = O(\sqrt{\log(p)})$ so that the matrix requires $O(\log(p)^2)$ bits storage.

Running the LLL algorithm with factor $\delta = 1/4 + 1/\sqrt{2}$ is a polynomial-time computation (the lattice is not a subset of $\mathbb{Z}^{n+1}$ so Remark 17.5.5 should be applied, noting that only one column has non-integer entries) which returns an LLL-reduced basis. Let $\underline{u}$ be as above. The Babai nearest plane algorithm finds $\underline{v}$ such that $\|\underline{v} - \underline{u}\| < (1.6)2^{(n+1)/4}\sqrt{n+1}p/2^{k+1}$ by Theorem 18.1.7 and Lemma 21.7.8. This computation requires $O(\log(p)^{4.5})$ bit operations by Exercise 18.1.9. To apply Theorem 21.7.9 we need the vector $\underline{v}$ output from the Babai algorithm to be within $p/2^{\mu+1}$ of $\underline{u}$ where $\mu = \frac{1}{2}\sqrt{\log_2(p)} + 3$. Hence, we need

$$\frac{(1.6)2^{(n+1)/4}\sqrt{n+1}}{2^{k+1}} < \frac{1}{2^{\mu+1}},$$

which is $\mu + \log_2(1.6) + (n+1)/4 + \log_2(\sqrt{n+1}) < k = \lceil\sqrt{\log_2(p)}\rceil + \lceil\log_2(\log_2(p))\rceil$. Since

$$\begin{aligned}\mu + \log_2(1.6) + (n+1)/4 + \log_2(\sqrt{n+1}) &= \sqrt{\log_2(p)}/2 + 3.95 + \lceil\sqrt{\log_2(p)}\rceil/2 + \tfrac{1}{2}\log_2(n+1) \\ &\leq \lceil\sqrt{\log_2(p)}\rceil + 3.95 + \tfrac{1}{2}\log_2(n+1)\end{aligned}$$

the result follows whenever p is sufficiently large (the reader can check that $p > 2^{32}$ is sufficient).

It follows from Theorem 21.7.9 that, with probability at least 63/64 the vector $\underline{v} = (v_1, \ldots, v_{n+1}) \in \mathbb{R}^{n+1}$ output by the Babai algorithm is such that $v_{n+1}2^{k+1} \equiv \alpha \pmod{p}$. It follows that the hidden number α can be efficiently computed. □

Note that if $p \approx 2^{160}$ then $\mu \approx 9.32$. In practice, the algorithm works well for primes of this size. For example, Howgrave-Graham and Smart [299] present results of practical experiments where 8 of the most significant bits are provided by an oracle. We stress that these results do not show that all of the $k = \lceil\sqrt{\log_2(p)}\rceil + \lceil\log_2(\log_2(p))\rceil$ most significant bits are hard. Instead, one can only deduce that there is a predicate defined on these k bits that is a hardcore predicate for CDH.

Nguyen and Shparlinski [459] also remark that one could use other methods than LLL and the Babai nearest plane algorithm. They show that if one uses the Ajtai, Kumar and Sivakumar algorithm for CVP then one only needs $k = \lfloor\log(\log(p))\rfloor$ bits to obtain an algorithm for the hidden number problem with complexity of $p^{O(1/\log(\log(p)))}$ bit operations. They further show that if one has a perfect oracle for CVP (with respect to the ℓ_∞ norm) then one can solve the hidden number problem in polynomial time given only $k = 1 + \epsilon$ bits for any $\epsilon > 0$.

One final remark, the methods in this section assume a perfect oracle that outputs $\mathrm{MSB}_1(\alpha t \pmod{p})$. Since there seems to be no way to determine whether the output of the oracle is correct, it is an open problem to get results in the presence of an oracle that sometimes makes mistakes (though, as we mention in the next section, when applying the hidden number problem to the bit security of CDH then there is a solution in the case of oracles with a relatively low probability of giving an incorrect answer). For further discussion and applications of the hidden number problem see Shparlinski [559].

21.7.2 Hard Bits for CDH Modulo a Prime

We can finally state a result about hard bits for CDH.

Theorem 21.7.11. *Let $p > 2^{32}$ be prime, let g be a primitive root modulo p and let $k = \lceil \sqrt{\log_2(p)} \rceil + \lceil \log_2(\log_2(p)) \rceil$. Suppose there is no polynomial-time algorithm to solve[10] CDH in $\mathbb{F}_p^*$. Then there is no polynomial-time algorithm to compute the k most significant bits of g^{ab} when given g, g^a and g^b.*

Proof: Let (g, g^a, g^b) be an instance of the CDH problem in $\langle g \rangle$ and write $\alpha = g^{ab}$ for the solution. We assume that $\gcd(b, p-1) = 1$ (this requirement is removed by González Vasco and Shparlinski [261]; other work mentioned below allows g to have prime order, in which case this restriction disappears).

Given a polynomial-time algorithm A such that $A(g, g^x, g^y) = \mathrm{MSB}_k(g^{xy} \pmod p)$ then one can call $A(g, g^a g^r, g^b)$ polynomially many times for uniformly random $r \in \{1, 2, \ldots, p-2\}$ to get $\mathrm{MSB}_k(\alpha t)$ where $t = g^{br} \pmod p$. Applying Corollary 21.7.10 gives a polynomial time algorithm to compute α. □

A number of significant open problems remain:

1. Theorem 21.7.11 shows it is hard to compute all of $\mathrm{MSB}_k(g^{ab})$ but that does not imply that, say, $\mathrm{MSB}_1(g^{ab})$ is hard. A stronger result would be to determine specific hardcore bits for CDH, or at least to extend the results to MSB_k for smaller values of k. Boneh and Venkatesan [86] give a method that works for $k = \lceil 2 \log(\log(p)) \rceil$ bits (where g is a primitive root in $\mathbb{F}_p^*$) but which needs a hint depending on p and g; they claim this is a non-uniform result but this depends on the instance generator (see the footnote of Section 21.4.3). For $k = \lfloor \log(\log(p)) \rfloor$ one can also consider the approach of Nguyen and Shparlinski [459] mentioned above.

   Akavia [8] uses a totally different approach to prove that MSB_1 is hard for CDH, but the method is again at best non-uniform (i.e., needs polynomial-sized auxiliary information depending on p and g^b).

2. We assumed perfect oracles for computing $\mathrm{MSB}_k(\alpha t)$ in the above results. For non-perfect oracles one can use the above methods to generate a list of candidate values for g^{ab} and then apply the CDH self-corrector of Section 21.3. We refer to González Vasco, Näslund and Shparlinski [260] for details.

   The method of Akavia [8] also works when the oracle for MSB_1 is unreliable.

3. The above results assumed that g is a primitive root modulo p, whereas in practice one chooses g to lie in a small subgroup of $\mathbb{F}_p^*$ of prime order. The proof of Theorem 21.7.11 generates values t that lie in $\langle g \rangle$ and so they are not uniformly at random in $\mathbb{F}_p^*$. González Vasco and Shparlinski have given results that apply when the order of g is less than $p-1$ (see Chapter 14 of [558] for details and references). Shparlinski and Winterhof [560, 561], building on work of Bourgain and Konyagin, have obtained results when the order of g is at least $\log(p)/\log(\log(p))^{1-\epsilon}$.

Exercise 21.7.12. This exercise concerns a static Diffie-Hellman key exchange protocol due to Boneh and Venkatesan [85] for which one can prove that the most significant bit is a hardcore bit. Suppose Alice chooses a prime p, an integer $1 \leq a < p-1$ such that $\gcd(a, p-1) = 1$ and sets $g = 2^{a^{-1} \pmod{p-1}} \pmod p$. Alice makes p and g public and keeps a private. When Bob wants to communicate with Alice he sends g^x for random $1 \leq x < p-1$ so that Alice and Bob share the key 2^x. Prove that $\mathrm{MSB}_1(2^x)$ is a hardcore bit.

[10] As we have seen, to make such a statement precise one needs an instance generator that outputs groups from a family.

[Hint: Suppose one has a perfect oracle A that on input g^y outputs $\mathrm{MSB}_1(2^y)$. Then one can store Bob's tranmission g^x and call $A(g^x g^y)$ to get $\alpha 2^y$, where $\alpha = 2^x$ is the desired hidden number. Then apply Lemma 21.7.3.]

Exercise 21.7.13. Let $g \in \mathbb{F}_p^*$ be a primitive root and let $\epsilon > 0$. Show that if one has a perfect oracle for $\mathrm{MSB}_{1+\epsilon}(g^{ab})$ then one can solve DDH in $\mathbb{F}_p^*$.

21.7.3 Hard Bits for CDH in Other Groups

So far we have only considered CDH in (subgroups of) $\mathbb{F}_p^*$ where p is prime. It is natural to consider CDH in subgroups of $\mathbb{F}_{p^m}^*$, in algebraic tori, in trace systems such as LUC and XTR, and in elliptic curves. The first issue is what is meant by "bits" of such a value. In practice, elements in such a group are represented as an n-tuple of elements in $\mathbb{F}_p$ and so it is natural to consider one component in $\mathbb{F}_p$ and take bits of it as done previously. When p is small one can consider a sequence of bits, each from different components. An early reference for bit security of CDH in this setting is Verheul [619].

It is possible to extend the results to traces relatively easily. The idea is that if $\{\theta_1, \ldots, \theta_m\}$ is a basis for $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$, if $\alpha = \sum_{j=1}^m \alpha_j \theta_j$ is hidden and if $t_i = \sum_{j=1}^m t_{i,j}\theta_j$ are known then $\mathrm{Tr}(\alpha t_i)$ is a linear equation in the unknown α_i. Li, Näslund and Shparlinski [387] have studied the bit security of CDH in LUC and XTR. We refer to Chapters 6 and 19 of Shparlinski [558] for further details and references.

Exercise 21.7.14. Let $\mathbb{F}_{2^m}$ be represented using a normal basis and let $g \in \mathbb{F}_{2^m}^*$. Suppose one has a perfect oracle A such that $A(g, g^a, g^b)$ returns the first coefficient of the normal basis representation of g^{ab}. Show how to use A to compute g^{ab}. Hence, conclude that the first coefficient is a hardcore bit for CDH in $\mathbb{F}_{2^m}^*$.

Exercise 21.7.15. Let $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/(F(x))$ and let $g \in \mathbb{F}_{2^m}^*$ have prime order $r > m$. Suppose one has a perfect oracle A such that $A(g, g^a, g^b)$ returns the constant coefficient of the polynomial basis representation of g^{ab}. Show how to use A to compute g^{ab}. Hence, conclude that the constant coefficient is a hardcore bit for CDH in $\mathbb{F}_{2^m}^*$.

Hard Bits for Elliptic Curve Diffie-Hellman

We now consider the case of elliptic curves E over $\mathbb{F}_q$. A typical way to extract bits from an elliptic curve point P is to consider the x-coordinate $x(P)$ as an element of $\mathbb{F}_q$ and then extract bits of this. It seems hard to give results for the bit security of CDH using an oracle $A(P, [a]P, [b]P) = \mathrm{MSB}_k(x([ab]P))$; the natural generalisation of the previous approach is to call $A(P, [a]P + [z]P, [b]P) = \mathrm{MSB}_k(x([ab]P + [zb]P))$ but the problem is that it is difficult to infer anything useful about $x([ab]P)$ from $x([ab]P + [zb]P)$ (similarly for least significant bits); see Jao, Jetchev and Venkatesan [309] for some results. However, Boneh and Shparlinski [84] had the insight to consider a more general oracle.

Definition 21.7.16. Let p be an odd prime and $k \in \mathbb{N}$. Let $A_{x,k}(A, B, P, [a]P, [b]P)$ be an oracle that returns $\mathrm{LSB}_k(x([ab]P))$ where $P \in E(\mathbb{F}_p)$ for the elliptic curve $E : y^2 = x^3 + Ax + B$. Similarly, let $A_{y,k}(A, B, P, [a]P, [b]P)$ be an oracle that returns $\mathrm{LSB}_k(y([ab]P))$.

The crucial idea is that, given a point $P = (x_P, y_P) \in E(\mathbb{F}_p)$ where $E : y^2 = x^3 + Ax + B$, one can consider an isomorphism $\phi(x, y) = (u^2 x, u^3 y)$ and $\phi(P) \in E'(\mathbb{F}_p)$ where $E' : Y^2 = X^3 + u^4 AX + u^6 B$. Hence, instead of randomising instances of CDH in a way analogous to that done earlier, one calls the oracle $A_{x,k}(u^4 A, u^6 B, \phi(P), \phi([a]P), \phi([b]P))$ to get $\mathrm{LSB}_k(x(\phi([ab]P))) = \mathrm{LSB}_k(u^2 x([ab]P) \pmod p)$ where u is controlled by the

attacker. This is very similar to the easy case of the hidden number problem in $\mathbb{F}_p^*$ from Lemma 21.7.5.

Lemma 21.7.17. *Suppose $p \equiv 2 \pmod 3$. Then $\mathrm{LSB}_1(y([ab]P))$ is a hardcore bit for CDH on elliptic curves over $\mathbb{F}_p$.*

Proof: We suppose $A_{y,1}$ is a perfect oracle for $\mathrm{LSB}_1(y([ab]P))$ as above. Calling

$$A_{y,1}(u^4 A, u^6 B, \phi(P), \phi([a]P), \phi([b]P))$$

gives $\mathrm{LSB}_1(u^3 y([ab]P))$. Since $\gcd(3, p-1) = 1$ it follows that cubing is a permutation of $\mathbb{F}_p^*$ and one can perform the method of Lemma 21.7.5 to compute $y([ab]P)$. Given $y([ab]P)$ there are at most 3 choices for $x([ab]P)$ and so CDH is solved with noticeable probability. □

In the general case (i.e., when $p \not\equiv 2 \pmod 3$) Boneh and Shparlinski have to work harder. They use the method of Alexi, Chor, Goldreich and Schnorr [9] or the simplified version by Fischlin and Schnorr [203] to extend the idea to non-perfect oracles.[11] Once this is done, the following trick can be applied to determine $\mathrm{LSB}_1(tx([ab]P))$: when t is a square one calls the oracle for $\mathrm{LSB}_1(u^2 x([ab]P))$ on $u = \sqrt{t} \pmod p$, and when t is not a square one flips a coin. The resulting non-perfect oracle for LSB_1 therefore solves the problem. We refer to [84] for the details.

We make some remarks.

1. A nice feature of the elliptic curve results is that they are independent of the order of the point P and so work for subgroups of any size.

2. The literature does not seem to contain bit security results for CDH on elliptic curves over non-prime fields. This would be a good student project.

3. Jetchev and Venkatesan [314] use isogenies to extend the applicability of the Boneh-Shparlinski method. Their motivation is that if one has an $\mathrm{LSB}_1(x([ab]P))$ oracle that works with only small (but noticeable) probability then it is possible to have a CDH instance on an elliptic curve E for which the oracle does not work for any twist of E. By moving around the isogeny class they claim that the probability of success increases. However, it is still possible to have a CDH instance on an elliptic curve E for which the oracle does not work for any elliptic curve in the isogeny class of E.

21.8 Further Topics

There are a number of other results related to the Diffie-Hellman problem that we do not have to space to cover. For example, Coppersmith and Shparlinski considered the existence of polynomial relations between g^x, g^y and g^{xy}. Canetti, Friedlander and Shparlinski considered the distribution of Diffie-Hellman triples (g^x, g^y, g^{xy}) in G^3. We refer to [558] for a survey of these topics and references.

[11] This is why Boneh and Shparlinski consider least significant bits rather than most significant bits for their result. The technique of Alexi et al is to randomise the query $\mathrm{LSB}_1(t\alpha)$ as $\mathrm{LSB}_1(s\alpha) \oplus \mathrm{LSB}_1((t+s)\alpha)$ for suitable values s. A good student project would be to obtain an analogous result for other bits (e.g., most significant bits).

Chapter 22

Digital Signatures Based on Discrete Logarithms

Public key signatures and their security notions were defined in Section 1.3.2. They are arguably the most important topic in public key cryptography (for example, to provide authentication of automatic software updates; see Section 1.1). This chapter gives some digital signature schemes based on the discrete logarithm problem. The literature on this topic is enormous and we only give a very brief summary of the area. RSA signatures are discussed in Section 24.6.

22.1 Schnorr Signatures

We assume throughout this section that an algebraic group G and an element $g \in G$ of prime order r are known to all users. The values (G, g, r) are known as **system parameters**. Let $h = g^a$ be a user's public key. A digital signature, on a message m with respect to a public key h, can be generated by a user who knows the private key a. It should be hard to compute a signature for a given public key without knowing the private key.

To explain the Schnorr signature scheme it is simpler to first discuss an identification scheme.

22.1.1 The Schnorr Identification Scheme

Informally, a **public key identification scheme** is a protocol between a Prover and a Verifier, where the Prover has a public key pk and private key sk, and the Verifier has a copy of pk. The protocol has three communication stages: first the Prover sends a commitment s_0; then the Verifier sends a challenge s_1; then the Prover sends a response s_2.

The Verifier either accepts or rejects the proof. The protocol is supposed to convince the Verifier that they are communicating with a user who knows the private key corresponding to the Prover's public key. In other words, the Verifier should be convinced that they are communicating with the Prover.

For the Schnorr scheme [522, 523] the Prover has public key $h = g^a$ where g is an element of an algebraic group of prime order r and $1 \leq a < r$ is chosen uniformly at random. The Prover chooses a random integer $0 \leq k < r$, computes $\mathsf{s}_0 = g^k$ and sends s_0 to the Verifier. The Verifier sends a "challenge" $1 \leq \mathsf{s}_1 < r$ to the Prover. The Prover returns $\mathsf{s}_2 = k + a\mathsf{s}_1 \pmod r$. The Verifier then checks whether

$$g^{\mathsf{s}_2} = \mathsf{s}_0 h^{\mathsf{s}_1} \tag{22.1}$$

and accepts the proof if this is the case. In other words, the Prover has successfully identified themself to the Verifier if the Verifier accepts the proof.

Exercise 22.1.1. Show that the Verifier in an execution of the Schnorr identification scheme does accept the proof when the Prover follows the steps correctly.

Exercise 22.1.2. Let $p = 311$ and $r = 31 \mid (p-1)$. Let $g = 169$, which has order r. Let $a = 11$ and $h = g^a \equiv 47 \pmod p$. Which of the following is a transcript $(\mathsf{s}_0, \mathsf{s}_1, \mathsf{s}_2)$ of a correctly performed execution of the Schnorr identification scheme?

$$(15, 10, 12),\ (15, 10, 27),\ (16, 10, 12),\ (15, 16, 0).$$

Security of the Private Key

Unlike public key encryption (at least, under passive attacks), with identification schemes and digital signature schemes a user is always outputting the results of computations involving their private key. Hence, it is necessary to ensure that we do not leak information about the private key. An attack of this type on GGH signatures was given by Nguyen and Regev; see Section 19.11. Hence, we now explain why executions of the Schnorr identification protocol do not leak the private key.

A protocol (involving a secret) that does not leak any information about the secret is known as "zero knowledge". It is beyond the scope of this book to discuss this topic in detail, but we make a few remarks in the setting of the Schnorr identification scheme. First, consider a Verifier who really does choose s_1 independently and uniformly at random (rather than as a function of s_0 and h). It is easy to see that anyone can produce triples $(\mathsf{s}_0, \mathsf{s}_1, \mathsf{s}_2)$ that satisfy equation (22.1), without knowing the private key (just choose s_1 and s_2 first and solve for s_0). Hence, a protocol transcript $(\mathsf{s}_0, \mathsf{s}_1, \mathsf{s}_2)$ itself carries no information about a (this shows that the protocol is "honest verifier zero knowledge"). However, this argument does not imply that the protocol leaks no information about the secret to an adversary who chooses s_1 carefully. We now argue that the protocol is secure in this setting. The idea is to consider any pair $(\mathsf{s}_1, \mathsf{s}_2)$. Then, for every $1 \leq a < r$, there is some integer $0 \leq k < r$ such that $\mathsf{s}_2 \equiv k + a\mathsf{s}_1 \pmod r$. Now, if k were known to the verifier then they could solve for a. But, since the discrete logarithm problem is hard, it is computationally infeasible to determine any significant information about the distribution of k from s_0. Hence s_2 leaks essentially no information about a. Furthermore, there are no choices for s_1 that more readily allow the Verifier to determine a.

For security, k must be chosen uniformly at random; see Exercise 22.1.3 and Section 22.3 for attacks if some information on k is known. We stress that such attacks are much stronger than the analogous attacks for Elgamal encryption (see Exercise 20.4.1); there the adversary only learns something about a single message, whereas here they learn the private key!

Exercise 22.1.3. Suppose the random values k used by a prover are generated using the linear congruential generator $k_{i+1} = Ak_i + B \pmod{r}$ for some $1 \leq A, B < r$. Suppose an adversary knows A and B and sees two protocol transcripts $(\mathsf{s}_0, \mathsf{s}_1, \mathsf{s}_2)$ and $(\mathsf{s}'_0, \mathsf{s}'_1, \mathsf{s}'_2)$ generated using consecutive outputs k_i and k_{i+1} of the generator. Show how the adversary can determine the private key a.

A generalisation of Exercise 22.1.3, where the modulus for the linear congruential generator is not r, is given by Bellare, Goldwasser and Micciancio [34].

Security Against Impersonation

Now we explain why the Verifier is convinced that the prover must know the private key a. The main ideas will also be used in the security proof of Schnorr signatures, so we go through the argument in some detail. First, we define an adversary against an identification protocol.

Definition 22.1.4. An **adversary against an identification protocol** (with an honest verifier) is a polynomial-time randomised algorithm A that takes as input a public key, plays the role of the Prover in the protocol with an honest Verifier, and tries to make the Verifier accept the proof. The adversary repeatedly and adaptively sends a value s_0, receives a challenge s_1 and answers with s_2 (indeed, the sessions of the protocol can be interleaved). The adversary is successful if the Verifier accepts the proof with noticeable probability (i.e., the probability, over all outputs s_0 by A and all choices for s_1, that the adversary can successfully respond with s_2 is at least one over a polynomial function of the security parameter). The protocol is secure if there is no successful adversary.

An adversary is just an algorithm A so it is reasonable to assume that A can be run in very controlled conditions. In particular, we will assume throughout this section that A can be repeatedly run so that it always outputs the same first commitment s_0 (think of A as a computer programme that calls a function `Random` to obtain random bits and then simply arrange that the function always returns the same values to A). This will allow us to respond to the same commitment with various different challenges s_1. Such an attack is sometimes known as a **rewinding attack** (Pointcheval and Stern [483] call it the **oracle replay attack**): If A outputs s_0, receives a challenge s_1, and answers with s_2 then re-running A on challenge s'_1 is the same as "rewinding" the clock back to when A had just output s_0 and then giving it a different challenge s'_1.

Theorem 22.1.5. *The Schnorr identification scheme is secure against impersonation (in the sense of Definition 22.1.4) if the discrete logarithm problem is hard.*

We first prove the result for perfect adversaries (namely, those that impersonate the user successfully every time the protocol is run). Later we discuss the result for more general adversaries.

Proof: (In the case of a perfect adversary) We build an expected polynomial-time algorithm (called the simulator) that solves a DLP instance (g, h) where g has prime order r and $h = g^a$ where $0 \leq a < r$ is chosen uniformly at random.

The simulator will play the role of the Verifier and will try to solve the DLP by interacting with A. First, the simulator starts A by giving it h as the public key and giving some choice for the function `Random`. The adversary outputs a value s_0, receives a response s_1 (chosen uniformly at random) from the simulator, then outputs s_2. Since A is perfect we assume that $(\mathsf{s}_0, \mathsf{s}_1, \mathsf{s}_2)$ satisfy the verification equation.

First note that if values s_0 and s_2 satisfy equation (22.1) then s_0 lies in the group generated by g and so is of the form $\mathsf{s}_0 = g^k$ for some $0 \leq k < r$. Furthermore, it then follows that $\mathsf{s}_2 \equiv k + a\mathsf{s}_1 \pmod{r}$.

Now the simulator can re-run A on the same h and the same function `Random` (this is the rewinding). It follows that A will output s_0 again. The simulator then gives A a challenge $\mathsf{s}'_1 \neq \mathsf{s}_1$. Since A is perfect, it responds with s'_2 satisfying equation (22.1).

We have $\mathsf{s}_2 \equiv k + a\mathsf{s}_1 \pmod{r}$ and $\mathsf{s}'_2 \equiv k + a\mathsf{s}'_1 \pmod{r}$. Hence the simulator can compute $a \equiv (\mathsf{s}_2 - \mathsf{s}'_2)(\mathsf{s}_1 - \mathsf{s}'_1)^{-1} \pmod{r}$ and solve the DLP. In other words, if there is no polynomial-time algorithm for the DLP then there can be no polynomial-time adversary A against the protocol. □

The above proof gives the basic idea, but is not sufficient since we must consider adversaries that succeed with rather small probability. There are various issues to deal with. For example, A may not necessarily succeed on the first execution of the identification protocol. Hence, one must consider many executions $(\mathsf{s}_{i,0}, \mathsf{s}_{i,1}, \mathsf{s}_{i,2})$ for $1 \leq i \leq t$ and guess the value i into which one introduces the challenge $\mathsf{s}'_{i,1}$. Also, A may only succeed for a small proportion of the challenges s_1 for a given s_0 (it is necessary for the proof that A can succeed on two different choices of s_1 for the same value s_0). This latter issue is not a problem (since A succeeds with noticeable probability, it must succeed for a noticeable proportion of values s_1 for most values s_0). The former issue is more subtle and is solved using the forking lemma.

The **forking lemma** was introduced by Pointcheval and Stern [483]. A convenient generalisation has been given by Bellare and Neven [36]. The forking lemma determines the probability that a rewinding attack is successful. More precisely, consider an algorithm A (the adversary against the signature scheme) that takes as input a `Random` function and a list of responses s_1 to its outputs s_0. We will repeatedly choose a `Random` function and run A twice, the first time with a set of values $(\mathsf{s}_{1,1}, \ldots, \mathsf{s}_{t,1})$ being the responses in the protocol and the second time with a set $(\mathsf{s}_{1,1}, \ldots, \mathsf{s}_{j-1,1}, \mathsf{s}'_{j,1}, \ldots, \mathsf{s}'_{t,1})$ of responses for some $1 \leq j \leq t$. Note that A will output the same values $\mathsf{s}_{i,0}$ in both runs when $1 \leq i \leq j$. The forking lemma gives a lower bound on the probability that A succeeds in the identification protocol in the j-th execution as desired. Lemma 1 of [36] states that the success probability is at least $p(p/t - 1/r)$ where p is the success probability of A, t is the number of executions of the protocol in each game, and r is the size of the set of possible responses. Hence, if p is noticeable, t is polynomial and $1/r$ is negligible then the simulator solves the DLP with noticeable probability. We refer to [36, 483] and Section 10.4.1 of Vaudenay [616] for further details.

Exercise 22.1.6. Show that if the challenge values s_1 chosen by a Verifier can be predicted (e.g., because the Verifier is using a weak pseudorandom number generator) then a malicious player can impersonate an honest user in the Schnorr identification scheme.

Exercise 22.1.7. In the Schnorr identification scheme as presented above, the challenge is a randomly chosen integer $1 \leq \mathsf{s}_1 < r$. Instead, for efficiency[1] reasons, one could choose $1 \leq \mathsf{s}_1 < 2^l$ for some l such that $l \geq \kappa$ (where κ is the security parameter, but where 2^l is significantly smaller than r). Show that the proof of Theorem 22.1.5 still holds in this setting.

Exercise 22.1.8. Explain why the Schnorr identification scheme cannot be implemented in an algebraic group quotient.

22.1.2 Schnorr Signatures

We now present the **Schnorr signature scheme** [522, 523], which has very attractive security and efficiency. The main idea is to make the identification protocol of the previous

[1] One could speed up signature verification using similar methods to Exercise 22.1.13.

section non-interactive by replacing the challenge s_1 by a random integer that depends on the message being signed. This idea is known as the **Fiat-Shamir transform**. By Exercise 22.1.6 it is important that s_1 cannot be predicted and so it is also necessary to make it depend on s_0.

More precisely, one sets $\mathsf{s}_1 = H(\mathsf{m}\|\mathsf{s}_0)$ where H is a cryptographic hash function from $\{0,1\}^*$ to $\{0,1\}^l$ for some parameter l and where m and s_0 are interpreted as binary strings (and where $\|$ denotes concatenation of binary strings as usual).

One would therefore obtain the following signature scheme, which we call **naive Schnorr signatures**: To sign a message m choose a random $0 \leq k < r$, compute $\mathsf{s}_0 = g^k$, $\mathsf{s}_1 = H(\mathsf{m}\|\mathsf{s}_0)$ and $\mathsf{s}_2 = k + a\mathsf{s}_1 \pmod r$, and send the signature $(\mathsf{s}_0, \mathsf{s}_2)$ together with m. A verifier, given $\mathsf{m}, (\mathsf{s}_0, \mathsf{s}_2)$ and the public key h, would compute $\mathsf{s}_1 = H(\mathsf{m}\|\mathsf{s}_0)$ and accept the signature if

$$g^{\mathsf{s}_2} = \mathsf{s}_0 h^{\mathsf{s}_1}. \tag{22.2}$$

Schnorr makes the further observation that instead of sending $(\mathsf{s}_0, \mathsf{s}_2)$ one could send $(\mathsf{s}_1, \mathsf{s}_2)$. This has major implications for the size of signatures. For example, g may be an element of order r in $\mathbb{F}_p^*$ (for example, with $r \approx 2^{256}$ and $p \approx 2^{3072}$). In this case, $\mathsf{s}_0 = g^k$ requires 3072 bits, s_2 requires 256 bits, and s_1 may require as little as 128 bits. In other words, signatures would have $3072 + 256 = 3328$ bits in the naive scheme, whereas Schnorr signatures only require $128 + 256 = 384$ bits.

We present the precise Schnorr signature scheme in Figure 22.1.

KeyGen: This is the same as classic textbook Elgamal encryption. It outputs an algebraic group, an element g of prime order r, a public key $h = g^a$ and a private key $1 \leq a < r$ where a is uniformly chosen.

Sign(g, a, m): Choose uniformly at random $0 \leq k < r$, compute $\mathsf{s}_0 = g^k$, $\mathsf{s}_1 = H(\mathsf{m}\|\mathsf{s}_0)$ and $\mathsf{s}_2 = k + a\mathsf{s}_1 \pmod r$, where the binary string s_1 is interpreted as an integer in the usual way. The signature is $(\mathsf{s}_1, \mathsf{s}_2)$.

Verify$(g, h, \mathsf{m}, (\mathsf{s}_1, \mathsf{s}_2))$: Ensure that h is a valid public key for the user in question then test whether

$$\mathsf{s}_1 = H(\mathsf{m}\|g^{\mathsf{s}_2} h^{-\mathsf{s}_1}).$$

Figure 22.1: Schnorr Signature Scheme.

Example 22.1.9. Let $p = 311$ and $r = 31 \mid (p-1)$. Let $g = 169$ which has order r. Let $a = 11$ and $h = g^a \equiv 47 \pmod p$.

To sign a message m (a binary string) let $k = 20$ and $\mathsf{s}_0 = g^k \equiv 225 \pmod p$. The binary expansion of s_0 is $(11100001)_2$. We must now compute $\mathsf{s}_1 = H(\mathsf{m}\|11100001)$. Since we don't want to get into the details of H, let's just suppose that the output length of H is 4 and that s_1 is the binary string 1001. Then s_1 corresponds to the integer 9. Finally, we compute $\mathsf{s}_2 = k + a\mathsf{s}_1 \equiv 20 + 11 \cdot 9 \equiv 26 \pmod r$. The signature is $(\mathsf{s}_1, \mathsf{s}_2) = (9 = (1001)_2, 26)$. To verify the signature one computes

$$g^{\mathsf{s}_2} h^{-\mathsf{s}_1} = 169^{26} 47^{-9} \equiv 225 \pmod p$$

and checks that $\mathsf{s}_1 = H(\mathsf{m}\|11100001)$.

Exercise 22.1.10. Show that the Verify algorithm does succeed when given a pair $(\mathsf{s}_1, \mathsf{s}_2)$ output by the Sign algorithm.

22.1.3 Security of Schnorr Signatures

The security of Schnorr signatures essentially follows from the same ideas as used in Theorem 22.1.5. In particular, the security depends on the discrete logarithm problem (rather than CDH or DDH as is the case for Elgamal encryption). However, since the challenge is now a function of the message m and s_0, the exact argument of Theorem 22.1.5 cannot be used directly.

One approach is to replace the hash function by a random oracle H (see Section 3.7). The simulator can then control the values of H and the proof of Theorem 22.1.5 can be adapted to work in this setting. A careful analysis of Schnorr signatures in the random oracle model, using this approach and the forking lemma, was given by Pointcheval and Stern [483]. We refer to Theorem 14 of their paper for a precise result in the case where the output of H is $(\mathbb{Z}/r\mathbb{Z})^*$. A proof is also given in Section 10.4.2 of Vaudenay [616]. An analysis of the case where the hash function H maps to $\{0,1\}^l$ where $l < \log_2(r)$ is given by Neven, Smart and Warinschi [453].

There is no known proof of the security of Schnorr signatures in the standard model (even under very strong assumptions about the hash function). Paillier and Vergnaud [476] give evidence that one cannot give a reduction, in the standard model, from signature forgery for Schnorr signatures (with H mapping to $\mathbb{Z}/r\mathbb{Z}$) to DLP. More precisely, they show that if there is a reduction of a certain type (which they call an algebraic reduction) in the standard model from signature forgery for Schnorr signatures to DLP, then there is an algorithm for the "one-more DLP". We refer to [476] for the details.

We now discuss some specific ways to attack the scheme:

1. Given a signature $(\mathsf{s}_1, \mathsf{s}_2)$ on message m, if one can find a message m' such that $H(\mathsf{m} \| g^{\mathsf{s}_2} h^{-\mathsf{s}_1}) = H(\mathsf{m}' \| g^{\mathsf{s}_2} h^{-\mathsf{s}_1})$, then one has a signature also for the message m'. This fact can be used to obtain an existential forgery under a chosen-message attack.

   While one expects to be able to find hash collisions after roughly $2^{l/2}$ computations of H (see Section 3.2), what is needed here is not a general hash collision. Instead, we need a collision of the form $H(\mathsf{m} \| R) = H(\mathsf{m}' \| R)$ where $R = g^{\mathsf{s}_2} h^{-\mathsf{s}_1}$ is *not known* until a signature $(\mathsf{s}_1, \mathsf{s}_2)$ on m has been obtained. Hence, the adversary must first output a message m, then get the signature $(\mathsf{s}_1, \mathsf{s}_2)$ on m, then find m' such that $H(\mathsf{m} \| R) = H(\mathsf{m}' \| R)$. This is called the random-prefix second-preimage problem in Definition 4.1 of [453]. When R is sufficiently large it seems that solving this problem is expected to require around 2^l computations of H.

2. There is a passive existential forgery attack on Schnorr signatures if one can compute pre-images of H of a certain form. Precisely, choose any $(\mathsf{s}_1, \mathsf{s}_2)$ (for example, if the output of H is highly non-uniform then choose s_1 to be a "very likely" output of H), compute $R = g^{\mathsf{s}_2} h^{-\mathsf{s}_1}$, then find a bitstring m such that $H(\mathsf{m} \| R) = \mathsf{s}_1$. This attack is prevented if the hash function is hard to invert.

Hence, given a security parameter κ (so that breaking the scheme is required to take more than 2^κ bit operations) one can implement the Schnorr signature scheme with $r \approx 2^{2\kappa}$ and $l = \kappa$. For example, taking $\kappa = 128$, $2^{255} < r < 2^{256}$ and $l = 128$ gives signatures of 384 bits.

Exercise 22.1.11. ★ Fix $g \in G$ of order r and $\mathsf{m} \in \{0,1\}^*$. Can a pair $(\mathsf{s}_1, \mathsf{s}_2)$ be a Schnorr signature on the same message m for two different public keys? Are there any security implications of this fact?

22.1.4 Efficiency Considerations for Schnorr Signatures

The Sign algorithm performs one exponentiation, one hash function evaluation, and one computation modulo r. The Verify algorithm performs a multi-exponentiation $g^{\mathsf{s}_2}h^{-\mathsf{s}_1}$ where $0 \leq \mathsf{s}_2 < r$ and $1 \leq \mathsf{s}_1 < 2^l$ and one hash function evaluation. Hence, signing is faster than verifying.

There are a number of different avenues to speed up signature verification, depending on whether g is fixed for all users, whether one is always verifying signatures with respect to the same public key h or whether h varies, etc. We give a typical optimisation in Example 22.1.13. More dramatic efficiency improvements are provided by online/offline signatures (see Section 22.4), server-aided signature verification etc.

Exercise 22.1.12. Show how to modify the Schnorr signature scheme (with no loss of security) so that the verification equation becomes

$$\mathsf{s}_1 = H(\mathsf{m} \| g^{\mathsf{s}_2} h^{\mathsf{s}_1}).$$

Example 22.1.13. Suppose a server must verify many Schnorr signatures (using the variant of Exercise 22.1.12), always for the same value of g but for varying values of h. Suppose that $2^{l-1} < \sqrt{r} < 2^l$ (where l is typically also the output length of the hash function). One strategy to speed up signature verification is for the server to precompute and store the group element $g_1 = g^{2^l}$.

Given a signature $(\mathsf{s}_1, \mathsf{s}_2)$ with $0 \leq \mathsf{s}_1 < 2^l$ and $0 \leq \mathsf{s}_2 < r$ one can write $\mathsf{s}_2 = \mathsf{s}_{2,0} + 2^l \mathsf{s}_{2,1}$ with $0 \leq \mathsf{s}_{2,0}, \mathsf{s}_{2,1} < 2^l$. The computation of $g^{\mathsf{s}_2} h^{\mathsf{s}_1}$ is performed as the 3-dimensional multi-exponentiation (see Section 11.2)

$$g^{\mathsf{s}_{2,0}} g_1^{\mathsf{s}_{2,1}} h^{\mathsf{s}_1}.$$

The cost is roughly l squarings and $3l/2$ multiplications (the number of multiplications can be easily reduced using window methods, signed representations etc).

Schnorr [523] presents methods to produce the group elements g^k without having to perform a full exponentiation for each signature (the paper [523] is particularly concerned with making signatures efficient for smartcards). Schnorr's specific proposals were cryptanalysed by de Rooij [168].

22.2 Other Public Key Signature Schemes

The Schnorr signature scheme is probably the best public key signature scheme for practical applications.[2] A number of similar schemes have been discovered, the most well-known of which are Elgamal and DSA signatures. We discuss these schemes very briefly in this section.

22.2.1 Elgamal Signatures in Prime Order Subgroups

Elgamal [192] proposed the first efficient digital signature based on the discrete logarithm problem. We present the scheme for historical reasons, and because it gives rise to some nice exercises in cryptanalysis. For further details see Section 11.5.2 of [418] or Section 7.3 of [592].

[2] However, Schnorr signatures are not very widely used in practice. The reason for their lack of use may be the fact that they were patented by Schnorr.

Assume that g is an element of prime[3] order r in an algebraic group G. In this section we always think of G as being the "full" algebraic group (such as $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$) and assume that testing membership $g \in G$ is easy. The public key of user A is $h = g^a$ and the private key is a, where $1 \leq a < r$ is chosen uniformly at random.

The Elgamal scheme requires a function $F : G \to \mathbb{Z}/r\mathbb{Z}$. The only property required of this function is that the output distribution of F restricted to $\langle g \rangle$ should be close to uniform (in particular, F is not required to be hard to invert). In the case where $G = \mathbb{F}_p^*$ it is usual to define $F : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, r-1\}$ by $F(n) = n \pmod r$. If G is the set of points on an elliptic curve over a finite field then one could define $F(x, y)$ by interpreting x (or x and y) as binary strings, letting n be the integer whose binary expansion is x (or $x \| y$), and then computing $n \pmod r$.

To sign a message m with hash $H(\mathsf{m}) \in \mathbb{Z}/r\mathbb{Z}$ one chooses a random integer $1 \leq k < r$, computes $\mathsf{s}_1 = g^k$, computes $\mathsf{s}_2 = k^{-1}(H(\mathsf{m}) - aF(\mathsf{s}_1)) \pmod r$, and returns $(\mathsf{s}_1, \mathsf{s}_2)$. To verify the signature $(\mathsf{s}_1, \mathsf{s}_2)$ on message m one checks whether $\mathsf{s}_1 \in \langle g \rangle$, $0 \leq \mathsf{s}_2 < r$, and

$$h^{F(\mathsf{s}_1)} \mathsf{s}_1^{\mathsf{s}_2} = g^{H(\mathsf{m})}$$

in G. Elgamal signatures are the same size as naive Schnorr signatures.

A striking feature of the scheme is the way that s_1 appears both as a group element and as an exponent (this is why we need the function F). In retrospect, this is a poor design choice for both efficiency and security. The following exercises explore these issues in further detail. Pointcheval and Stern give a variant of Elgamal signatures (the trick is to replace $H(\mathsf{m})$ by $H(\mathsf{m} \| \mathsf{s}_1)$) and prove the security in Sections 3.3.2 and 3.3.3 of [483].

Exercise 22.2.1. Show that the Verify algorithm succeeds if the Sign algorithm is run correctly.

Exercise 22.2.2. Show that one can verify Elgamal signatures by computing a single 3-dimensional multi-exponentiation. Show that the check $\mathsf{s}_1 \in \langle g \rangle$ can therefore be omitted if $\gcd(\mathsf{s}_2, \#G) = 1$. Hence, show that the time to verify an Elgamal signature when F and H map to $\mathbb{Z}/r\mathbb{Z}$ is around twice the time of the method in Example 22.1.13 to verify a Schnorr signature. Explain why choosing F and H to map to l-bit integers where $l \approx \log_2(r)/2$ does not lead to a verification algorithm as fast as the one in Example 22.1.13.

Exercise 22.2.3. (Elgamal [192]) Suppose the hash function H is deleted in Elgamal signatures (i.e., we are signing messages $\mathsf{m} \in \mathbb{Z}/r\mathbb{Z}$). Give a passive existential forgery in this case. (i.e., the attack only requires the public key).

Exercise 22.2.4. ★ Consider the Elgamal signature scheme in $\mathbb{F}_p^*$ with the function $F(n) = n \pmod r$. Suppose the function $F(n)$ computes $n \pmod r$ for all $n \in \mathbb{N}$ (not just $0 \leq n < p$) and that the check $\mathsf{s}_1 \in \langle g \rangle$ does not include any check on the size of the integer s_1 (for example, it could simply be the check that $\mathsf{s}_1^r \equiv 1 \pmod p$ or the implicit check of Exercise 22.2.2). Give a passive selective forgery attack.

Exercise 22.2.5. Consider the following variant of Elgamal signatures in a group $\langle g \rangle$ of order r: The signature on a message m for public key h is a pair $(\mathsf{s}_1, \mathsf{s}_2)$ such that $0 \leq \mathsf{s}_1, \mathsf{s}_2 < r$, and

$$h^{\mathsf{s}_1} g^{H(\mathsf{m})} = g^{\mathsf{s}_2}.$$

Show how to determine the private key of a user given a valid signature.

[3] The original Elgamal signature scheme specifies that g is a primitive root in $\mathbb{F}_p^*$, but for compatibility with all other cryptographic protocols in this book we have converted it to work with group elements of prime order in any algebraic group.

Exercise 22.2.6.★ (Bleichenbacher [66]) Consider the Elgamal encryption scheme in $\mathbb{F}_p^*$ with the function $F(n) = n \pmod r$. Suppose the checks $\mathsf{s}_1 \in \langle g \rangle$ and $0 \leq \mathsf{s}_2 < r$ are not performed by the Verify algorithm. Show how an adversary who has maliciously chosen the system parameter g can produce selective forgeries for any public key under a passive attack.

Exercise 22.2.7. (Vaudenay [615]) Let H be a hash function with l-bit output. Show how to efficiently compute an l-bit prime r, and messages $\mathsf{m}_1, \mathsf{m}_2$ such that $H(\mathsf{m}_1) \equiv H(\mathsf{m}_2) \pmod r$. Hence, show that if one can arrange for an algebraic group with subgroup of order r to be used as the system parameters for a signature scheme then one can obtain a signature on m_1 for any public key h by obtaining from user A a signature on m_2.

A convenient feature of Elgamal signatures is that one can verify a batch of signatures faster than individually verifying each of them. Some details are given in Exercise 22.2.8. Early work on this problem was done by Naccache, M'Raïhi, Vaudenay and Raphaeli [449] (in the context of DSA) and Yen and Laih [637]. Further discussion of the problem is given by Bellare, Garay and Rabin [33].

Exercise 22.2.8. Let $(\mathsf{s}_{1,i}, \mathsf{s}_{2,i})$ be purported signatures on messages m_i with respect to public keys h_i for $1 \leq i \leq t$. A verifier can choose random integers $1 \leq w_i < r$ and verify all signatures together by testing whether $\mathsf{s}_{1,i} \in \langle g \rangle$ and $0 \leq \mathsf{s}_{2,i} < r$ for all i and the single equation

$$\left(\prod_{i=1}^{t} h_i^{w_i F(\mathsf{s}_{1,i})} \right) \left(\prod_{i=1}^{t} \mathsf{s}_{1,i}^{w_i \mathsf{s}_{2,i}} \right) = g^{\sum_{i=1}^{t} w_i H(\mathsf{m}_i)}. \tag{22.3}$$

Show that if all the signatures $(\mathsf{s}_{1,i}, \mathsf{s}_{2,i})$ are valid then the batch is declared valid. Show that if there is at least one invalid signature in the batch then the probability the batch is declared valid is at most $1/(r-1)$. Show how to determine, with high probability, the invalid signatures using a binary search.

If one uses the methods of Exercise 22.2.2 then verifying the t signatures separately requires t three-dimensional multi-exponentiations. One can break equation (22.3) into about $2t/3$ three-dimensional multi-exponentiations. So, for groups where testing $\mathsf{s}_{1,i} \in \langle g \rangle$ is easy (e.g., elliptic curves of prime order), the batch is asymptotically verified in about $2/3$ the time of verifying the signatures individually. Show how to speed up verification of a batch of signatures further if the public keys h_i are all equal. How much faster is this than verifying the signatures individually?

Yen and Laih [637] consider batch verification of naive Schnorr signatures as mentioned in Section 22.1.2. Given t signatures $(\mathsf{s}_{0,i}, \mathsf{s}_{2,i})$ on messages m_i and for keys h_i, Yen and Laih choose $1 \leq w_i < 2^l$ (for a suitable small value of l; they suggest $l = 15$) and verify the batch by testing $\mathsf{s}_{0,i} \in \langle g \rangle$, $0 \leq \mathsf{s}_{2,i} < r$ and

$$g^{\sum_{i=1}^{t} w_i \mathsf{s}_2} = \prod_{i=1}^{t} \mathsf{s}_{0,i}^{w_i} \prod_{i=1}^{t} h_i^{w_i H(\mathsf{m}_i \| \mathsf{s}_{0,i})}.$$

Give the verification algorithm when the public keys are all equal. Show that the cost is roughly $l/(3\log_2(r))$ times the cost of verifying t Elgamal signatures individually.

Explain why it seems impossible to verify batches of Schnorr signatures faster than verifying each individually.

22.2.2 DSA

A slight variant of the Elgamal signature scheme was standardised by NIST[4] as a digital signature standard. This is often called **DSA**.[5] In the case where the group G is an elliptic curve then the scheme is often called **ECDSA**.

In brief, the scheme has the usual public key $h = g^a$ where g is an element of prime order r in an algebraic group G and $1 \leq a < r$ is chosen uniformly at random. As with Elgamal signatures, a function $F : G \to \mathbb{Z}/r\mathbb{Z}$ is required. To sign a message with hash value $H(\mathsf{m})$ one chooses a random $1 \leq k < r$ and computes $\mathsf{s}_1 = F(g^k)$. If $\mathsf{s}_1 = 0$ then repeat[6] for a different value of k. Then compute $\mathsf{s}_2 = k^{-1}(H(\mathsf{m}) + a\mathsf{s}_1) \pmod r$ and, if $\mathsf{s}_2 = 0$ then repeat for a different value of k. The signature on message m is $(\mathsf{s}_1, \mathsf{s}_2)$. To verify the signature one first checks that $1 \leq \mathsf{s}_1, \mathsf{s}_2 < r$, then computes $u_1 = H(\mathsf{m})\mathsf{s}_2^{-1} \pmod r$, $u_2 = \mathsf{s}_1\mathsf{s}_2^{-1} \pmod r$, then determines whether or not

$$\mathsf{s}_1 = F(g^{u_1}h^{u_2}). \tag{22.4}$$

Note that a DSA signature is a pair of integers modulo r so is shorter in general than an Elgamal signature but longer in general than a Schnorr signature. Verification is performed using multi-exponentiation.

Exercise 22.2.9. Show that Verify succeeds on values output by Sign.

Exercise 22.2.10. The case $\mathsf{s}_1 = 0$ is prohibited in DSA signatures. Show that if this check was omitted and if an adversary could find an integer k such that $F(g^k) = 0$ then the adversary could forge DSA signatures for any message. Hence show that, as in Exercise 22.2.6, an adversary who maliciously chooses the system parameters could forge signatures for any message and any public key.

Exercise 22.2.11. The case $\mathsf{s}_2 = 0$ is prohibited in DSA signatures since the Verify algorithm fails when s_2 is not invertible. Show that if a signer outputs a signature $(\mathsf{s}_1, \mathsf{s}_2)$ produced by the Sign algorithm but with $\mathsf{s}_2 = 0$ then an adversary would be able to determine the private key a.

We saw in Exercise 22.2.2 that verifying Elgamal signatures is slow compared with verifying Schnorr signatures using the method in Example 22.1.13. Exercise 22.2.12 shows a variant of DSA (analogous to naive Schnorr signatures) that allows signature verification closer in speed to Schnorr signatures.

Exercise 22.2.12. (Antipa, Brown, Gallant, Lambert, Struik and Vanstone [11]) Consider the following variant of the DSA signature scheme: To sign m choose $1 \leq k < r$ randomly, compute $\mathsf{s}_0 = g^k$, $\mathsf{s}_2 = k^{-1}(H(m) + aF(\mathsf{s}_0)) \pmod r$ and return $(\mathsf{s}_0, \mathsf{s}_2)$. To verify $(\mathsf{m}, \mathsf{s}_0, \mathsf{s}_2)$ one computes $u_1 = H(\mathsf{m})\mathsf{s}_2^{-1} \pmod r$, $u_2 = F(\mathsf{s}_0)\mathsf{s}_2^{-1} \pmod r$ as in standard DSA and checks whether

$$\mathsf{s}_0 = g^{u_1}h^{u_2}. \tag{22.5}$$

Show that one can also verify the signature by checking, for any $1 \leq v < r$, whether

$$\mathsf{s}_0^v = g^{u_1 v}h^{u_2 v}. \tag{22.6}$$

Show that one can efficiently compute an integer $1 \leq v < r$ such that the equation (22.6) can be verified more quickly than equation (22.5).

[4] NIST stands for "National Institute of Standards and Technology" and is an agency that develops technology standards for the USA.

[5] DSA stands for "digital signature algorithm".

[6] The events $\mathsf{s}_1 = 0$ and $\mathsf{s}_2 = 0$ occur with negligible probability and so do not effect the performance of the signing algorithm.

There is no proof of security for DSA signatures in the standard or random oracle model. A proof of security in the random oracle model of a slightly modified version of DSA (the change is to replace $H(\mathsf{m})$ with $H(\mathsf{m}\|\mathsf{s}_1)$) was given by Pointcheval and Vaudenay [484, 105] (also see Section 10.4.2 of [616]). A proof of security for DSA in the generic group model[7] was given by Brown; see Chapter II of [65].

Exercise 22.2.13. Consider a digital signature scheme where a signature on message m with respect to public key h is an integer $0 \leq \mathsf{s} < r$ such that

$$\mathsf{s} = H(\mathsf{m}\|h^{\mathsf{s}}).$$

What is the problem with this signature scheme?

22.2.3 Signatures Secure in the Standard Model

None of the signature schemes considered so far has a proof of security in the standard model. Indeed, as mentioned, Paillier and Vergnaud [476] give evidence that Schnorr signatures cannot be proven secure in the standard model. In this section we briefly mention a signature scheme due to Boneh and Boyen [76, 77] that is secure in the standard model. However, the security relies on a very different computational assumption than DLP and the scheme needs groups with an extra feature (namely, a pairing; see Definition 22.2.14). We present a simple version of their scheme that is unforgeable under a weak chosen-message attack if the q-strong Diffie-Hellman problem holds (these notions are defined below).

We briefly introduce pairing groups (more details are given in Chapter 26). We use multiplicative notation for pairing groups, despite the fact that G_1 and G_2 are typically subgroups of elliptic curves over finite fields and hence are usually written additively.

Definition 22.2.14. (**Pairing groups**) Let G_1, G_2, G_T be cyclic groups of prime order r. A **pairing** is a map $e : G_1 \times G_2 \to G_T$ such that

1. e is non-degenerate and bilinear, i.e., $g_1 \in G_1 - \{1\}$ and $g_2 \in G_2 - \{1\}$ implies $e(g_1, g_2) \neq 1$ and $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for $a, b \in \mathbb{Z}$,
2. there is a polynomial-time algorithm to compute $e(g_1, g_2)$.

For the Boneh-Boyen scheme we also need there to be an efficiently computable injective group homomorphism $\psi : G_2 \to G_1$ (for example, a distortion map; see Section 26.6.1).

We will assume that elements in G_1 have a compact representation (i.e., requiring not much more than $\log_2(r)$ bits) whereas elements of G_2 do not necessarily have a compact representation. The signature is an element of G_1 and hence is very short. Figure 22.2 gives the (weakly secure) Boneh-Boyen Signature Scheme.

Exercise 22.2.15. Show that if the Verify algorithm for weakly secure Boneh-Boyen signatures accepts (m, s) then $\mathsf{s} = g_1^{(\mathsf{m}+a)^{-1} \pmod r}$.

The Boneh-Boyen scheme is unforgeable under a weak chosen-message attack if the q-strong Diffie-Hellman problem holds. We define these terms now.

Definition 22.2.16. A **weak chosen-message attack** (called a **generic chosen-message attack** by Goldwasser, Micali and Rivest [258]) on a signature scheme is an

[7] The generic group model assumes that any algorithm to attack the scheme is a generic algorithm for the group G. This seems to be a reasonable assumption when using elliptic curves.

KeyGen: Choose $g_2 \in G_2 - \{1\}$ uniformly at random and set $g_1 = \psi(g_2)$. Let $z = e(g_1, g_2)$. Choose $1 \leq a < r$ and set $u = g_2^a$. The public key is $\mathsf{pk} = (g_1, g_2, u, z)$ and the private key is a.

Sign(m, a): We assume that $\mathsf{m} \in \mathbb{Z}/r\mathbb{Z}$. If $a + \mathsf{m} \equiv 0 \pmod r$ then return $\perp$, else compute $\mathsf{s} = g_1^{(a+\mathsf{m})^{-1} \pmod r}$ and return s.

Verify$(\mathsf{m}, \mathsf{s}, \mathsf{pk})$: Check that $\mathsf{s} \in G_1$ and then check that

$$e(\mathsf{s}, ug_2^{\mathsf{m}}) = z.$$

Figure 22.2: Weakly Secure Boneh-Boyen Signature Scheme.

adversary A that outputs a list $\mathsf{m}_1, \ldots, \mathsf{m}_t$ of messages, receives a public key and signatures $\mathsf{s}_1, \ldots, \mathsf{s}_t$ on these messages, and then must output a message m and a signature s. The adversary wins if Verify$(\mathsf{m}, \mathsf{s}, \mathsf{pk})$ = "valid" and if $\mathsf{m} \notin \{\mathsf{m}_1, \ldots, \mathsf{m}_t\}$.

Hence, a weak chosen message attack is closer to a known message attack than a chosen message attack.

Definition 22.2.17. Let $q \in \mathbb{N}$ (not necessarily prime). Let G_1, G_2, G_T be pairing groups as in Definition 22.2.14. Let $g_1 \in G_1 - \{1\}$ and $g_2 \in G_2 - \{1\}$. The **q-strong Diffie-Hellman problem** (q-**SDH**) is, given $(g_1, g_2, g_2^a, g_2^{a^2}, \ldots, g_2^{a^q})$, where $1 \leq a < r$ is chosen uniformly at random, to output a pair

$$\left(\mathsf{m}, g_1^{(\mathsf{m}+a)^{-1} \pmod r}\right)$$

where $0 \leq \mathsf{m} < r$.

This problem may look rather strange at first sight since the value q can vary. The problem is mainly of interest when q is polynomial in the security parameter (otherwise, reading the problem description is not polynomial-time). Problems (or assumptions) like this are sometimes called parameterised since there is a parameter (in this case q) that determines the size for a problem instance. Such problems are increasingly used in cryptography, though many researchers would prefer to have systems whose security relies on more familiar assumptions.

There is evidence that the computational problem is hard. Theorem 5.1 of Boneh and Boyen [76] shows that a generic algorithm for q-SDH needs to make $\Omega(\sqrt{r/q})$ group operations to have a good chance of success. The algorithms of Section 21.5 can be used to solve q-SDH. In particular, if $q \mid (r-1)$ (and assuming $q < \sqrt{r}$) then Theorem 21.5.1 gives an algorithm to compute a with complexity $O(\sqrt{r/q})$ group operations, which meets the lower bound for generic algorithms.

Exercise 22.2.18. Show that one can use ψ and e to verify that the input to an instance of the q-SDH is correctly formed. Similarly, show how to use e to verify that a solution to a q-SDH instance is correct.

Theorem 22.2.19. *If the q-SDH problem is hard then the weak Boneh-Boyen signature scheme is secure under a weak chosen message attack, where the adversary requests at most $q-1$ signatures.*

Proof: (Sketch) Let $(g_1, g_2, g_2^a, g_2^{a^2}, \ldots, g_2^{a^q})$ be a q-SDH instance and let A be an adversary against the scheme. Suppose A outputs messages $\mathsf{m}_1, \ldots, \mathsf{m}_t$ with $t < q$.

Without loss of generality, $t = q - 1$ (since one can just add dummy messages). The idea of the proof is to choose a public key so that one knows $g_1^{(\mathsf{m}_i+a)^{-1}}$ for all $1 \leq i \leq t$. The natural way to do this would be to set

$$g_1' = g_1^{\prod_{i=1}^{t}(\mathsf{m}_i+a)}$$

but the problem is that we don't know a. The trick is to note that $F(a) = \prod_{i=1}^{t}(\mathsf{m}_i+a) = \sum_{i=0}^{t} F_i a^i$ is a polynomial in a with explicitly computable coefficients in $\mathbb{Z}/r\mathbb{Z}$. One can therefore compute $g_2' = g_2^{F(a)}$, $g_1' = \psi(g_2')$ and $h = g_2^{aF(a)}$ using, for example,

$$g_2' = \prod_{i=0}^{t} \left(g^{a^i}\right)^{F_i}.$$

Similarly, one can compute signatures for all the messages m_i. Hence, the simulator provides to A the public key $(g_1', g_2', h, z' = e(g_1', g_2'))$ and all t signatures.

Eventually, A outputs a forgery (m, s) such that $\mathsf{m} \neq \mathsf{m}_i$ for $1 \leq i \leq t$. If $t < q - 1$ and q is polynomial in the security parameter then m is one of the dummy messages with negligible probability $(q - 1 - t)/r$. One has

$$\mathsf{s} = g_1'^{(\mathsf{m}+a)^{-1} \pmod r} = g_1^{F(a)(\mathsf{m}+a)^{-1} \pmod r}.$$

The final trick is to note that the polynomial $F(a)$ can be written as $G(a)(a + \mathsf{m}) + c$ for some explicitly computable values $G(a) \in (\mathbb{Z}/r\mathbb{Z})[a]$ and $c \in (\mathbb{Z}/r\mathbb{Z})^*$. Hence, the rational function $F(a)/(a + \mathsf{m})$ can be written as

$$\frac{F(a)}{a+\mathsf{m}} = G(a) + \frac{c}{a+\mathsf{m}}.$$

One can therefore deduce $g_1^{(a+\mathsf{m})^{-1} \pmod r}$ as required. □

A fully secure signature scheme is given in [76] and it requires an extra element in the public key and an extra element (in $\mathbb{Z}/r\mathbb{Z}$) in the signature. The security proof is rather more complicated, but the essential idea is the same.

Jao and Yoshida [313] showed the converse result, namely that if one can solve q-SDH then one can forge signatures for the Boneh-Boyen scheme.

22.3 Lattice Attacks on Signatures

As mentioned earlier, there is a possibility that signatures could leak information about the private key. Indeed, Nguyen and Regev [457] give such an attack on lattice-based signatures.

The aim of this section is to present an attack due to Howgrave-Graham and Smart [299]. They determine the private key when given some signatures and given some bits of the random values k (for example, due to a side-channel attack or a weak pseudorandom number generator). The analysis of their attack was improved by Nguyen and Shparlinski [459, 460] (also see Chapter 16 of [558]).

The attack works for any signature scheme where one can obtain from a valid signature a linear equation modulo r with two unknowns, namely the private key a and the randomness k. We now clarify that this attack applies to the s_2 value for the Schnorr, Elgamal and DSA signature schemes:

Schnorr: $\mathsf{s}_2 \equiv k + a\mathsf{s}_1 \pmod r$ where $\mathsf{s}_1, \mathsf{s}_2$ are known.

Elgamal: $k\mathsf{s}_2 \equiv H(\mathsf{m}) - aF(\mathsf{s}_1) \pmod{r}$ where $H(\mathsf{m}), F(\mathsf{s}_1)$ and s_2 are known.

DSA: $k\mathsf{s}_2 \equiv H(\mathsf{m}) + a\mathsf{s}_1 \pmod{r}$ where $H(\mathsf{m}), \mathsf{s}_1$ and s_2 are known.

Suppose we are given a message m and a valid signature $(\mathsf{s}_1, \mathsf{s}_2)$ and also the l most or least significant bits of the random value k used by the Sign algorithm to generate s_1. Writing these known bits as k_0 we have, in the case of least significant bits, $k = k_0 + 2^l z$ where $0 \leq z < r/2^l$. Indeed, one gets a better result by writing

$$k = k_0 + 2^l \lfloor r/2^{l+1} \rfloor + 2^l z \tag{22.7}$$

with $-r/2^{l+1} \leq z \leq r/2^{l+1}$. Then one can re-write any of the above linear equations in the form

$$z \equiv ta - u \pmod{r}$$

for some $t, u \in \mathbb{Z}$ that are known. In other words, we know

$$\Big(t, u = \mathrm{MSB}_l(at \pmod{r})\Big), \tag{22.8}$$

which is an instance of the hidden number problem (see Section 21.7.1).

If the values t in equation (22.8) are uniformly distributed in $\mathbb{Z}/r\mathbb{Z}$ then Corollary 21.7.10 directly implies that if $r > 2^{32}$ and if we can determine $l \geq \lceil \sqrt{\log_2(r)} \rceil + \lceil \log_2(\log_2(r)) \rceil$ consecutive bits of the randomness k then one can determine the private key a in polynomial-time given $n = 2\lceil \sqrt{\log_2(r)} \rceil$ message-signature pairs. As noted in [459], in the practical attack the values t arising are not uniformly distributed. We refer to [459, 460] for the full details. In practice, the attack works well for current values for r when $l = 4$, see Section 4.2 of [459].

Exercise 22.3.1. Show how to obtain an analogue of equation (22.7) when the l most significant bits are known.

Bleichenbacher has described a similar attack on a specific implementation of DSA that used a biased random generator for the values k.

22.4 Other Signature Functionalities

There are many topics that are beyond the scope of this book. We briefly mention some of them now.

- One time signatures. These are fundamental in provable security and are used as a tool in many theoretical public key schemes. However, since these are usually realised without using the number theoretic structures presented in this book we do not give the details. Instead, we refer the reader to Section 11.6 of [418], Section 12.5 of [334] and Section 7.5.1 of [592].

- Online/offline signatures. The goal here is to design public key signature schemes that possibly perform some (slow) precomputations when they are "offline" but that generate a signature on a given message m extremely quickly. The typical application is smart cards or other tokens that may have extremely constrained computing power.

  The first to suggest a solution to this problem seems to have been Schnorr in his paper [522] on efficient signatures for smart cards. The Schnorr signature scheme

already has this functionality: if $\mathsf{s}_0 = g^k$ is precomputed during the idle time of the device, then generating a signature on message m only requires computing $\mathsf{s}_1 = H(\mathsf{m}\|\mathsf{s}_0)$ and $\mathsf{s}_2 = k + a\mathsf{s}_1 \pmod r$. The computation of s_1 and s_2 is relatively fast since no group operations are performed.

A simple idea due to Girault [254] (proposed for groups of unknown order, typically $(\mathbb{Z}/N\mathbb{Z})^*$) is to make Schnorr signatures even faster by omitting the modular reduction in the computation of s_2. In other words, k, a, s_1 are all treated as integers and s_2 is computed as the integer $k + a\mathsf{s}_1$. To maintain security it is necessary to take k to be bigger than $2^l r$ (i.e., bigger than any possible value for the integer $a\mathsf{s}_1$). This idea was fully analysed (and generalised to groups of known order) by Girault, Poupard and Stern [255].

- Threshold signatures. The idea is to have a signature that can only be generated by a collection of users. There is a large literature on this problem and we do not attempt a full treatment of the subject here.

  A trivial example is when two users hold additive shares a_1, a_2 of a private key (in other words, $h = g^{a_1+a_2} = g^{a_1}g^{a_2}$ is the public key). A Schnorr signature on message m can be computed as follows: User $i \in \{1, 2\}$ chooses a random integer $0 \leq k_i < r$, computes g^{k_i}, and sends it to the other. Both users can compute $\mathsf{s}_0 = g^{k_1}g^{k_2}$. User $i \in \{1, 2\}$ can then compute $\mathsf{s}_1 = H(\mathsf{m}\|\mathsf{s}_0)$ and $\mathsf{s}_{2,i} = k_i + a_i\mathsf{s}_1 \pmod r$. The signature is $(\mathsf{s}_0, \mathsf{s}_{2,1} + \mathsf{s}_{2,2} \pmod r)$.

- Signatures with message recovery. Usually a signature and a message are sent together. Signatures with message recovery allow some (or all) of the message to be incorporated in the signature. The whole message is recovered as part of the signature verification process. We refer to Section 11.5.4 of [418] for Elgamal signatures with message recovery.

- Undeniable signatures. These are public key signatures that can only be verified by interacting with the signer (or with some other designated verifier). A better name would perhaps be "invisible signatures" or "unverifiable signatures". We refer to Section 7.6 of [592].

- Identity-Based Signatures. Identity-based cryptography is a concept introduced by Shamir. The main feature is that a user's public key is defined to be a function of their "identity" (for example, their email address) together with some master public key. Each user obtains their private key from a Key Generation Center that possesses the master secret. One application of identity-based cryptography is to simplify public-key infrastructures.

  An identity-based signature is a public-key signature scheme for which it is not necessary to verify a public key certificate on the signer's key before verifying the signature (though note that it may still be necessary to verify a certificate for the master key of the system). There are many proposals in the literature, but we do not discuss them in this section. One example is given in Section 24.6.3).

Chapter 23

Public Key Encryption Based on Discrete Logarithms

Historically, encryption has been considered the most important part of cryptography. So it is not surprising that there is a vast literature about public key encryption. It is important to note that, in practice, public key encryption is not usually used to encrypt documents. Instead, one uses public key encryption to securely send keys, and the data is encrypted using symmetric encryption.

It is beyond the scope of this book to discuss all known results on public key encryption, or even to sketch all known approaches to designing public key encryption schemes. The goal of this chapter is very modest. We simply aim to give some definitions and to provide two efficient encryption schemes (one secure in the random oracle model and one secure in the standard model). The encryption schemes in this chapter are all based on Elgamal encryption, the "textbook" version of which has already been discussed in Sections 20.3 and 20.4.

Finally, we emphasise that this Chapter only discusses confidentiality and not simultaneous confidentiality and authentication. The reader is warned that naively combining signatures and encryption does not necessarily provide the expected security (see, for example, the discussion in Section 1.2.3 of Joux [317]).

23.1 CCA Secure Elgamal Encryption

Recall that security notions for public key encryption were given in Section 1.3.1. As we have seen, the textbook Elgamal encryption scheme does not have OWE-CCA security, since one can easily construct a related ciphertext whose decryption yields the original message. A standard way to prevent such attacks is to add a message authentication code (MAC); see Section 3.3.

We have also seen (see Section 20.3) that Elgamal can be viewed as static Diffie-Hellman key exchange followed by a specific symmetric encryption. Hence, it is natural to generalise Elgamal encryption so that it works with any symmetric encryption scheme. The scheme we present in this section is known as **DHIES** and, when implemented with elliptic curves, is called **ECIES**. We refer to Abdalla, Bellare and Rogaway [1] or Chapter III of [65] for background and discussion.

Let κ be a security parameter. The scheme requires a symmetric encryption scheme, a MAC scheme and a key derivation function. The symmetric encryption functions Enc and Dec take an l_1-bit key and encrypt messages of arbitrary length. The MAC function MAC takes an l_2-bit key and a message of arbitrary length and outputs an l_3-bit binary string. The key derivation function is a function $\mathsf{kdf} : G \to \{0,1\}^{l_1+l_2}$. The values l_1, l_2 and l_3 depend on the security parameter. Note that it is important that the MAC is evaluated on the ciphertext not the message, since a MAC is not required to have any confidentiality properties. The DHIES encryption scheme is given in Figure 23.1.

KeyGen(κ): Generate an algebraic group or algebraic group quotient G whose order is divisible by a large prime r (so that the discrete logarithm problem in the subgroup of prime order r requires at least 2^κ bit operations).
Choose a random $g \in G$ of exact order r. Choose a random integer $0 < a < r$ and set $h = g^a$.
The public key is (G, g, h) and the private key is a. Alternatively, (G, g) are system parameters that are fixed for all users and only h is the public key.

The message space is $\mathsf{M}_\kappa = \{0,1\}^*$.
The ciphertext space is $\mathsf{C}_\kappa = G \times \{0,1\}^* \times \{0,1\}^{l_3}$.

Encrypt(m, h): ($\mathsf{m} \in \{0,1\}^*$ and h is the authentic public key of the receiver)

- Choose a random $0 < k < r$ and set $\mathsf{c}_1 = g^k$.
- Set $K = \mathsf{kdf}(h^k)$ and parse K as $K_1 \| K_2$ where K_1 and K_2 are l_1 and l_2 bit binary strings respectively.
- Set $\mathsf{c}_2 = \mathsf{Enc}_{K_1}(m)$ and $\mathsf{c}_3 = \mathsf{MAC}_{K_2}(\mathsf{c}_2)$.
- Transmit the ciphertext $(\mathsf{c}_1, \mathsf{c}_2, \mathsf{c}_3)$.

Decrypt$(\mathsf{c}_1, \mathsf{c}_2, \mathsf{c}_3, a)$:

- Check that $\mathsf{c}_1 \in G$ and that c_3 is an l_3-bit string (if not then return $\perp$ and halt).
- Compute $K = \mathsf{kdf}(\mathsf{c}_1^a)$ and parse it as $K_1 \| K_2$.
- Check whether $\mathsf{c}_3 = \mathsf{MAC}_{K_2}(\mathsf{c}_2)$ (if not then return $\perp$ and halt).
- Return $\mathsf{m} = \mathsf{Dec}_{K_1}(\mathsf{c}_2)$.

Figure 23.1: DHIES Public Key Encryption.

Exercise 23.1.1. Show that decryption does return the message when given a ciphertext produced by the DHIES encryption algorithm.

A variant of DHIES is to compute the key derivation function on the pair of group (or algebraic group quotient) elements (g^k, h^k) rather than just h^k. This case is presented in

Section 10 of Cramer and Shoup [161]. As explained in Section 10.7 of [161], this variant can yield a tighter security reduction.

23.1.1 The KEM/DEM Paradigm

Shoup introduced a formalism for public key encryption that has proved to be useful. The idea is to separate the "public key" part of the system (i.e., the value c_1 in Figure 23.1) from the "symmetric" part (i.e., $(\mathsf{c}_2, \mathsf{c}_3)$ in Figure 23.1). A **key encapsulation mechanism** (or **KEM**) outputs a public key encryption of a random symmetric key (this functionality is very similar to **key transport**; the difference being that a KEM generates a fresh random key as part of the algorithm). A **data encapsulation mechanism** (or **DEM**) is the symmetric part. The name **hybrid encryption** is used to describe an encryption scheme obtained by combining a KEM with a DEM.

More formally, a KEM is a triple of three algorithms (KeyGen, Encrypt and Decrypt)[1] that depend on a security parameter κ. Instead of a message space, there is space $\mathcal{K}_\kappa$ of possible keys to be encapsulated. The randomised algorithm Encrypt takes as input a public key and outputs a ciphertext c and a symmetric key $K \in \mathcal{K}_\kappa$ (where κ is the security parameter). One says that c **encapsulates** K. The Decrypt algorithm for a KEM takes as input a ciphertext c and the private key and outputs a symmetric key K (or $\perp$ if the decryption fails). The Encrypt algorithm for a DEM takes as input a message and a symmetric key K and outputs a ciphertext. The Decrypt algorithm of a DEM takes a ciphertext and a symmetric key K and outputs either $\perp$ or a message.

The simplest way to obtain a KEM from Elgamal is given in Figure 23.2. The DEM corresponding to the hybrid encryption scheme in Section 23.1 takes as input m and K, parses K as $K_1 \| K_2$, computes $\mathsf{c}_2 = \mathsf{Enc}_{K_1}(\mathsf{m})$ and $\mathsf{c}_3 = \mathsf{MAC}_{K_2}(\mathsf{c}_2)$ and outputs $(\mathsf{c}_2, \mathsf{c}_3)$.

KeyGen(κ): This is the same as standard Elgamal; see Figure 23.1.
Encrypt(h): Choose random $0 \leq k < r$ and set $\mathsf{c} = g^k$ and $K = \mathsf{kdf}(h^k)$. Return the ciphertext c and the key K.
Decrypt(c, a): Return $\perp$ if $\mathsf{c} \notin \langle g \rangle$. Otherwise return $\mathsf{kdf}(\mathsf{c}^a)$.

Figure 23.2: Elgamal KEM.

Shoup has defined an analogue of IND-CCA security for a KEM. We refer to Section 7 of Cramer and Shoup [161] for precise definitions for KEMs, DEMs and their security properties, but give an informal statement now.

Definition 23.1.2. An IND-CCA adversary for a KEM is an algorithm A that plays the following game: The input to A is a public key. The algorithm A can also query a decryption oracle that will provide decryptions of any ciphertext of its choosing. At some point the adversary requests a challenge, which is a KEM ciphertext c^* together with a key $K^* \in \mathcal{K}_\kappa$. The challenger chooses K^* to be either the key corresponding to the ciphertext c^* or an independently chosen random element of $\mathcal{K}_\kappa$ (both cases with probability 1/2). The game continues with the adversary able to query the decryption oracle with any ciphertext $\mathsf{c} \neq \mathsf{c}^*$. Finally, the adversary outputs a guess for whether K^* is the key corresponding to c^*, or a random key (this is the same as the "real or random" security notion for key exchange in Section 20.5). Denote by $\Pr(A)$ the success probability of A in this game and define the **advantage** $\mathrm{Adv}(A) = |\Pr(A) - 1/2|$. The KEM is IND-CCA secure if every polynomial-time adversary has negligible advantage.

[1] Sometimes the names Encap and Decap are used instead of Encrypt and Decrypt.

Theorem 5 of Section 7.3 of [161] shows that, if a KEM satisfies IND-CCA security and if a DEM satisfies an analogous security property, then the corresponding hybrid encryption scheme has IND-CCA security. Due to lack of space we do not present the details.

23.1.2 Proof of Security in the Random Oracle Model

We now sketch a proof that the Elgamal KEM of Figure 23.2 has IND-CCA security. The proof is in the random oracle model. The result requires a strong assumption (namely, the Strong-Diffie-Hellman or gap-Diffie-Hellman assumption). Do not be misled by the use of the word "strong"! This computational problem is not harder than the Diffie-Hellman problem. Instead, the assumption that this problem is hard is a *stronger* (i.e., less likely to be true) assumption than the assumption that the Diffie-Hellman problem is hard.

Definition 23.1.3. Let G be a group of prime order r. The **strong Diffie-Hellman problem** (**Strong-DH**) is: Given $g, g^a, g^b \in G$ (where $1 \leq a, b < r$), together with a decision static Diffie-Hellman oracle (**DStatic-DH oracle**) $A_{g,g^a}(h_1, h_2)$ (i.e., $A_{g,g^a}(h_1, h_2) = 1$ if and only if $h_2 = h_1^a$), to compute g^{ab}.

An instance generator for Strong-DH takes as input a security parameter κ, outputs a group G and an element g of prime order r (with $r > 2^{2\kappa}$) and elements $g^a, g^b \in G$ where $1 \leq a, b < r$ are chosen uniformly at random. As usual, we say that Strong-DH is hard for the instance generator if all polynomial-time algorithms to solve the problem have negligible success probability. The **strong Diffie-Hellman assumption** is that there is an instance generator for which the Strong-DH problem is hard.

It may seem artificial to include access to a decision oracle as part of the assumption. Indeed, it is a significant drawback of the encryption scheme that such an assumption is needed for the security. Nevertheless, the problem is well-defined and seems to be hard in groups for which the DLP is hard. A related problem is the **gap Diffie-Hellman problem**: again the goal is to compute g^{ab} given (g, g^a, g^b), but this time one is given a full DDH oracle. In some situations (for example, when using supersingular elliptic or hyperelliptic curves) one can use pairings to provide a DDH oracle and the artificial nature of the assumption disappears. The proof of Theorem 23.1.4 does not require a full DDH oracle and so it is traditional to only make the Strong-DH assumption.

Theorem 23.1.4. *The Elgamal KEM of Figure 23.2, with the key derivation function replaced by a random oracle, is IND-CCA secure if the strong Diffie-Hellman problem is hard.*

Proof: (Sketch) Let (g, g^a, g^b) be the Strong-DH instance and let A_{g,g^a} be the DStatic-DH oracle. Let B be an IND-CCA adversary against the KEM. We want to use B to solve our Strong-DH instance. To do this we will simulate the game that B is designed to play. The simulation starts B by giving it the public key (g, g^a). Note that the simulator does not know the corresponding private key.

Since the key derivation function is now a random oracle, it is necessary for B to query the simulator whenever it wants to compute kdf; this fact is crucial for the proof. Indeed, the whole idea of the proof is that when B requests the challenge ciphertext we reply with $\mathsf{c}^* = g^b$ and with a randomly chosen $K^* \in \mathcal{K}_\kappa$. Since kdf is a random oracle, the adversary can have no information about whether or not c^* encapsulates K^* unless the query $\mathsf{kdf}((\mathsf{c}^*)^a)$ is made. Finally, note that $(\mathsf{c}^*)^a = g^{ab}$ is precisely the value the simulator wants to find.

More precisely, let E be the event (on the probability space of Strong-DH instances and random choices made by B) that B queries kdf on $(\mathsf{c}^*)^a = g^{ab}$. The advantage of B is

$\mathrm{Adv}(B) = \left|\Pr(B) - \frac{1}{2}\right|$ where $\Pr(B)$ is the probability that B wins the IND-CCA security game. Note that $\Pr(B) = \Pr(B|E)\Pr(E) + \Pr(B|\neg E)\Pr(\neg E)$. When kdf is a random oracle we have $\Pr(B|\neg E) = 1/2$. Writing $\Pr(B|E) = 1/2 + u$ for some $-1/2 \leq u \leq 1/2$ we have $\Pr(B) = 1/2 + u\Pr(E)$ and so $\mathrm{Adv}(B) = |u|\Pr(E)$. Since $\mathrm{Adv}(B)$ is assumed to be non-negligible it follows that $\Pr(E)$ is non-negligible. In other words, a successful adversary makes an oracle query on the value g^{ab} with non-negligible probability.

To complete the proof it is necessary to explain how to simulate kdf and Decrypt queries, and to analyse the probabilities. The simulator maintains a list of all queries to kdf. The list is initially empty. Every time that $\mathsf{kdf}(u)$ is queried the simulator first checks whether $u \in G$ and returns $\perp$ if not. Then the simulator checks whether an entry (u, K) appears in the list of queries and, if so, returns K. If no entry appears in the list then use the oracle A_{g,g^a} to determine whether $u = g^{ab}$ (i.e., if $A_{g,g^a}(g^b, u) = 1$). If this is the case then g^{ab} has been computed and the simulation outputs that value and halts. In all other cases, a value K is chosen uniformly and independently at random from $\mathcal{K}_\kappa$, (u, K) is added to the list of kdf queries, and K is returned to B.

Similarly, when a decryption query on ciphertext c is made then one checks, for each pair (u, K) in the list of kdf values, whether $A_{g,g^a}(\mathsf{c}, u) = 1$. If this is the case then return K. If there is no such triple then return a random $K' \in \mathcal{K}$.

One can check that the simulation is sound (in the sense that Decrypt does perform the reverse of Encrypt) and that the outputs of kdf are indistinguishable from random. Determining the advantage of the simulator in solving the strong-DH problem is then straightforward. We refer to Section 10.4 of Cramer and Shoup [161] for a careful proof using the "game hopping" methodology (actually, that proof applies to the variant in Exercise 23.1.5, but it is easily adapted to the general case). □

Exercise 23.1.5. A variant of the scheme has the key derivation function applied to the pair (g^k, h^k) in Encrypt instead of just h^k (respectively, $(\mathsf{c}_1, \mathsf{c}_1^a)$ in Decrypt). Adapt the security proof to this case. What impact does this have on the running time of the simulator?

The IND-CPA security of the Elgamal KEM can be proved in the standard model (the proof is analogous to the proof of Theorem 20.4.10) under the assumption of Definition 23.1.6. The IND-CCA security can also be proved in the standard model under an interactive assumption called the oracle Diffie-Hellman assumption. We refer to Abdalla, Bellare and Rogaway [1] for the details of both these results.

Definition 23.1.6. Let G be a group and $\mathsf{kdf} : G \to \mathcal{K}$ a key derivation function. The **hash Diffie-Hellman problem** (**Hash-DH**) is to distinguish the distributions $(g, g^a, g^b, \mathsf{kdf}(g^{ab}))$ and (g, g^a, g^b, K) where K is chosen uniformly from $\mathcal{K}$. The **hash Diffie-Hellman assumption** is that there exist instance generators such that all polynomial-time algorithms for Hash-DH have negligible advantage.

Exercise 23.1.7. Let G be a group of prime order r and let $\mathsf{kdf} : G \to \{0,1\}^l$ be a key derivation function such that $\log_2(r)/2 < l < \log_2(r)$ and such that the output distribution is statistically close to uniform. Show that DDH $\leq_R$ Hash-DH $\leq_R$ CDH.

An elegant variant of Elgamal, with IND-CCA security in the random oracle model depending only on CDH rather than strong Diffie-Hellman, is given by Cash, Kiltz and Shoup [120].

23.2 Cramer-Shoup Encryption

In their landmark paper [159], Cramer and Shoup gave an encryption scheme with a proof of CCA security in the standard model. Due to lack of space we will only be able to give a sketch of the security analysis of the scheme.

To motivate how they achieve their result, consider the proof of security for the Elgamal KEM (Theorem 23.1.4). The simulator uses the adversary to solve an instance of the CDH problem. To do this one puts part of the CDH instance in the public key (and hence, one does not know the private key) and part in the challenge ciphertext. To prove CCA security we must be able to answer decryption queries without knowing the private key. In the proof of Theorem 23.1.4 this requires a DDH oracle (to determine correct ciphertexts from incorrect ones) and also the use of the random oracle model (to be able to "see" some internal operations of the adversary).

In the random oracle model one generally expects to be able to prove security under an assumption of similar flavour to CDH (see Theorem 20.4.11 and Theorem 23.1.4). On the other hand, in the standard model one only expects[2] to be able to prove security under a decisional assumption like DDH (see Theorem 20.4.10). The insight of Cramer and Shoup is to design a scheme whose security depends on DDH and is such that the entire DDH instance can be incorporated into the challenge ciphertext. The crucial consequence is that the simulator can now generate public and private keys for the scheme, run the adversary, and be able to handle decryption queries.

The proof of security hinges (among other things) on the following result.

Lemma 23.2.1. *Let G be a group of prime order r. Let $g_1, g_2, u_1, u_2, h \in G$ with $(g_1, g_2) \neq (1, 1)$. Consider the set*

$$\mathcal{X}_{g_1,g_2,h} = \{(z_1, z_2) \in (\mathbb{Z}/r\mathbb{Z})^2 \ : \ h = g_1^{z_1} g_2^{z_2}\}.$$

Then $\#\mathcal{X}_{g_1,g_2,h} = r$. Let $0 \leq k < r$ be such that $u_1 = g_1^k$. If $u_2 = g_2^k$ then $u_1^{z_1} u_2^{z_2} = h^k$ for all $(z_1, z_2) \in \mathcal{X}_{g_1,g_2,h}$. If $u_2 \neq g_2^k$ then

$$\{u_1^{z_1} u_2^{z_2} : (z_1, z_2) \in \mathcal{X}_{g_1,g_2,h}\} = G.$$

Exercise 23.2.2. Prove Lemma 23.2.1.

Figure 23.3 presents the basic **Cramer-Shoup encryption scheme**. The scheme requires a group G of prime order r and the message m is assumed to be an element of G. Of course, it is not necessary to "encode" data into group elements, in practice one would use the Cramer-Shoup scheme as a KEM; we briefly describe a Cramer-Shoup KEM at the end of this section. The scheme requires a target-collision-resistant hash function $H : G^3 \to \mathbb{Z}/r\mathbb{Z}$ (see Definition 3.1.2) chosen at random from a hash family.

Exercise 23.2.3. Show that the value $v = c^k d^{k\alpha}$ computed in the Encrypt algorithm does satisfy equation (23.1).

Exercise 23.2.4. Show that the tests $u_1, u_2 \in G$ and equation (23.1) imply that $v \in G$.

Exercise 23.2.5. Show that the final stage of Decrypt in the Cramer-Shoup scheme can be efficiently performed using multiexponentiation as

$$\mathsf{m} = e u_1^{r-z_1} u_2^{r-z_2}.$$

[2]Unless performing "bit by bit" encryption, which is a design approach not considered in this book.

KeyGen(κ): Generate a group G of prime order r as in Figure 23.1. Choose random $g_1, g_2 \in G - \{1\}$. Choose integers $0 \leq x_1, x_2, y_1, y_2, z_1, z_2 < r$ uniformly at random and set

$$c = g_1^{x_1} g_2^{x_2}, \quad d = g_1^{y_1} g_2^{y_2}, \quad h = g_1^{z_1} g_2^{z_2}.$$

Choose a target-collision-resistant hash function H. The public key is $\mathsf{pk} = (G, H, g_1, g_2, c, d, h)$. The private key is $\mathsf{sk} = (x_1, x_2, y_1, y_2, z_1, z_2)$.

Encrypt(m, pk): Choose $0 \leq k < r$ uniformly at random, compute $u_1 = g_1^k, u_2 = g_2^k, e = h^k \mathsf{m}, \alpha = H(u_1, u_2, e)$ and $v = c^k d^{k\alpha \pmod r}$. The ciphertext is $\mathsf{c} = (u_1, u_2, e, v)$.

Decrypt($u_1, u_2, e, v, \mathsf{sk}$): First check that $u_1, u_2, e \in G$ and output $\perp$ if this is not the case. Next, compute $\alpha = H(u_1, u_2, e)$ and check whether

$$v = u_1^{x_1 + y_1 \alpha \pmod r} u_2^{x_2 + y_2 \alpha \pmod r}. \tag{23.1}$$

Return $\perp$ if this condition does not hold. Otherwise output

$$\mathsf{m} = e u_1^{-z_1} u_2^{-z_2}.$$

Figure 23.3: Basic Cramer-Shoup Encryption Scheme.

Example 23.2.6. Let $p = 311$, $r = 31$ and denote by G the subgroup of order r in $\mathbb{F}_p^*$. Take $g_1 = 169$ and $g_2 = 121$. Suppose $(x_1, x_2, y_1, y_2, z_1, z_2) = (1, 2, 3, 4, 5, 6)$ so that the public key is

$$(g_1, g_2, c, d, h) = (169, 121, 13, 260, 224).$$

To encrypt $\mathsf{m} = 265 \in G$ choose, say, $k = 15$ and set $u_1 = g_1^k = 24, u_2 = g_2^k = 113$ and $e = \mathsf{m} h^k = 126$. Finally, we must compute α. Since we don't want to get into the details of H, suppose $\alpha = H(u_1, u_2, e) = 20$ and so set $v = c^k d^{k\alpha \pmod r} = c^{15} d^{21} = 89$. The ciphertext is $(u_1, u_2, e, v) = (24, 113, 126, 89)$.

To decrypt one first checks that $u_1^r = u_2^r = e^r = 1$. Then one recomputes α and checks equation (23.1). Since

$$u_1^{x_1 + y_1 \alpha \pmod r} u_2^{x_2 + y_2 \alpha \pmod r} = u_1^{30} u_2^{20} = 89$$

the ciphertext passes this test. One then computes $e u_1^{r - z_1} u_2^{r - z_2} = 126 \cdot 24^{26} \cdot 113^{25} = 265$.

Exercise 23.2.7. Using the same private keys as Example 23.2.6, which of the following ciphertexts are valid, and for those that are, what is the corresponding message? Assume that $H(243, 83, 13) = 2$.

$$(243, 83, 13, 97), \ (243, 83, 13, 89), \ (243, 83, 13, 49).$$

We now turn to the security analysis. Note that the condition of equation (23.1) does not imply that the ciphertext (u_1, u_2, e, v) was actually produced by the Encrypt algorithm. However, we now show that, if u_1 and u_2 are not of the correct form, then the probability that a randomly chosen v satisfies this condition is $1/r$. Indeed, Lemma 23.2.8 shows that an adversary who can solve the discrete logarithm problem cannot even construct an invalid ciphertext that satisfies this equation with probability better than $1/r$.

Lemma 23.2.8. *Let G be a cyclic group of prime order r. Let $g_1, g_2, c, d, v \in G$ and $\alpha \in \mathbb{Z}/r\mathbb{Z}$ be fixed. Suppose $u_1 = g_1^k$ and $u_2 = g_2^{k + k'}$ where $k' \not\equiv 0 \pmod r$. Then the probability, over all choices (x_1, x_2, y_1, y_2) such that $c = g_1^{x_1} g_2^{x_2}$ and $d = g_1^{y_1} g_2^{y_2}$, that $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$ is $1/r$.*

Proof: Write $g_2 = g_1^w, c = g_1^{w_1}$ and $d = g_1^{w_2}$ for some $0 \leq w, w_1, w_2 < r$ with $w \neq 0$. The values c and d imply that $x_1 + wx_2 = w_1$ and $y_1 + wy_2 = w_2$. Now $u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$ equals g_1 to the power

$$\begin{aligned} k(x_1 + \alpha y_1) + (k + k')w(x_2 + \alpha y_2) &= k((x_1 + wx_2) + \alpha(y_1 + wy_2)) + k'w(x_2 + \alpha y_2) \\ &= k(w_1 + \alpha w_2) + k'w(x_2 + \alpha y_2). \end{aligned}$$

The values $w, w_1, w_2, k, k', \alpha$ are all uniquely determined but, by Lemma 23.2.1, x_2 and y_2 can take any values between 0 and $r-1$. Hence, $u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$ equals any fixed value v for exactly r of the r^2 choices for (x_2, y_2). □

Theorem 23.2.9. *The basic Cramer-Shoup encryption scheme is IND-CCA secure if DDH is hard and if the function H is target-collision-resistant.*

Proof: (Sketch) Let A be an adversary against the Cramer-Shoup scheme. Given a DDH instance (g_1, g_2, u_1, u_2) the simulator performs the KeyGen algorithm using the given values g_1, g_2. Hence, the simulator knows the private key $(x_1, x_2, y_1, y_2, z_1, z_2)$. The simulator runs A with this public key.

The algorithm A makes decryption queries and these can be answered correctly by the simulator since it knows the private key. Eventually, A outputs two messages $(\mathsf{m}_0, \mathsf{m}_1)$ and asks for a challenge ciphertext. The simulator chooses a random $b \in \{0, 1\}$, computes $e = u_1^{z_1} u_2^{z_2} \mathsf{m}_b$, $\alpha = H(u_1, u_2, e)$ and $v = u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha}$. Here, and throughout this proof, u_1 and u_2 denote the values in the DDH instance that was given to the simulator. The simulator returns

$$\mathsf{c}^* = (u_1, u_2, e, v).$$

to A. The adversary A continues to make decryption queries, which are answered as above. Eventually, A outputs a bit b'. The simulator returns "valid" as the answer to the DDH instance if $b = b'$ and "invalid" otherwise.

The central idea is that if the input is a valid DDH tuple then c^* is a valid encryption of m_b and so A ought to be able to guess b correctly with non-negligible probability. On the other hand, if the input is not a valid DDH tuple then, by Lemma 23.2.1, $u_1^{z_1} u_2^{z_2}$ could be any element in G (with equal probability) and so c^* could be an encryption of any message $\mathsf{m} \in G$. Hence, given c^*, both messages m_0 and m_1 are equally likely and so the adversary can do no better than output a random bit. (Of course, A may actually output a fixed bit in this case, such as 0, but this is not a problem since b was randomly chosen.)

There are several subtleties remaining in the proof. First, by Lemma 23.2.8, before the challenge ciphertext has been received there is a negligible probability that a ciphertext that was not produced by the Encrypt algorithm satisfies equation (23.1). Hence, the simulation is correct with overwhelming probability. However, the challenge ciphertext is potentially an example of a ciphertext that satisfies equation (23.1) and yet is not a valid output of the algorithm Encrypt. It is necessary to analyse the probability that A can somehow produce another ciphertext that satisfies equation (23.1) without just running the Encrypt algorithm. The target-collision-resistance of the hash function enters at this point (since a ciphertext of the form (u_1, u_2, e', v) such that $H(u_1, u_2, e') = H(u_1, u_2, e)$ would pass the test). Due to lack of space we refer to Section 4 of [159] (for a direct proof) or Section 6.2 of [161] (for a proof using "game hopping"). □

A number of variants of the basic scheme are given by Cramer and Shoup [161] and other authors. In particular, one can design a KEM based on the Cramer-Shoup scheme (see Section 9 of [161]): just remove the component e of the ciphertext and set the encapsulated key to be $K = \mathsf{kdf}(g_1^k, h^k)$. An alternative KEM (with even shorter ciphertext)

was proposed by Kurosawa and Desmedt [359]. Their idea was to set $K = \mathsf{kdf}(v)$ where $v = c^k d^{\alpha k}$ for $\alpha = H(u_1, u_2)$. The KEM ciphertext is therefore just $(u_1, u_2) = (g_1^k, g_2^k)$. The security again follows from Lemma 23.2.8: informally, querying the decryption oracle on badly formed (u_1, u_2) gives no information about the key K.

Exercise 23.2.10. Write down a formal description of the Cramer-Shoup KEM.

Exercise 23.2.11. Show that an adversary against the Cramer-Shoup scheme who knows any pair (z_1, z_2) such that $h = g_1^{z_1} g_2^{z_2}$ can decrypt valid ciphertexts.

Exercise 23.2.12. Suppose an adversary against the Cramer-Shoup scheme knows x_1, x_2, y_1, y_2. Show how the adversary can win the OWE-CCA security game.

Exercise 23.2.13. Suppose the checks that $u_1, u_2 \in G$ are omitted in the Cramer-Shoup cryptosystem. Suppose $G \subset \mathbb{F}_p^*$ where $l \mid (p-1)$ is a small prime (say $l < 2^{10}$). Suppose the Decrypt algorithm uses the method of Exercise 23.2.5. Show how to determine, using a decryption oracle, $z_1 \pmod l$ and $z_2 \pmod l$. Show that if $p - 1$ has many such small factors l then one could recover the values z_1 and z_2 in the private key of the Cramer-Shoup scheme.

Cramer and Shoup [160] have shown how the above cryptosystem fits into a general framework for constructing secure encryption schemes using "universal hash proof systems". We do not have space to present this topic.

23.3 Other Encryption Functionalities

There are many variants of public key encryption (such as threshold decryption, server-aided decryption, etc). In this section we briefly sketch two important variants: homomorphic encryption and identity-based encryption.

23.3.1 Homomorphic Encryption

Let $\mathsf{c}_1, \ldots, \mathsf{c}_k$ be ciphertexts that are encryptions under some public key of messages $\mathsf{m}_1, \ldots, \mathsf{m}_k$. The goal of homomorphic encryption is for any user to be able to efficiently compute a ciphertext that encrypts $F(\mathsf{m}_1, \ldots, \mathsf{m}_k)$ for any function F, given only a description of the function F and the ciphertexts $\mathsf{c}_1, \ldots, \mathsf{c}_k$. An encryption scheme that has this property is called **fully homomorphic**.

Homomorphic encryption schemes allow third parties to perform computations on encrypted data. A common additional security requirement is that the resulting ciphertexts do not reveal to a user with the private key what computation was performed (except its result). A typical application of homomorphic encryption is voting: If users encrypt either 0 or 1 under a certain public key[3] then a trusted third party can compute a ciphertext that is an encryption of the sum of all the users' votes, and then this ciphertext can be decrypted to give the total number of votes. If the user with the private key never sees the individual votes then they cannot determine how an individual user voted. A general survey on homomorphic encryption that gives some references for applications is Fontaine and Galand [208].

For many applications it is sufficient to consider encryption schemes that only allow a user to compute $F(\mathsf{m}_1, \ldots, \mathsf{m}_k)$ for certain specific functions (for example, addition in the voting application). In this section we focus on the case where $F(\mathsf{m}_1, \mathsf{m}_2)$ is a group operation.

[3]It is necessary for users to prove that their vote lies in $\{0, 1\}$.

Definition 23.3.1. Let G be a group (written multiplicatively). A public key encryption scheme with message space G and ciphertext space C is said to be **homomorphic** for the group G if there is some efficiently computable binary operation $\star$ on C such that, for all $\mathsf{m}_1, \mathsf{m}_2 \in G$, if c_1 is an encryption of m_1 and c_2 is an encryption of m_2 (both with respect to the same public key) then $\mathsf{c}_1 \star \mathsf{c}_2$ is an encryption of $\mathsf{m}_1\mathsf{m}_2$.

Exercise 23.3.2 shows that one cannot have CCA security when using homomorphic encryption. Hence, the usual security requirement of a homomorphic encryption scheme is that it should have IND-CPA security.

Exercise 23.3.2. Show that a homomorphic encryption scheme does not have IND-CCA security.

Exercise 23.3.3. Let $G = \langle g \rangle$ where g is an element of order r in a group. Let $\mathsf{c}_1 = (\mathsf{c}_{1,1}, \mathsf{c}_{1,2}) = (g^{k_1}, \mathsf{m}_1 h^{k_1})$ and $\mathsf{c}_2 = (\mathsf{c}_{2,1}, \mathsf{c}_{2,2}) = (g^{k_2}, \mathsf{m}_2 h^{k_2})$ be classic textbook Elgamal encryptions of $\mathsf{m}_1, \mathsf{m}_2 \in G$. Define $\mathsf{c}_1 \star \mathsf{c}_2 = (\mathsf{c}_{1,1}\mathsf{c}_{2,1}, \mathsf{c}_{1,2}\mathsf{c}_{2,2})$. Show that $\mathsf{c}_1 \star \mathsf{c}_2$ is an encryption of $\mathsf{m}_1\mathsf{m}_2$ and hence that classic textbook Elgamal encryption is homomorphic for the group G.

Exercise 23.3.4. Let $G = \mathbb{F}_2^l \cong \{0,1\}^l$. Note that G is a group under addition modulo 2 (equivalently, under exclusive-or $\oplus$). For $1 \leq i \leq 2$ let $\mathsf{c}_i = (\mathsf{c}_{i,1}, \mathsf{c}_{i,2}) = (g^{k_i}, \mathsf{m}_i \oplus H(h^{k_i}))$ be semi-textbook Elgamal encryptions of messages $\mathsf{m}_i \in G$. Consider the operation $\mathsf{c}_1 \star \mathsf{c}_2 = (\mathsf{c}_{1,1}\mathsf{c}_{2,1}, \mathsf{c}_{1,2} \oplus \mathsf{c}_{2,2})$. Show that semi-textbook Elgamal is not homomorphic with respect to this operation.

Exercise 23.3.5. A variant of Elgamal encryption that is homomorphic with respect to addition is to encrypt m as $(\mathsf{c}_1 = g^k, \mathsf{c}_2 = g^{\mathsf{m}} h^k)$. Prove that if $(\mathsf{c}_{i,1}, \mathsf{c}_{i,2})$ are ciphertexts encrypting messages m_i for $i = 1, 2$ then $(\mathsf{c}_{1,1}\mathsf{c}_{2,1}, \mathsf{c}_{1,2}\mathsf{c}_{2,2})$ encrypts $\mathsf{m}_1 + \mathsf{m}_2$. Give a decryption algorithm for this system and explain why it is only practical when the messages m are small integers. Hence show that this scheme does not strictly satisfy Definition 23.3.1 when the order of g is large.[4]

23.3.2 Identity-Based Encryption

Section 22.4 briefly mentioned identity-based signatures. Recall that in identity-based cryptography a user's public key is defined to be a function of their "identity" (for example, their email address). There is a master public key. Each user obtains their private key from a key generation center (which possesses the master secret).

In this section we sketch the **basic Boneh-Franklin scheme** [80] (the word "basic" refers to the fact that this scheme only has security against a chosen plaintext attack). The scheme uses pairing groups (see Definition 22.2.14 and Chapter 26). Hence, let G_1, G_2 and G_T be groups of prime order r and let $e : G_1 \times G_2 \to G_T$ be a non-degenerate bilinear pairing.

The first task is to determine the master keys, which are created by the key generation center. Let $g \in G_2$ have order r. The key generation center chooses $1 \leq s < r$ and computes $g' = g^s$. The master public key is (g, g') and the master private key is s. The scheme also requires hash functions $H_1 : \{0,1\}^* \to G_1$ and $H_2 : G_T \to \{0,1\}^l$ (where l depends on the security parameter). The message space will be $\{0,1\}^l$ and the ciphertext space will be $G_2 \times \{0,1\}^l$.

The public key of a user with identity $\mathsf{id} \in \{0,1\}^*$ is $Q_{\mathsf{id}} = H_1(\mathsf{id}) \in G_1$. With overwhelming probability $Q_{\mathsf{id}} \neq 1$, in which case $e(Q_{\mathsf{id}}, g) \neq 1$. The user obtains the

[4]The order of g must be large for the scheme to have IND-CPA security.

private key

$$Q'_{\mathsf{id}} = H_1(\mathsf{id})^s$$

from the key generation center.

To Encrypt a message $\mathsf{m} \in \{0,1\}^l$ to the user with identity id one obtains the master key (g, g'), computes $Q_{\mathsf{id}} = H_1(\mathsf{id})$, chooses a random $1 \leq k < r$ and computes $\mathsf{c}_1 = g^k, \mathsf{c}_2 = \mathsf{m} \oplus H_2(e(Q_{\mathsf{id}}, g')^k)$. The ciphertext is $(\mathsf{c}_1, \mathsf{c}_2)$.

To Decrypt the ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$ the user with private key Q'_{id} computes

$$\mathsf{m} = \mathsf{c}_2 \oplus H_2(e(Q'_{\mathsf{id}}, \mathsf{c}_1)).$$

This completes the description of the basic Boneh-Franklin scheme.

Exercise 23.3.6. Show that the Decrypt algorithm does compute the correct message when $(\mathsf{c}_1, \mathsf{c}_2)$ are the outputs of the Encrypt algorithm.

Exercise 23.3.7. Show that the basic Boneh-Franklin scheme does not have IND-CCA security.

The security model for identity-based encryption takes into account that an adversary can ask for private keys on various identities. Hence, the IND security game allows an adversary to output a challenge identity id^* and two challenge messages $\mathsf{m}_0, \mathsf{m}_1$. The adversary is not permitted to know the private key for identity id^* (though it can receive private keys for any other identities of its choice). The adversary then receives an encryption with respect to identity id^* of m_b for randomly chosen $b \in \{0,1\}$ and must output a guess for b.

Exercise 23.3.8. Suppose there is an efficiently computable group homomorphism $\psi : G_2 \to G_1$. Show that if an adversary knows ψ and can compute preimages of the hash function H_1 then it can determine the private key for any identity by making a private key query on a different identity.

If the output of H_2 is indistinguishable from random l-bit strings then it is natural to believe that obtaining the message from a ciphertext under a passive attack requires computing

$$e(Q'_{\mathsf{id}}, \mathsf{c}_1) = e(Q^s_{\mathsf{id}}, g^k) = e(Q_{\mathsf{id}}, g)^{sk}.$$

Hence, it is natural that the security (at least, in the random oracle model) depends on the following computational problem.

Definition 23.3.9. Let G_1, G_2 and G_T be groups of prime order r and let $e : G_1 \times G_2 \to G_T$ be a non-degenerate bilinear pairing. The **bilinear Diffie-Hellman problem** (**BDH**) is: Given $Q \in G_1$, $g \in G_2$, g^a and g^b, where $1 \leq a, b < r$, to compute

$$e(Q, g)^{ab}.$$

Exercise 23.3.10. Show that if one can solve CDH in G_2 or in G_T then one can solve BDH.

As seen in Exercise 23.3.7, the basic Boneh-Franklin scheme does not have IND-CCA security. To fix this one needs to provide some extra components in the ciphertext. Alternatively, one can consider the basic Boneh-Franklin scheme as an identity-based KEM: The ciphertext is $\mathsf{c}_1 = g^k$ and the encapsulated key is $K = \mathsf{kdf}(e(Q_{\mathsf{id}}, g')^k)$. In the random oracle model (treating both H_1 and kdf as random oracles) one can show that the Boneh-Franklin identity-based KEM has IND-CCA security (in the security model for

identity-based encryption as briefly mentioned above) assuming that the BDH problem is hard. We refer to Boneh and Franklin [80, 81] for full details and security proofs.

There is a large literature on identity-based encryption and its extensions, including schemes that are secure in the standard model. We do not discuss these topics further in this book.

Part VI

Cryptography Related to Integer Factorisation

Chapter 24

The RSA and Rabin Cryptosystems

The aim of this chapter is to briefly present some cryptosystems whose security is based on computational assumptions related to the integer factorisation problem. In particular, we study the RSA and Rabin cryptosystems. We also present some security arguments and techniques for efficient implementation.

Throughout the chapter we take 3072 bits as the benchmark length for an RSA modulus. We make the assumption that the cost of factoring a 3072-bit RSA modulus is 2^{128} bit operations. These figures should be used as a very rough guideline only.

24.1 The Textbook RSA Cryptosystem

Figure 24.1 recalls the "textbook" RSA cryptosystem, which was already presented in Section 1.2. We remind the reader that the main application of RSA encryption is to transport symmetric keys, rather than to encrypt actual documents. For digital signatures we always sign a hash of the message, and it is necessary that the hash function used in signatures is collision-resistant.

In Section 1.3 we noted that the security parameter κ is not necessarily the same as the bit-length of the RSA modulus. In this chapter it will be convenient to ignore this, and use the symbol κ to denote the bit-length of an RSA modulus N. We always assume that κ is even.

As we have seen in Section 1.2, certain security properties can only be satisfied if the encryption process is randomised. Since the RSA encryption algorithm is deterministic it follows that the message m used in RSA encryption should be obtained from some **randomised padding scheme**. For example, if N is a 3072-bit modulus then the "message" itself may be a 256-bit AES key and may have 2815 random bits appended to

KeyGen(κ): (Assume κ even.) Generate two distinct primes p and q uniformly at random in the range $2^{\kappa/2-1} < p, q < 2^{\kappa/2}$. Set $N = pq$ so that $2^{\kappa-2} < N < 2^{\kappa}$ is represented by κ bits (see Exercise 24.1.1 to ensure that N has leading bit 1).
Choose a random κ-bit integer e coprime to $(p-1)$ and $(q-1)$ (or choose $e = 2^{16}+1 = 65537$ and insist $p, q \not\equiv 1 \pmod{e}$). Define $d = e^{-1} \pmod{\lambda(N)}$ where $\lambda(N) = \mathrm{lcm}(p-1, q-1)$ is the **Carmichael lambda function**. Output the public key $\mathsf{pk} = (N, e)$ and the private key $\mathsf{sk} = (N, d)$.
Renaming p and q, if necessary, we may assume that $p < q$. Then $p < q < 2p$ and so $\sqrt{N/2} < p < \sqrt{N}$.

In textbooks, the message space and ciphertext space are usually taken to be $\mathsf{C}_\kappa = \mathsf{M}_\kappa = (\mathbb{Z}/N\mathbb{Z})^*$, but it fits Definition 1.3.1 better (and is good training) to define them to be $\mathsf{C}_\kappa = \{0,1\}^\kappa$ and $\mathsf{M}_\kappa = \{0,1\}^{\kappa-2}$ or $\{0,1\}^{\kappa-1}$.

Encrypt($\mathsf{m}, (N, e)$): Assume that $\mathsf{m} \in \mathsf{M}_\kappa$.

- Compute $\mathsf{c} = \mathsf{m}^e \pmod{N}$ (see later for padding schemes).
- Return the ciphertext c.

Decrypt($\mathsf{c}, (N, d)$): Compute $\mathsf{m} = \mathsf{c}^d \pmod{N}$ and output either m, or $\perp$ if $\mathsf{m} \notin \mathsf{M}_\kappa$.

Sign($\mathsf{m}, (N, d)$): Compute $\mathsf{s} = \mathsf{m}^d \pmod{N}$.

Verify($\mathsf{m}, \mathsf{s}, (N, e)$): Check whether $\mathsf{m} \equiv \mathsf{s}^e \pmod{N}$.

Figure 24.1: Textbook RSA Public Key Encryption and Signature Schemes.

it. More elaborate padding schemes will be described in Section 24.7.2.

Exercise 24.1.1. Give a KeyGen algorithm that takes as input a security parameter κ (assumed to be even) and an l-bit string u (where $l < \kappa/2$) and outputs a κ-bit product $N = pq$ of two $\kappa/2$-bit primes such that the l most significant bits of N are equal to u. In particular, one can ensure that $2^{\kappa-1} < N < 2^{\kappa}$ and so N is a κ-bit integer.

Exercise 24.1.2. Let $N \in \mathbb{N}$. Prove that the Carmichael function $\lambda(N)$ divides the Euler function $\varphi(N)$. Prove that RSA decryption does return the message.

An odd prime p is a **safe prime** (or **Sophie-Germain prime**) if $(p-1)/2$ is also prime (see Exercise 12.2.10). For certain applications it is necessary to restrict to RSA moduli that are products of safe primes (usually so that $(\mathbb{Z}/N\mathbb{Z})^*$ has no elements of small order, except for order 2). It is conjectured that there is some constant $c > 0$ such that, for all sufficiently large $k \in \mathbb{N}$, there are at least $c2^k/k^2$ safe primes p such that $2^{k-1} < p < 2^k$.

Exercise 24.1.3. Once upon a time it was thought to be necessary to insist that p and q be strong primes for RSA.[1] A prime p is a **strong prime** if $p-1$ and $p+1$ have large prime factors r_1 and r_2 respectively, and $r_1 - 1$ has a large prime factor r_3. It is conjectured that there are infinitely many strong primes. Give an algorithm that takes as input integers k, k_1, k_2, k_3 such that $k_3 < k_1 < k$ and $k_2 < k$ and generates a k-bit strong prime p such that each prime r_i as above has k_i bits.

[1] This was so that $N = pq$ would not succumb to certain special purpose factoring algorithms. Nowadays it is realised that if p and q are chosen uniformly at random then no special purpose factoring algorithm will be successful with noticeable probability and so it is unnecessary to test for special cases.

24.1.1 Efficient Implementation of RSA

As we have seen in Section 12.2, $\kappa/2$-bit probable primes can be found in expected time of $O(\kappa^5)$ bit operations (or $O(\kappa^{4+o(1)})$ using fast arithmetic). One can make this provable using the AKS method, with asymptotic complexity $O(\kappa^{5+o(1)})$ bit operations using fast arithmetic. In any case, RSA key generation is polynomial-time. A more serious challenge is to ensure that encryption and decryption (equivalently, signing and verification) are as fast as possible.

Encryption and decryption are exponentiation modulo N and thus require $O(\log(N)M(\log(N)))$ bit operations, which is polynomial-time. For current RSA key sizes, Karatsuba multiplication is most appropriate, hence one should assume that $M(\log(N)) = \log(N)^{1.58}$. Many of the techniques mentioned in earlier chapters to speed up exponentiation can be used in RSA, particularly sliding window methods. Since e and d are fixed one can also pre-compute addition chains to minimise the cost of exponentiation.

In practice the following two improvements are almost always used.

- **Small public exponents** e (also called **low-exponent RSA**). Traditionally $e = 3$ was proposed, but these days $e = 65537 = 2^{16} + 1$ is most common. Encryption requires only 16 modular squarings and a modular multiplication.
- Use the Chinese remainder theorem (CRT) to decrypt.[2] Let $d_p \equiv e^{-1} \pmod{p-1}$ and $d_q \equiv e^{-1} \pmod{q-1}$. These are called the **CRT private exponents**. Given a ciphertext c one computes $\mathsf{m}_p = \mathsf{c}^{d_p} \pmod{p}$ and $\mathsf{m}_q = \mathsf{c}^{d_q} \pmod{q}$. The message m is then computed using the Chinese remainder theorem (it is convenient to use the method of Exercise 2.6.3 for the CRT).

  For this system the private key is then $\mathsf{sk} = (p, q, d_p, d_q)$. If we denote by $T = c\log(N)M(\log(N))$ the cost of a single exponentiation modulo N to a power $d \approx N$ then the cost using the Chinese remainder theorem is approximately $2c(\log(N)/2)M(\log(N)/2)$ (this is assuming the cost of the Chinese remaindering is negligible). When using Karatsuba multiplication this speeds up RSA decryption by a factor of approximately 3 (in other words, the new running time is a third of the old running time).

24.1.2 Variants of RSA

There has been significant effort devoted to finding more efficient variants of the RSA cryptosystem. We briefly mention some of these now.

Example 24.1.4. (**Multiprime-RSA**[3]) Let $p_1, \ldots, p_k$ be primes of approximately κ/k bits and let $N = p_1 \cdots p_k$. One can use N as a public modulus for the RSA cryptosystem. Using the Chinese remainder theorem for decryption has cost roughly the same as k exponentiations to powers of bit-length κ/k and modulo primes of bit-length κ/k. Hence, the speedup is roughly by a factor $k/k^{2.58} = 1/k^{1.58}$.

To put this in context, going from a single exponentiation to using the Chinese remainder theorem in the case of 2 primes gave a speedup by a factor of 3. Using 3 primes gives an overall speedup by a factor of roughly 5.7, which is a further speedup of a factor 1.9 over the 2-prime case. Using 4 primes gives an overall speedup of about 8.9, which is an additional speedup over 3 primes by a factor 1.6.

However, there is a limit to how large k can be, as the complexity of the elliptic curve factoring method mainly depends on the size of the smallest factor of N.

[2] This idea is often credited to Quisquater and Couvreur [493] but it also appears in Rabin [494].
[3] This idea was proposed (and patented) by Collins, Hopkins, Langford and Sabin.

Exercise 24.1.5. (Tunable balancing of RSA) An alternative approach is to construct the public key $(N = pq, e)$ so that the Chinese remainder decryption exponents are relatively short. The security of this system will be discussed in Section 24.5.2.

Let κ, n_e, n_d be the desired bit-lengths of N, e and $d \pmod{p-1}, d \pmod{q-1}$. Assume that $n_e + n_d > \kappa/2$. Give an algorithm to generate primes p and q of bit-length $\kappa/2$, integers d_p and d_q of bit-length n_d and an integer e of bit-length n_e such that $ed_p \equiv 1 \pmod{p-1}$ and $ed_q \equiv 1 \pmod{q-1}$.

The fastest variant of RSA is due to Takagi and uses moduli of the form $N = p^r q$. For some discussion about factoring such integers see Section 19.4.3.

Example 24.1.6. (**Takagi-RSA** [599]) Let $N = p^r q$ where p and q are primes and $r > 1$. Suppose the public exponent e in RSA is small. One can compute $\mathsf{c}^d \pmod{N}$ as follows. Let $d_p \equiv d \pmod{p-1}$ and $d_q \equiv d \pmod{q-1}$. One first computes $\mathsf{m}_p = \mathsf{c}^{d_p} \pmod{p}$ and $\mathsf{m}_q = \mathsf{c}^{d_q} \pmod{q}$.

To determine $\mathsf{m} \pmod{p^r}$ one uses Hensel lifting. If we have determined $\mathsf{m}_i = \mathsf{m} \pmod{p^i}$ such that $\mathsf{m}_i^e \equiv \mathsf{c} \pmod{p^i}$ then we lift to a solution modulo p^{i+1} by writing $\mathsf{m}_{i+1} = \mathsf{m}_i + xp^i$, where x is a variable. Then

$$\mathsf{m}_{i+1}^e = (\mathsf{m}_i + xp^i)^e \equiv \mathsf{m}_i^e + x(e\mathsf{m}_i^{e-1})p^i \equiv \mathsf{c} \pmod{p^{i+1}} \tag{24.1}$$

gives a linear equation in x modulo p. Note that computing $\mathsf{m}_i^e \pmod{p^{i+1}}$ in equation (24.1) is only efficient when e is small. If e is large then the Hensel lifting stage is no faster than just computing $\mathsf{c}^{e^{-1} \pmod{\varphi(p^r)}} \pmod{p^r}$ directly.

The total cost is two "full" exponentiations to compute m_p and m_q, $r-1$ executions of the Hensel lifting stage, plus one execution of the Chinese remainder theorem. Ignoring everything except the two big exponentiations one has an algorithm whose cost is $2/(r+1)^{2.58}$ times faster than naive textbook RSA decryption. Taking $r = 2$ this is about 9 times faster than standard RSA (i.e., about 1.6 times faster than using 3-prime RSA) and taking $r = 3$ is about 18 times faster than standard RSA (i.e., about 2 times faster than using 4-prime RSA).

Exercise 24.1.7. Let $N = (2^{20}+7)^3(2^{19}+21)$ and let $\mathsf{c} = 474776119073176490663504$ be the RSA encryption of a message m using public exponent $e = 3$. Determine the message using the Takagi decryption algorithm.

Exercise 24.1.8. Describe and analyse the RSA cryptosystem using moduli of the form $N = p^r q^s$. Explain why it is necessary that $r \neq s$.

Exercise 24.1.9. Write pseudocode for Takagi-RSA decryption.

Exercise 24.1.10. (Shamir's RSA for paranoids [548]) Let $N = pq$ where q is much larger than p (for example, $p \approx 2^{500}$ and $q \approx 2^{4500}$). The assumption is that factoring numbers of this form is much harder than factoring $N = pq$ where $p, q \approx 2^{500}$. Suppose one is encrypting a (padded) message m such that $1 \leq \mathsf{m} < p$ and suppose we use public exponent $e > 2\log_2(N)/\log_2(p)$ (so that, typically, $\mathsf{m}^e \approx N^2$). Encryption is computing $\mathsf{c} = \mathsf{m}^e \pmod{N}$ as usual. Shamir's observation is that one can decrypt by computing $\mathsf{m} = \mathsf{c}^{d_p} \pmod{p}$ where $ed_p \equiv 1 \pmod{p-1}$.

How much faster is this than RSA decryption using CRT with a 5000-bit modulus if the primes have equal size? If no padding scheme is used (i.e., every $1 \leq \mathsf{m} < p$ is a valid message) give an adaptive (CCA1) attack on this scheme that yields the factorisation of a user's modulus.

24.1.3 Security of Textbook RSA

We have presented "textbook" RSA above. This is unsuitable for practical applications for many reasons. In practice, RSA should only be used with a secure randomised padding scheme. Nevertheless, it is instructive to consider the security of textbook RSA with respect to the security definitions presented earlier.

Exercise 1.3.4 showed that textbook RSA encryption does not have OWE-CCA security and Exercise 1.3.9 showed that textbook RSA signatures do not have existential forgery security even under a passive attack. We recall one more easy attack.

Exercise 24.1.11. Show that one can use the Jacobi symbol to attack the IND-CPA security of RSA encryption.

Despite the fact that RSA is supposed to be related to factoring, the security actually relies on the following computational problem.

Definition 24.1.12. Let N, e be such that $\gcd(e, \lambda(N)) = 1$. The **RSA problem** (also called the **e-th roots problem**) is: Given $y \in (\mathbb{Z}/N\mathbb{Z})^*$ to compute x such that $x^e \equiv y \pmod{N}$.

It is clear that the RSA problem is not harder than factoring.

Lemma 24.1.13. *The OWE-CPA security of textbook RSA is equivalent to the RSA problem.*

Proof: (Sketch) We show that an algorithm to break OWE-CPA security of textbook RSA can be used to build an algorithm to solve the RSA problem. Let A be an adversary against the OWE-CPA security of RSA. Let (N, e, c) be a challenge RSA problem instance. If $1 < \gcd(\mathsf{c}, N) < N$ then split N and solve the RSA problem. Otherwise, call the adversary A on the public key (N, e) and offer the challenge ciphertext c. If A returns the message m then we are done. If A returns $\perp$ (e.g., because the decryption of c does not lie in M_κ) then replace c by $\mathsf{c}r^e \pmod{N}$ for a random $1 < r < N$ and repeat. When $\mathsf{M}_\kappa = \{0,1\}^{\kappa-2}$ then, with probability at least $1/4$, the reduction will succeed, and so one expects to perform 4 trials. The converse is also immediate. □

Exercise 24.1.14. Show that textbook RSA has selective signature forgery under passive attacks if and only if the RSA problem is hard.

One of the major unsolved problems in cryptography is to determine the relationship between the RSA problem and factoring. There is no known reduction of factoring to breaking RSA. Indeed, there is some indirect evidence that breaking RSA with small public exponent e is not as hard as factoring: Boneh and Venkatesan [87] show that an efficient "algebraic reduction"[4] from FACTOR to low-exponent RSA can be converted into an efficient algorithm for factoring. Similarly, Coppersmith [141] shows that some variants of the RSA problem, where e is small and only a small part of an e-th root x is unknown, are easy (see Exercise 19.1.15).

Definition 24.1.15 describes some computational problems underlying the security of RSA. The reader is warned that some of these names are non-standard.

Definition 24.1.15. Let S be a set of integers, for example $S = \mathbb{N}$ or $S = \{pq : p \text{ and } q \text{ are primes such that } p < q < 2p\}$. We call the latter set the **set of RSA moduli**.

[4] We do not give a formal definition. Essentially this is an algorithm that takes as input N, queries an oracle for the RSA problem, and outputs a finite set of short algebraic formulae, one of which splits the integer N.

FACTOR: Given $N \in S$ to compute the list of prime factors of N.

COMPUTE-PHI: Given $N \in S$ to compute $\varphi(N)$.

COMPUTE-LAMBDA: Given $N \in S$ to compute $\lambda(N)$.

RSA-PRIVATE-KEY: Given $(N, e) \in S \times \mathbb{N}$ to output $\perp$ if e is not coprime to $\lambda(N)$, or d such that $ed \equiv 1 \pmod{\lambda(N)}$.

Exercise 24.1.16. Show that RSA $\leq_R$ RSA-PRIVATE-KEY $\leq_R$ COMPUTE-LAMBDA $\leq_R$ FACTOR for integers $N \in \mathbb{N}$.

Exercise 24.1.16 tells us that FACTOR is at least as hard as RSA. A more useful interpretation is that the RSA problem is no harder than factoring. We are interested in the relative difficulty of such problems, as a function of the input size. Lemma 24.1.17 is the main tool for comparing these problems.[5]

Lemma 24.1.17. *Let A be a perfect oracle that takes as input an integer N and outputs a multiple of $\lambda(N)$. Then one can split N in randomised polynomial-time using an expected polynomially many queries to A.*

Proof: Let N be the integer to be factored. We may assume that N is composite, not a prime power, odd and has no very small factors. Let M be the output of the oracle A on N. (Note that the case of non-perfect oracles is not harder: one can easily test whether the output of A is correct by taking a few random integers $1 < a < N$ such that $\gcd(a, N) = 1$ and checking whether $a^M \equiv 1 \pmod{N}$.)

Since N is odd we have that M is even. Write $M = 2^r m$ where m is odd. Now choose uniformly at random an integer $1 < a < N$. Check whether $\gcd(a, N) = 1$. If not then we have split N, otherwise compute $a_0 = a^m \pmod{N}$, $a_1 = a_0^2 \pmod{N}, \ldots, a_r = a^M \pmod{N}$ (this is similar to the Miller-Rabin test; see Section 12.1.2). We know that $a_r = 1$, so either $a_0 = 1$ or else somewhere along the way there is a non-trivial square root x of 1. If $x \neq -1$ then $\gcd(x + 1, N)$ yields a non-trivial factor of N. All computations require a polynomially bounded number of bit operations.

Let p and q be two distinct prime factors of N. Since a is chosen uniformly at random it follows that $\gcd(a, N) > 1$ or $(\frac{a}{p}) = -(\frac{a}{q})$ with probability at least $1/2$. In either case the above process splits N. The expected number of trials to split N is therefore at most 2.

Repeating the above process on each of the factors in turn one can factor N completely. The expected number of iterations is $O(\log(N))$. For a complete anaysis of this reduction see Section 7.7 of Talbot and Welsh [600] or Section 10.6 of Shoup [556]. □

Two special cases of Lemma 24.1.17 are FACTOR $\leq_R$ COMPUTE-LAMBDA and FACTOR $\leq_R$ COMPUTE-PHI. Note that these reductions are randomised and the running time is only an expected value. Coron and May [151] showed a deterministic polynomial time reduction FACTOR $\leq_R$ RSA-PRIVATE-KEY (also see Section 4.6 of [411]).

Exercise 24.1.18. Restricting attention to integers of the form $N = pq$ where p and q are distinct primes, show that FACTOR $\leq_R$ RSA-PRIVATE KEY.

Exercise 24.1.19. Give a more direct (and deterministic) reduction of FACTOR to COMPUTE-PHI for integers of the form $N = pq$ where p and q are distinct primes.

[5]The original RSA paper credits this result to G. Miller.

Exercise 24.1.20.★ Suppose one has a perfect oracle A that takes as input pairs (N, g), where N is an RSA modulus and g is uniformly chosen in $(\mathbb{Z}/N\mathbb{Z})^*$, and returns the order of g modulo N. Show how to use A to factor an RSA modulus N in expected polynomial-time.

Exercise 24.1.21. The **STRONG-RSA** problem is: Given an RSA modulus N and $y \in \mathbb{N}$ to find any pair (x, e) of integers such that $e > 1$ and

$$x^e \equiv y \pmod{N}.$$

Give a reduction from STRONG-RSA to RSA. This shows that the STRONG-RSA problem is not harder than the RSA problem.[6]

We end with some cryptanalysis exercises.

Exercise 24.1.22. Let $N = pq$ be an RSA modulus. Let A be an oracle that takes as input an integer a and returns $a \pmod{\varphi(N)}$. Show how to use A to factor N.

An interesting question is to study the bit security of RSA. More precisely, if (N, e) is an RSA public key one considers an (not necessarily perfect) oracle which computes the least significant bit of x given $y = x^e \pmod{N}$. It can be shown that if one has such an oracle then one can compute x. One approach is to use the binary Euclid algorithm; due to lack of space we simply refer to Alexi, Chor, Goldreich and Schnorr [9] for details of the method and a comprehensive list of references. A simpler approach, which does not use the binary Euclid algorithm, was given by Fischlin and Schnorr [203]. A complete analysis of the security of any bit (not just the least significant bit) was completed by Håstad and Näslund [279].

Exercise 24.1.23. Consider the following variant of RSA encryption. Alice has a public key N and two public exponents e_1, e_2 such that $e_1 \neq e_2$ and $\gcd(e_i, \lambda(N)) = 1$ for $i = 1, 2$. To encrypt to Alice one is supposed to send $\mathsf{c}_1 = \mathsf{m}^{e_1} \pmod{N}$ and $\mathsf{c}_2 = \mathsf{m}^{e_2} \pmod{N}$. Show that if $\gcd(e_1, e_2) = 1$ then an attacker can determine the message given the public key and a ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$.

Exercise 24.1.24. Consider the following signature scheme based on RSA. The public key is an integer $N = pq$, an integer e coprime to $\lambda(N)$ and an integer a such that $\gcd(a, N) = 1$. The private key is the inverse of e modulo $\lambda(N)$, as usual. Let H be a collision-resistant hash function. The signature on a message m is an integer s such that

$$\mathsf{s}^e \equiv a^{H(\mathsf{m})} \pmod{N}$$

where $H(\mathsf{m})$ is interpreted as an integer. Explain how the signer can generate signatures efficiently. Find a known message attack on this system that allows an adversary to make selective forgery of signatures.

24.2 The Textbook Rabin Cryptosystem

The textbook Rabin cryptosystem [494] is given in Figure 24.2. Rabin is essentially RSA with the optimal choice of e, namely $e = 2$.[7] As we will see, the security of Rabin is

[6] The word "strong" is supposed to indicate that the *assumption* that STRONG-RSA is hard is a *stronger assumption* than the assumption that RSA is hard. Of course, the computational problem is weaker than RSA, in the sense that it might be easier to solve STRONG-RSA than RSA.

[7] The original paper [494] proposed encryption as $E_{N,b}(x) = x(x + b) \pmod{N}$ for some integer b. However, there is a gain in efficiency with no loss of security by taking $b = 0$.

more closely related to factoring than RSA. We first have to deal with the problem that if $N = pq$ where p and q are distinct primes then squaring is a four-to-one map (in general) so it is necessary to have a rule to choose the correct solution in decryption.

Lemma 24.2.1. *Suppose p and q are primes such that $p \equiv q \equiv 3 \pmod 4$. Let $N = pq$ and $1 < x < N$ be such that $(\frac{x}{N}) = 1$. Then either x or $N - x$ is a square modulo N.*

Exercise 24.2.2. Prove Lemma 24.2.1.

Definition 24.2.3. Let $p \equiv q \equiv 3 \pmod 4$ be primes. Then $N = pq$ is called a **Blum integer**.

KeyGen(κ): Generate two random $\kappa/2$-bit primes p and q such that $p \equiv q \equiv 3 \pmod 4$ and set $N = pq$. Output the public key $\mathsf{pk} = N$ and the private key $\mathsf{sk} = (p, q)$.

The message space and ciphertext space depend on the redundancy scheme (suppose for the moment that they are $\mathsf{C}_\kappa = \mathsf{M}_\kappa = (\mathbb{Z}/N\mathbb{Z})^*$).

Encrypt(m, N): Compute $\mathsf{c} = \mathsf{m}^2 \pmod N$ (with some redundancy or padding scheme).

Decrypt($\mathsf{c}, (p, q)$): We want to compute $\sqrt{\mathsf{c}} \pmod N$, and this is done by the following method: Compute $\mathsf{m}_p = \mathsf{c}^{(p+1)/4} \pmod p$ and $\mathsf{m}_q = \mathsf{c}^{(q+1)/4} \pmod q$ (see Section 2.9). Test that $\mathsf{m}_p^2 \equiv \mathsf{c} \pmod p$ and $\mathsf{m}_q^2 \equiv \mathsf{c} \pmod q$, and if not then output $\perp$. Use the Chinese remainder theorem (Exercise 2.6.3) to obtain four possibilities for $\mathsf{m} \pmod N$ such that $\mathsf{m} \equiv \pm\mathsf{m}_p \pmod p$ and $\mathsf{m} \equiv \pm\mathsf{m}_q \pmod q$. Use the redundancy (see later) to determine the correct value m and return $\perp$ if there is no such value.

Sign($\mathsf{m}, (p, q)$): Ensure that $(\frac{\mathsf{m}}{N}) = 1$ (possibly by adding some randomness). Then either m or $N - \mathsf{m}$ is a square modulo N. Compute $\mathsf{s} = \sqrt{\pm\mathsf{m}} \pmod N$ by computing $(\pm\mathsf{m})^{(p+1)/4} \pmod p$, $(\pm\mathsf{m})^{(q+1)/4} \pmod q$ and applying the Chinese remainder theorem.

Verify($\mathsf{m}, \mathsf{s}, N$): Check whether $\mathsf{m} \equiv \pm\mathsf{s}^2 \pmod N$.

Figure 24.2: Textbook Rabin.

Note that, as with RSA, the value m in encryption is actually a symmetric key (passed through a padding scheme) while in signing it is a hash of the message. The choice of $p, q \equiv 3 \pmod 4$ is to simplify the taking of square roots (and is also used in the redundancy schemes below); the Rabin scheme can be used with other moduli.

24.2.1 Redundancy Schemes for Unique Decryption

To ensure that decryption returns the correct message it is necessary to have some redundancy in the message, or else to send some extra bits. We now describe three solutions to this problem.

- **Redundancy in the message for Rabin**: For example, insist that the least significant l bits (where $l > 2$ is some known parameter) of the binary string m are all ones. (Note 8.14 of [418] suggests repeating the last l bits of the message.) If l is big enough then it is unlikely that two different choices of square root would have the right pattern in the l bits.

A message m is encoded as $x = 2^l\mathsf{m} + (2^l - 1)$, and so the message space is $\mathsf{M}_\kappa = \{\mathsf{m} : 1 \leq \mathsf{m} < N/2^l, \gcd(N, 2^l\mathsf{m} + (2^l - 1)) = 1\}$ (alternatively, $\mathsf{M}_\kappa = \{0,1\}^{\kappa-l-2}$). The ciphertext is $\mathsf{c} = x^2 \pmod N$. Decryption involves computing the four square roots of c. If none, or more than one, of the roots has all l least significant bits equal to one and so corresponds to an element of M_κ then decryption fails (return $\perp$). Otherwise output the message $\mathsf{m} = \lfloor x/2^l \rfloor$.

This method is a natural choice, since some padding schemes for CCA security (such as OAEP) already have sections of the message with a fixed pattern of bits.

Note that, since N is odd, the least significant bit of $N - x$ is different to the least significant bit of x. Hence, the $l \geq 1$ least significant bits of x and $N - x$ are never equal. Treating the other two square roots of $x^2 \pmod N$ as random integers it is natural to conjecture that the probability that either of them has a specific pattern of their l least significant bits is roughly $2/2^l$. This conjecture is confirmed by experimental evidence. Hence, the probability of decryption failure is approximately $1/2^{l-1}$.

- **Extra bits for Rabin**: Send two extra bits of information to specify the square root. For example, one could send the value $b_1 = (\frac{\mathsf{m}}{N})$ of the Jacobi symbol (the set $\{-1, 1\}$ can be encoded as a bit under the map $x \mapsto (x+1)/2$), together with the least significant bit b_2 of the message. The ciphertext space is now $\mathsf{C}_\kappa = (\mathbb{Z}/N\mathbb{Z})^* \times \{0,1\}^2$ and, for simplicity of exposition, we take $\mathsf{M}_\kappa = (\mathbb{Z}/N\mathbb{Z})^*$.

  These two bits allow unique decryption, since $(\frac{-1}{N}) = 1$, m and $N - \mathsf{m}$ have the same Jacobi symbol, and if m is odd then $N - \mathsf{m}$ is even.

  Indeed, when using the Chinese remainder theorem to compute square roots then one computes m_p and m_q such that $(\frac{\mathsf{m}_p}{p}) = (\frac{\mathsf{m}_q}{q}) = 1$. Then decryption using the bits b_1, b_2 is: if $b_1 = 1$ then the decryption is $\pm CRT(\mathsf{m}_p, \mathsf{m}_q)$ and if $b_1 = -1$ then solution is $\pm CRT(-\mathsf{m}_p, \mathsf{m}_q)$.

  This scheme is close to optimal in terms of ciphertext expansion (though see Exercise 24.2.6 for an improvement) and decryption never fails. The drawbacks are that the ciphertext contains some information about the message (and so the scheme is not IND-CPA secure), and encryption involves computing the Jacobi symbol, which typically requires far more computational resources than the single squaring modulo N.

- **Williams**: Let $N = pq$ where $p, q \equiv 3 \pmod 4$. If $p \not\equiv \pm q \pmod 8$ then $(\frac{2}{N}) = -1$. Hence, for every $1 \leq x < N$ exactly one of x, $N - x$, $2x$, $N - 2x$ is a square modulo N (see Exercise 24.6.3). Without loss of generality we therefore assume that $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$. The integer N is called a **Williams integer** in this situation.

  Williams [633] suggests encoding a message $1 \leq \mathsf{m} < N/8 - 1$ (alternatively, $\mathsf{m} \in \mathsf{M}_\kappa = \{0,1\}^{\kappa-5}$) as an integer x such that x is even and $(\frac{x}{N}) = 1$ (and so x or $-x$ is a square modulo N) by

$$x = P(\mathsf{m}) = \begin{cases} 4(2\mathsf{m}+1) & \text{if } (\frac{2\mathsf{m}+1}{N}) = 1, \\ 2(2\mathsf{m}+1) & \text{if } (\frac{2\mathsf{m}+1}{N}) = -1 \end{cases}$$

  The encryption of m is then $\mathsf{c} = P(\mathsf{m})^2 \pmod N$. One has $\mathsf{C}_\kappa = (\mathbb{Z}/N\mathbb{Z})^*$.

  To decrypt one computes square roots to obtain the unique even integer $1 < x < N$ such that $(\frac{x}{N}) = 1$ and $x^2 \equiv \mathsf{c} \pmod N$. If $8 \mid x$ then decryption fails (return $\perp$). Otherwise, return $\mathsf{m} = (x/2 - 1)/2$ if $x \equiv 2 \pmod 4$ and $\mathsf{m} = (x/4 - 1)/2$ if $x \equiv 0 \pmod 4$.

Unlike the extra bits scheme, this does not reveal information about the ciphertext. It is almost optimal from the point of view of ciphertext expansion. But it still requires the encrypter to compute a Jacobi symbol (hence losing the performance advantage of Rabin over RSA). The Rabin cryptosystem with the Williams padding is sometimes called the **Rabin-Williams cryptosystem**.

Exercise 24.2.4. Prove all the unproved claims in the above discussion of the Williams redundancy scheme.

Exercise 24.2.5. Let $N = (2^{59} + 21)(2^{20} + 7)$. The three ciphertexts below are Rabin encryptions for each of the three redundancy schemes above (in the first case, $l = 5$). Determine the corresponding message in each case.

$$273067682422\,, \quad (309135051204, -1, 0)\,, \quad 17521752799.$$

Exercise 24.2.6. (Freeman-Goldreich-Kiltz-Rosen-Segev [211]) Let N be a Williams integer. This is a variant of the "extra bits" method. Let $u_1 = -1$ and $u_2 = 2$. To encrypt message $\mathsf{m} \in (\mathbb{Z}/N\mathbb{Z})^*$ one first determines the bits b_1 and b_2 of the "extra bits" redundancy scheme (i.e., $b_1 = 1$ if and only if $(\frac{\mathsf{m}}{N}) = +1$ and b_2 is the least significant bit of m). Compute the ciphertext

$$\mathsf{c} = \mathsf{m}^2 u_1^{1-b_1} u_2^{b_2} \pmod{N}.$$

Show how a user who knows p and q can decrypt the ciphertext. Show that this scheme still leaks the least significant bit of m (and hence is still not IND-CPA secure), but no longer leaks $(\frac{\mathsf{m}}{N})$.

24.2.2 Variants of Rabin

In terms of computational performance, Rabin encryption is extremely fast (as long as encryption does not require computing a Jacobi symbol) while decryption, using the Chinese remainder theorem, is roughly the same speed as RSA decryption.

Exercise 24.2.7. Describe and analyse the Rabin cryptosystem using moduli of the form $N = pqr$ where p, q and r are distinct primes. What are the advantages and disadvantages of Rabin in this setting?

Exercise 24.2.8. (Takagi-Rabin) Describe and analyse the Rabin cryptosystem using moduli of the form $N = p^r q^s$ $(r \neq s)$. Is there any advantage from using Rabin in this setting?

We now discuss compression of Rabin signatures. For further discussion of these ideas, and an alternative method, see Gentry [252].

Example 24.2.9. (Bleichenbacher [68]) Suppose s is a Rabin signature on a message m, so that $\mathsf{s}^2 \equiv \pm H(\mathsf{m}) \pmod{N}$. To compress s to half the size one uses the Euclidean algorithm on (s, N) to compute a sequence of values $r_i, u_i, v_i \in \mathbb{Z}$ such that $r_i = u_i\mathsf{s} + v_i N$. Let i be the index such that $|r_i| < \sqrt{N} < |r_{i-1}|$. Then $r_i \equiv u_i \mathsf{s} \pmod{N}$ and so

$$r_i^2 \equiv u_i^2 \mathsf{s}^2 \equiv \pm u_i^2 H(\mathsf{m}) \pmod{N}.$$

One can therefore send u_i as the signature. Verification is to compute $w = \pm u_i^2 H(\mathsf{m}) \pmod{N}$ and check that w is a perfect square in $\mathbb{Z}$ (e.g., using the method of Exercise 2.4.9 or Exercise 2.2.8). Part 6 of Lemma 2.3.3 states $|r_{i-1}u_i| \leq N$ and so $|u_i| < \sqrt{N}$. Hence, this approach compresses the signature to half the size.

Example 24.2.10. (Bernstein; Coron and Naccache) Another way to compress Rabin signatures is to send the top half of the bits of s. In other words, the signature is $\mathsf{s}' = \lfloor \mathsf{s}/2^{\kappa/2} \rfloor$ if $N < 2^\kappa$. To verify s' one uses Coppersmith's method to find the small solution x to the equation

$$(\mathsf{s}'2^{\kappa/2} + x)^2 \pm H(\mathsf{m}) \equiv 0 \pmod{N}.$$

Verification of this signature is much slower than the method of Example 24.2.9.

24.2.3 Security of Textbook Rabin

Since the Rabin cryptosystem involves squaring it is natural to assume the security is related to computing square roots modulo N, which in turn is equivalent to factoring. Hence, an important feature of Rabin compared with RSA is that the hardness of breaking Rabin can be shown to be equivalent to factoring.

Definition 24.2.11. Let $S = \mathbb{N}$ or $S = \{pq : p, q \equiv 3 \pmod 4, \text{ primes}\}$. The computational problem **SQRT-MOD-N** is: Given $N \in S$ and $y \in \mathbb{Z}/N\mathbb{Z}$ to output $\perp$ if y is not a square modulo N, or a solution x to $x^2 \equiv y \pmod N$.

Lemma 24.2.12. *SQRT-MOD-N is equivalent to FACTOR.*

Proof: Suppose we have a FACTOR oracle and are given a pair (N, y). Then one can use the oracle to factor N and then solve SQRT-MOD-N using square roots modulo p and Hensel lifting and the Chinese remainder theorem. This reduction is polynomial-time.

Conversely, suppose we have a SQRT-MOD-N oracle A and let N be given. First, if $N = p^e$ then we can factor N in polynomial time (see Exercise 2.2.9). Hence we may now assume that N has at least two distinct prime factors.

Choose a random $x \in \mathbb{Z}_N^*$ and set $y = x^2 \pmod N$. Call A on y to get x'. We have $x^2 \equiv (x')^2 \pmod N$ and there are at least four possible solutions x'. All but two of these solutions will give a non-trivial value of $\gcd(x - x', N)$. Hence, since x was chosen randomly, there is probability at least $1/2$ that we can split N. Repeating this process splits N (the expected number of trials is at most 2). As in Lemma 24.1.17 one can repeat the process to factor N in $O(\log(N))$ iterations. The entire reduction is therefore polynomial-time. □

An important remark about the above proof is that the oracle A is not assumed to output a random square root x' of y. Indeed, A could be deterministic. The randomness comes from the choice of x in the reduction.

Exercise 24.2.13. Consider the computational problem FOURTH-ROOT: Given $y \in \mathbb{Z}_N^*$ compute a solution to $x^4 \equiv y \pmod N$ if such a solution exists. Give reductions that show that FOURTH-ROOT is equivalent to FACTOR in the case $N = pq$ with p, q distinct odd primes.

It is intuitively clear that any algorithm that breaks the one-way encryption property (or selective signature forgery) of Rabin under passive attacks must compute square roots modulo N. We have seen that SQRT-MOD-N is equivalent to FACTOR. Thus we expect breaking Rabin under passive atacks to be as hard as factoring. However, giving a precise security proof involves taking care of the redundancy scheme.

Theorem 24.2.14. *Let $N = pq$, where $p \equiv q \equiv 3 \pmod 4$ are primes, and define $S_{N,l} = \{1 \leq x < N : \gcd(x, N) = 1, 2^l \mid (x + 1)\}$. Assume the probability, over $x \in \mathbb{Z}_N^* - S_{N,l}$, that there exists $y \in S_{N,l}$ with $x \neq y$ but $x^2 \equiv y^2 \pmod N$, is $1/2^{l-1}$. Then breaking*

the one-way encryption security property of the Rabin cryptosystem with the "redundancy in the message" redundancy scheme where $l = O(\log(\log(N)))$ under passive attacks is equivalent to factoring Blum integers.

Theorem 24.2.15. *Breaking the one-way encryption security property of the Rabin cryptosystem with the "extra bits" redundancy scheme under passive attacks is equivalent to factoring products $N = pq$ of primes $p \equiv q \equiv 3 \pmod 4$.*

Theorem 24.2.16. *Breaking the one-way encryption security property of the Rabin cryptosystem with the Williams redundancy scheme under passive attacks is equivalent to factoring products $N = pq$ of primes $p \equiv q \equiv 3 \pmod 4$, $p \not\equiv \pm q \pmod 8$.*

Note that Theorem 24.2.14 gives a strong security guarantee when l is small, but in that case decryption failures are frequent. Indeed, there is no choice of l for the Rabin scheme with redundancy in the message that provides both a tight reduction to factoring and negligible probability of decryption failure.

We prove the first and third of these theorems and leave Theorem 24.2.15 as an exercise.

Proof: (Theorem 24.2.14) Let A be an oracle that takes a Rabin public key N and a ciphertext c (with respect to the "redundancy in the message" padding scheme) and returns either the corresponding message m or an invalid ciphertext symbol $\perp$.

Choose a random $x \in \mathbb{Z}_N^*$ such that neither x nor $N-x$ satisfy the redundancy scheme (i.e., the l least significant bits are not all 1). Set $\mathsf{c} = x^2 \pmod N$ and call the oracle A on c. The oracle A answers with either a message m or $\perp$.

According to the (heuristic) assumption in the theorem, the probability that exactly one of the two (unknown) square roots of c modulo N has the correct l least significant bits is $2^{-(l-1)}$. If this is the case then calling the oracle A on c will output a value m such that, writing $x' = 2^l\mathsf{m} + (2^l - 1)$, we have $(x')^2 \equiv x^2 \pmod N$ and $x' \not\equiv \pm x \pmod N$. Hence $\gcd(x' - x, N)$ will split N.

We expect to require approximately 2^{l-1} trials before factoring N with this method. Hence, the reduction is polynomial-time if $l = O(\log(\log(N)))$. □

Proof: (Proof of Theorem 24.2.16; following Williams [633]) Let A be an oracle that takes a Rabin public key N and a ciphertext c (with respect to the Williams redundancy scheme) and returns either the corresponding message m or an invalid ciphertext symbol $\perp$.

Choose a random integer x such that $(\frac{x}{N}) = -1$, e.g., let $x = \pm 2z^2 \pmod N$ for random $z \in (\mathbb{Z}/N\mathbb{Z})^*$. Set $\mathsf{c} = x^2 \pmod N$ and call A on (N, c). The oracle computes the unique even integer $1 < x' < N$ such that $(x')^2 \equiv \mathsf{c} \pmod N$ and $(\frac{x'}{N}) = 1$. The oracle then attempts to decode x' to obtain the message. If $8 \nmid x'$ (which happens with probability 3/4) then decoding succeeds and the corresponding message m is output by the oracle. Given m we can recover the value x' as $2(2\mathsf{m}+1)$ or $4(2\mathsf{m}+1)$, depending on the value of $(\frac{2\mathsf{m}+1}{N})$, and then factor N as $\gcd(x' - x, N)$.

If $8 \mid x'$ then the oracle outputs $\perp$ so we compute $\mathsf{c}' = \mathsf{c}2^{-4} \pmod N$ and call the oracle on c'. The even integer x'' computed by the oracle is equal to $x'/4$ and so the above argument may apply. In extremely rare cases one might have to repeat the process $\frac{1}{2}\log_2(N)$ times, but the expected number of trials is constant. □

Exercise 24.2.17. Prove Theorem 24.2.15.

Exercise 24.2.18. Prove Theorem 24.2.14 when the message space is $\{0,1\}^{\kappa-l-2}$.

The above theorems show that the hardness guarantee for the Rabin cryptosystem is often stronger than for the RSA cryptosystem (at least, under passive attacks). Hence

the Rabin cryptosystem is very attractive: it has faster public operations and also has a stronger security guarantee than RSA. On the other hand, the ideas used in the proofs of these theorems can also be used to give adaptive (CCA) attacks on the Rabin scheme that allow the attacker to determine the private key (i.e., the factorisation of the modulus). In comparison, a CCA attack on textbook RSA only decrypts a single message rather than computes the private key.

Example 24.2.19. We describe a CCA attacker giving a total break of Rabin with "redundancy in the message".

As in the proof of Theorem 24.2.14 the adversary chooses a random $x \in \mathbb{Z}_N^*$ such that neither x nor $N-x$ satisfy the redundancy scheme (i.e., the l least significant bits are not all 1). Set $\mathsf{c} = x^2 \pmod N$ and call the decryption oracle on c. The oracle answers with either a message m or $\perp$. Given m one computes x' such that $\gcd(x'-x, N)$ splits N.

Exercise 24.2.20. Give CCA attacks giving a total break of Rabin when using the other two redundancy schemes ("extra bits" and Williams).

As we have seen, the method to prove that Rabin encryption has one-way security under a passive attack is also the method to give a CCA attack on Rabin encryption. It was remarked by Williams [633] that such a phenomenon seems to be inevitable. This remark has been formalised and discussed in detail by Paillier and Villar [477].

Exercise 24.2.21. Generalise Rabin encryption to $N = pq$ where $p \equiv q \equiv 1 \pmod 3$ and encryption is $\mathsf{c} = \mathsf{m}^3 \pmod N$. How can one specify redundancy? Is the security related to factoring in this case?

Exercise 24.2.22. Consider the following public key cryptosystem related to Rabin: A user's public key is a product $N = pq$ where p and q are primes congruent to 3 modulo 4. To encrypt a message $1 < \mathsf{m} < N$ to the user compute and send

$$\mathsf{c}_1 = \mathsf{m}^2 \pmod N \qquad \text{and} \qquad \mathsf{c}_2 = (\mathsf{m}+1)^2 \pmod N.$$

Show that if $x^2 \equiv y^2 \pmod N$ and $(x+1)^2 \equiv (y+1)^2 \pmod N$ then $x \equiv y \pmod N$. Hence show that decryption is well-defined.

Show that this cryptosystem does not have OWE security under a passive attack.

24.2.4 Other Computational Problems Related to Factoring

We now give some other computational problems in algebraic groups modulo N that are related to factoring.

Exercise 24.2.23. Let $N = pq \in \mathbb{N}$ be a product of two large primes $p \equiv q \equiv 3 \pmod 4$ and let $G = \{x^2 : x \in (\mathbb{Z}/N\mathbb{Z})^*\}$. Let A be an oracle for CDH in G (i.e., $A(g, g^a, g^b) = g^{ab}$). Show how to use A to factor N.

Exercise 24.2.24. Let $N = pq$. Show how to factor N when given $M = (p+1)(q+1)$.

More generally, given $N = pq$ and $M = \Phi_k(p)\Phi_k(q)$ one can split N as follows: Write $F_1(x,y) = xy - N$ and $F_2(x,y) = \Phi_k(x)\Phi_k(y) - M$. One then takes the resultant of $F_1(x,y)$ and $F_2(x,y)$ to get a polynomial $G(x)$. Note that $G(x)$ has p as a root, so one can find p by taking real roots of $G(x)$ to high precision.

Exercise 24.2.25. Let $N = pq = 1125907426181141$ and $M = (p^2+p+1)(q^2+q+1) = 1267668742445499725931290297061$. Determine p and q using resultants as above.

Exercise 24.2.26. Let $N = pq$ where $p \equiv q \equiv 1 \pmod 4$ are primes. Recall that the torus $\mathbb{T}_2(\mathbb{Z}/N\mathbb{Z})$ has order $(p+1)(q+1)$. Let $G = \{g^2 : g \in \mathbb{T}_2(\mathbb{Z}/N\mathbb{Z})\}$. Let A be an oracle for CDH in G. Use the method of Exercise 24.2.23 to factor N using A.

Exercise 24.2.27. Let $N = pq$ where p and q are odd primes and let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve. Suppose A is an oracle that, on input $(P, [a]P, [b]P)$, where P has odd order, outputs $[ab]P$ in $\langle P \rangle$. Explain why one can not immediately factor N using this oracle. Consider now an oracle A, taking input $(a_4, a_6, P, [a]P, [b]P)$ where P lies on the elliptic curve $y^2 = x^3 + a_4x + a_6$ modulo N and P has odd order, that outputs $[ab]P$. Show how to use A to factor N.

There are two approaches to using information about $\#E(\mathbb{Z}/N\mathbb{Z})$ to split N. One is more suitable when one has an oracle that computes $\#E(\mathbb{Z}/N\mathbb{Z})$ and the other is more suitable when E is fixed.

Example 24.2.28. (Kunihiro and Koyama [358]) Let $N = pq$ be a product of two primes. Let A be an oracle that takes as input (N, a_4, a_6) and returns $M = \#E(\mathbb{Z}/N\mathbb{Z})$ where $E : y^2 = x^3 + a_4x + a_6$.

Given the oracle A one can split N using exactly the same method as Lemma 24.1.17. First choose a random elliptic curve E together with a point P on it modulo N. Use the oracle A to compute $M = \#E(\mathbb{Z}/N\mathbb{Z})$. Now, find small prime factors l of M (such as $l = 2$) and compute $[M/l]P = (x : y : z)$ in projective coordinates. There is a good chance that l divides both $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$ and that $P \pmod p$ has order divisible by l but $P \pmod q$ does not. Hence, $\gcd(z, N)$ splits N.

Exercise 24.2.29. (Martín Molleví, Morillo and Villar [400]) Use the method of Example 24.2.28 to show how to factor N given an oracle A that takes as input (N, a_4, a_6, x_P, y_P) and returns the order of the point $P = (x_P, y_P) \in E(\mathbb{Z}/N\mathbb{Z})$.

Example 24.2.30. Let $N = pq$ be a product of two primes. Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve modulo N such that E is not supersingular modulo p or q. Let $M = \#E(\mathbb{Z}/N\mathbb{Z})$ be given.

Now choose a random integer $1 \leq x_P < N$. There may not be a point on $E(\mathbb{Z}/N\mathbb{Z})$ with x-coordinate x_P. Indeed, we hope that there is not. Then there is a quadratic twist $E' : uY^2 = X^3 + a_4X + a_6$ of E with a point $P = (x_P, y_P) \in E'(\mathbb{Z}/N\mathbb{Z})$. With probability $1/2$ we have $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$ but $\#E(\mathbb{F}_p) \neq \#E'(\mathbb{F}_p)$ (or vice versa). It is not necessary to compute y_P or to determine E'. Using x-coordinate only arithmetic on E one can compute the projective representation $(x_Q : z_Q)$ for the x-coordinate of $Q = [M](x_P, y_P)$ on E'. Then $\gcd(z_Q, N)$ splits N.

Exercise 24.2.31. Adapt the methods in Examples 24.2.28 and 24.2.30 to give alternative methods to factor $N = pq$ given $\#\mathbb{T}_2(\mathbb{Z}/N\mathbb{Z})$ or $\#\mathbb{T}_6(\mathbb{Z}/N\mathbb{Z})$.

24.3 Homomorphic Encryption

Homomorphic encryption was defined in Section 23.3.1. We first remark that the textbook RSA scheme is homomorphic for multiplication modulo N: If $\mathsf{c}_1 \equiv \mathsf{m}_1^e \pmod N$ and $\mathsf{c}_2 \equiv \mathsf{m}_2^e \pmod N$ then $\mathsf{c}_1\mathsf{c}_2 \equiv (\mathsf{m}_1\mathsf{m}_2)^e \pmod N$. Indeed, this property is behind the CCA attack on textbook RSA encryption. Padding schemes can destroy this homomorphic feature.

Exercise 24.3.1. Show that textbook Rabin encryption is not homomorphic for multiplication when using any of the redundancy schemes of Section 24.2.1.

We now give a scheme that is homomorphic for addition, and that allows a much larger range of values for the message compared with the scheme in Exercise 23.3.5.

Example 24.3.2. (Paillier [474]) Let $N = pq$ be a user's public key. To encrypt a message $\mathsf{m} \in \mathbb{Z}/N\mathbb{Z}$ to the user choose a random integer $1 < u < N$ (note that, with overwhelming probability, $u \in (\mathbb{Z}/N\mathbb{Z})^*$) and compute the ciphertext

$$\mathsf{c} = (1 + N\mathsf{m})u^N \pmod{N^2}.$$

To decrypt compute

$$\mathsf{c}^{\lambda(N)} \equiv 1 + \lambda(N)N\mathsf{m} \pmod{N^2}$$

and hence determine $\mathsf{m} \pmod N$ (this requires multiplication by $\lambda(N)^{-1} \pmod N$).

The homomorphic property is: if c_1 and c_2 are ciphertexts encrypting m_1 and m_2 respectively, then

$$\mathsf{c}_1\mathsf{c}_2 \equiv (1 + N(\mathsf{m}_1 + \mathsf{m}_2))(u_1u_2)^N \pmod{N^2}$$

encrypts $\mathsf{m}_1 + \mathsf{m}_2 \pmod N$.

Exercise 24.3.3. Verify the calculations in Example 24.3.2.

As always, one cannot obtain CCA secure encryption using a homomorphic scheme. Hence, one is only interested in passive attacks. To check whether or not a Paillier ciphertext c corresponds to a specific message m is precisely solving the following computational problem.

Definition 24.3.4. Let $N = pq$. The **composite residuosity problem** is: Given $y \in \mathbb{Z}/N^2\mathbb{Z}$ to determine whether or not $y \equiv u^N \pmod{N^2}$ for some $1 < u < N$.

Exercise 24.3.5. Show that the Paillier encryption scheme has IND-CPA security if and only if the composite residuosity problem is hard.

Exercise 24.3.6. Show that composite residuosity is not harder than factoring.

Exercise 24.3.7. Show how to use the Chinese remainder theorem to speed up Paillier decryption.

Encryption using the Paillier scheme is rather slow, since one needs an exponentiation to the power N modulo N^2. One can use sliding windows for this exponentiation, though since N is fixed one might prefer to use an addition chain optimised for N. Exercises 24.3.8 and 24.3.9 suggest variants with faster encryption. The disadvantage of the scheme in Exercise 24.3.8 is that it requires a different computational assumption. The disadvantage of the scheme in Exercise 24.3.9 is that it is no longer homomorphic.

Exercise 24.3.8.★ Consider the following efficient variant of the Paillier cryptosystem. The public key of a user consists of N and an integer $h = u^N \pmod{N^2}$ where $1 < u < N$ is chosen uniformly at random. To encrypt a message m to the user, choose a random integer $0 \leq x < 2^k$ (e.g., with $k = 256$) and set

$$\mathsf{c} \equiv (1 + N\mathsf{m})h^x \pmod{N^2}.$$

State the computational assumption underlying the IND-CPA security of the scheme. Give an algorithm to break the IND-CPA security that requires $O(2^{k/2})$ multiplications modulo N^2. Use multi-exponentiation to give an even more efficient variant of the Paillier cryptosystem, at the cost of even larger public keys.

Exercise 24.3.9. (Catalano, Gennaro, Howgrave-Graham, Nguyen [125]) A version of the Paillier cryptosystem for which encryption is very efficient is the following: The public key is (N, e) such that $\gcd(e, N\lambda(N)) = 1$. One thinks of e as being small. To encrypt one chooses a random integer $1 < u < N$ and computes

$$\mathsf{c} = (1 + N\mathsf{m})u^e \pmod{N^2}.$$

Decryption begins by performing RSA decryption of c modulo N to obtain u.

Write down the decryption algorithm for this system. Explain why this encryption scheme is no longer homomorphic.

Exercise 24.3.10. Consider the following variant of the Paillier cryptosystem: The public key consists of $N = pq$ and an integer g such that $g^{\lambda(N)} \equiv 1 + N \pmod{N^2}$. To encrypt a message $0 \leq \mathsf{m} < N$ compute $g^{\mathsf{m}}u^N \pmod{N^2}$ where $1 < u < N$ is random.

Give key generation and decryption algorithms for this cryptosystem. Give a chosen ciphertext attack on this cryptosystem that reveals the private key.[8]

Exercise 24.3.11. (Damgård-Jurik [165]) Generalise the Paillier cryptosystem so the message space is $\mathbb{Z}/N^k\mathbb{Z}$. Explain how to decrypt.

Exercise 24.3.12. (Okamoto-Uchiyama [471]) Let $N = p^2q$ where p and q are distinct primes of similar size such that $p \nmid (q-1)$. Choose a random element $1 < u < N$ (note that, with overwhelming probability, $u \in (\mathbb{Z}/N\mathbb{Z})^*$) and set $g = u^N(1-p) \pmod{N}$. The public key of the **Okamoto-Uchiyama scheme** is (N, g). To encrypt a message $\mathsf{m} \in \mathbb{Z}/p\mathbb{Z}$ (in practice, since p is not known, one would assume $0 \leq \mathsf{m} < N^{1/3}$) one chooses a random element $1 < u < N$ and computes

$$\mathsf{c} = g^{\mathsf{m}}u^N \pmod{N}.$$

To decrypt one computes $((\mathsf{c}^{p-1} \pmod{p^2}) - 1)/p$.

Show that $g^{p-1} \equiv 1 + p \pmod{p^2}$ and hence that decryption does compute m. Show that the scheme is homomorphic with respect to addition modulo p. Define the computational problem underlying the IND-CPA security of this scheme.

Show that if one has access to a decryption oracle then one can determine the factorisation of N.

24.4 Algebraic Attacks on Textbook RSA and Rabin

The goal of this section is to briefly describe a number of relatively straightforward attacks on the textbook RSA and Rabin cryptosystems. These attacks can all be prevented if one uses a sufficiently good padding scheme. Indeed, by studying these attacks one develops a better idea of what properties are required of a padding scheme.

24.4.1 The Håstad Attack

We now present an attack that can be mounted on the RSA or Rabin schemes in a multi-user situation. Note that such attacks are not covered by the standard security model for encryption as presented in Chapter 1.

[8] This scheme was proposed by Choi, Choi and Won at ICISC 2001 and an attack was given by Sakurai and Takagi at ACISP 2002.

Example 24.4.1. Suppose three users have RSA public keys N_1, N_2, N_3 and all use encryption exponent $e = 3$. Let $0 < \mathsf{m} < \min\{N_1, N_2, N_3\}$ be a message. If m is encrypted to all three users then an attacker can determine m from the three ciphertexts $\mathsf{c}_1, \mathsf{c}_2$ and c_3 as follows: The attacker uses the Chinese remainder theorem to compute $1 < \mathsf{c} < N_1N_2N_3$ such that $\mathsf{c} \equiv \mathsf{m}^3 \pmod{N_i}$ for $1 \leq i \leq 3$. It follows that $\mathsf{c} = \mathsf{m}^3$ over $\mathbb{Z}$ and so one can determine m using root finding algorithms.

This attack is easily prevented by using randomised padding schemes (assuming that the encryptor is not so lazy that they re-use the same randomness each time). Nevertheless, this attack seems to be one of the reasons why modern systems use $e = 65537 = 2^{16}+1$ instead of $e = 3$.

Exercise 24.4.2. Show that the Håstad attack applies when the same message is sent using textbook Rabin encryption (with any of the three redundancy schemes) to two users.

Exercise 24.4.3. Two users have Rabin public keys $N_1 = 144946313$ and $N_2 = 138951937$. The same message m is encrypted using the "extra bits" padding scheme to the two users, giving ciphertexts

$$C_1 = (48806038, -1, 1) \text{ and } C_2 = (14277753, -1, 1).$$

Use the Håstad attack to find the corresponding message.

24.4.2 Algebraic Attacks

We already discussed a number of easy algebraic attacks on textbook RSA, all of which boil down to exploiting the multiplicative property

$$\mathsf{m}_1^e \mathsf{m}_2^e \equiv (\mathsf{m}_1\mathsf{m}_2)^e \pmod{N}.$$

We also noted that, since textbook RSA is deterministic, it can be attacked by trying all messages. Hence, if one knows that $1 \leq \mathsf{m} < 2^k$ (for example, if m is a k-bit symmetric key) then one can attack the system in at most 2^k exponentiations modulo N. We now show that one can improve this to roughly $\sqrt{2^k}$ exponentiations in many cases.

Exercise 24.4.4. (Boneh, Joux, Nguyen [82]) Suppose $\mathsf{c} = \mathsf{m}^e \pmod{N}$ where $1 \leq \mathsf{m} < 2^k$. Show that if $\mathsf{m} = \mathsf{m}_1\mathsf{m}_2$ for two integers $1 < \mathsf{m}_1, \mathsf{m}_2 < B$ then one can determine m in $O(B)$ exponentiations modulo N. If $B = 2^{k/2+\epsilon}$ then the probability that m splits in this way is noticeable.

24.4.3 Desmedt-Odlyzko Attack

This is a "lunchtime attack", proposed by Desmedt and Odlyzko in [170], on textbook RSA signatures. It can produce more forgeries than calls to the signing oracle. The basic idea is to query the signing oracle on the first r prime numbers $p_1, \ldots, p_r$ to get signatures $\mathsf{s}_1, \ldots, \mathsf{s}_r$. Then, for any message m, if m is a product of powers of the first r primes $\mathsf{m} = \prod_{i=1}^r p_i^{f_i}$ then the corresponding signature is

$$\mathsf{s} = \prod_{i=1}^r \mathsf{s}_i^{f_i}.$$

This attack is not feasible if messages are random elements between 1 and N (as the probability of smoothness is usually negligible) but it can be effective if messages in the system are rather small.

Exercise 24.4.5. Let $N = 9178628368309$ and $e = 7$ be an RSA public key. Suppose one learns that the signatures of 2, 3 and 5 are 872240067492, 6442782604386 and 1813566093366 respectively. Determine the signatures for messages $\mathsf{m} = 6, 15, 12$ and 100.

An analogous attack applies to encryption: Ask for decryptions of the first r primes (treating them as ciphertexts) and then, given a challenge ciphertext c, if $\mathsf{c} \equiv \prod_{i=1}^{r} p_i^{e_i}$ then one can work out the decryption of c. Since ciphertexts (even of small messages) are of size up to N this attack is usually not faster than factoring the modulus.

This idea, together with a number of other techniques, has been used by Coron, Naccache, Tibouchi and Weinmann [153] to attack real-world signature proposals.

24.4.4 Related Message Attacks

This attack is due to Franklin and Reiter.[9] Consider textbook RSA with small exponent e or textbook Rabin ($e = 2$). Suppose we obtain ciphertexts c_1 and c_2 (with respect to the same public key (N, e)) for messages m and $\mathsf{m} + a$ for some known integer a. Then m is a common root modulo N of the two polynomials $F_1(x) = x^e - \mathsf{c}_1$ and $F_2(x) = (x+a)^e - \mathsf{c}_2$ (in the case of Rabin we may have polynomials like $F_1(x) = (2^l(x+1) - 1)^2 - \mathsf{c}_1$ or $F_1(x) = (2(2x+1))^2 - \mathsf{c}_1$). Hence one can run Euclid's algorithm on $F_1(x)$ and $F_2(x)$ in $(\mathbb{Z}/N\mathbb{Z})[x]$ and this will either lead to a factor of N (since performing polynomial division in $(\mathbb{Z}/N\mathbb{Z})[x]$ involves computing inverses modulo N) or will output, with high probability, a linear polynomial $G(x) = x - \mathsf{m}$.

Euclid's algorithm for polynomials of degree e has complexity $O(e^2 M(\log(N)))$ or $O(M(e)\log(e)M(\log(N)))$ bit operations. Hence, this method is feasible only when e is rather small (e.g., $e < 2^{30}$).

Exercise 24.4.6. Extend the Franklin-Reiter attack to ciphertexts c_1 and c_2 (again, for the same public key) where c_1 is an encrypion of m and c_2 is an encryption of $a\mathsf{m} + b$ for known integers a and b.

Exercise 24.4.7. Let $N = 2157212598407$ and $e = 3$. Suppose we have ciphertexts

$$\mathsf{c}_1 = 1429779991932 \quad \text{and} \quad \mathsf{c}_2 = 655688908482$$

such that c_1 is the encryption of m and c_2 is the encryption of $\mathsf{m} + 2^{10}$. Determine the message m.

These ideas have been extended by Coppersmith, Franklin, Patarin and Reiter [144]. Among other things they study how to break related encryptions for any polynomial relation by using resultants (see Exercise 24.4.8).

Exercise 24.4.8. Let (N, e) be an RSA key. Suppose one is given $\mathsf{c}_1 = \mathsf{m}_1^e \pmod N$, $\mathsf{c}_2 = \mathsf{m}_2^e \pmod N$ and a polynomial $P(x, y) \in \mathbb{Z}[x, y]$ such that $P(\mathsf{m}_1, \mathsf{m}_2) \equiv 0 \pmod N$. Let d be a bound on the total degree of $P(x, y)$. Show how to compute m_1 and m_2 in $O((d+e)^3 d^2 M(\log(N)))$ bit operations.

24.4.5 Fixed Pattern RSA Signature Forgery

The aim of this section is to present a simple padding scheme, often called **fixed pattern padding** for RSA. We then sketch why this approach may not be sufficient to obtain RSA signatures secure against adaptive attackers. These ideas originate in the work

[9] The idea was presented at the "rump session" of CRYPTO 1995.

of De Jonge and Chaum and later work by Girault and Misarsky. We present the more recent attacks by Brier, Clavier, Coron and Naccache [106]. An attack on RSA encryption with fixed padding is given in Section 19.4.1.

Example 24.4.9. Suppose we are using moduli of length 3072 bits and that messages (or message digests) m are of length at most 1000 bits.

The padding scheme uses a fixed value $P = 2^{3071}$ and the signature on the message digest m (such that $0 \leq \mathsf{m} < 2^{1000}$) is

$$\mathsf{s} = (P + \mathsf{m})^d \pmod{N}.$$

The verifier computes $\mathsf{s}^e \pmod{N}$ and checks it is of the correct form $P + \mathsf{m}$ with $0 \leq \mathsf{m} < 2^{1000}$.

The following method (from [106]) forges signatures if messages are roughly $N^{1/3}$ in size. We assume that a signing oracle is available (we assume the signing oracle will only generate signatures if the input is correctly padded) and that a hash function is not applied to the messages. Suppose m is the target message, so we want to compute the d-th power of $z = P + \mathsf{m}$. The idea is to find small values u, v, w such that

$$z(z + u) \equiv (z + v)(z + w) \pmod{N}. \tag{24.2}$$

Then given signatures on $\mathsf{m} + u, \mathsf{m} + v$ and $\mathsf{m} + w$ (i.e., d-th powers of $z + u, z + v$ and $z + w$) one can compute the signature on m as required.

To find small solutions to equation (24.2) we expand and simplify to

$$z(u - v - w) \equiv vw \pmod{N}.$$

Running the extended Euclidean algorithm (the basic version rather than the fast version of Algorithm 1) on z and N gives a number of integers s, r such that

$$zs \equiv r \pmod{N} \quad \text{and} \quad |rs| \approx N.$$

One can run Euclid until a solution with $|s| \approx N^{1/3}$ and $|r| \approx N^{2/3}$ is found. One then tries to factor r as a product $r = vw$ of numbers of a similar size. If this is feasible (for example, if r has a large number of small prime factors) then set $u = s + v + w$ and we have a solution. This approach is reasonable as long as the messages are at least one third of the bit-length of the modulus.

Example 24.4.10. Let $N = 1043957 \approx 2^{20}$.

Suppose $P = 2^{19}$ is the fixed padding and suppose messages are restricted to be 10-bit binary strings. Thus

$$z = P + \mathsf{m}$$

where $0 \leq \mathsf{m} < 2^{10}$.

Suppose have access to a signing oracle and would like to forge a signature on the message $\mathsf{m} = 503$ that corresponds to $z = P + 503 = 524791$.

We apply Euclid's algorithm on N and z to solve the congruence $zs \equiv r \pmod{N}$ where $s \approx N^{1/3} \approx 101$.

i	q	r_i	s_i	t_i
-1	–	1043957	1	0
0	–	524791	0	1
1	1	519166	1	-1
2	1	5625	-1	2
3	92	1666	93	-185

This gives the solution $-185z \equiv 1666 \pmod{N}$ and $|-185| \approx N^{1/3}$. So set $s = -185$ and $r = 1666$. We try to factor r and are lucky that $1666 = 2 \cdot 7^2 \cdot 17$. So choose $v = 34$ and $w = 49$. Finally, choose $u = v + w - 185 = -102$. One can check that

$$z(z+u) \equiv (z+v)(z+w) \pmod{N}$$

and that $z+u, z+v$ and $z+w$ are all between P and $P + 2^{10}$. Hence, if one obtains signatures $\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3$ on $\mathsf{m} + u = 401, \mathsf{m} + v = 537$ and $\mathsf{m} + w = 552$ then one has the signature on z as $\mathsf{s}_2\mathsf{s}_3\mathsf{s}_1^{-1} \pmod{N}$.

The success of this attack depends on the cost of factoring r and the probability that it can be written as a product of integers of similar size. Hence, the attack has subexponential complexity. For fixed m the attack may not succeed (since r might not factor as a product of integers of the required size). On the other hand, if m can vary a little (this is now more like an existential forgery) then the attack should succeed. A method for existential forgery that does not require factoring is given in Example 24.4.13.

Exercise 24.4.11. Give a variant of the above attack for the case where messages can be of size $N^{1/2}$ and for which it is only necessary to obtain signatures on two messages.

Exercise 24.4.12. One could consider affine padding $A\mathsf{m} + B$ instead of $P + \mathsf{m}$, where A and B are fixed integers and m is small. Show that, from the point of view of attacks, the two padding schemes are equivalent.

Example 24.4.13. We show sketch the existential forgery from [106]. As before we seek messages $\mathsf{m}_1, \ldots, \mathsf{m}_4$ of size $N^{1/3}$ such that

$$(P + \mathsf{m}_1)(P + \mathsf{m}_2) \equiv (P + \mathsf{m}_3)(P + \mathsf{m}_4) \pmod{N}.$$

Writing $\mathsf{m}_1 = x + t, \mathsf{m}_2 = y + t, \mathsf{m}_3 = t$ and $\mathsf{m}_4 = x + y + z + t$ the equation is seen to be equivalent to $Pz \equiv xy - tz \pmod{N}$. One again uses Euclid to find $s \approx N^{1/3}, r \approx N^{2/3}$ such that $Ps \equiv r \pmod{N}$. One sets $z = s$ and then wants to find x, y, t such that $xy = r + tz$. To do this choose a random integer $N^{1/3} < y < 2N^{1/3}$ such that $\gcd(y, z) = 1$ and set $t \equiv -z^{-1}r \pmod{y}$. One then easily solves for the remaining values and one can check that the m_i are roughly of the right size.

For further details and results we refer to Brier, Clavier, Coron and Naccache [106] and Lenstra and Shparlinski [374].

This idea, together with other techniques, has been used to cryptanalyse the ISO/IEC 9796-1 signature standard with great success. We refer to Coppersmith, Coron, Grieu, Halevi, Jutla, Naccache and Stern [143].

24.4.6 Two Attacks by Bleichenbacher

Example 24.4.14. (Bleichenbacher) Consider a padding scheme for RSA signatures with $e = 3$ that is of the following form.

00 01	FF FF $\cdots$ FF	Special block	$H(\mathsf{m})$

In other words, to verify a signature s one computes $\mathsf{s}^3 \pmod{N}$ and checks if the resulting integer corresponds to a binary string of the above form.

Suppose now that the verification algorithm parses the binary string from the left hand side (most significant bit) and does not check that $H(\mathsf{m})$ sits in the least significant bits (this was the case for some padding schemes in practice). In other words, a signature will verify if $\mathsf{s}^3 \pmod{N}$ is an integer whose binary representation is as follows, where r is any binary string.

00 01	FF FF $\cdots$ FF	Special block	$H(\mathsf{m})$	r

Bleichenbacher noticed that a forger could choose r to ensure that the integer is a cube in $\mathbb{Z}$.

Precisely, suppose $2^{3071} < N < 2^{3072}$, that the "special block" is 0000 (i.e., 32 zero bits), and that H has 256-bit output. Let m be a message such that $H(\mathsf{m}) \equiv 1 \pmod 3$. We want to find r such that

$$y = 2^{3057} - 2^{2360} + H(\mathsf{m})2^{2072} + r$$

is a cube. Note that

$$(2^{1019} - (2^{288} - H(\mathsf{m}))2^{34}/3)^3 = 2^{3057} - 2^{2360} + H(\mathsf{m})2^{2072} + 2^{1087}((2^{288} - H(\mathsf{m}))/3)^2 + z$$

where $|z| < 2^{980}$ and so is of the right form. To find the right value one can take an integer of the form y, take its cube root in $\mathbb{R}$ and then round up to the nearest integer.

Exercise 24.4.15. Compute a signature using the method of example 24.4.14 for the hash value $H(\mathsf{m}) = 4$. Check your answer.

Bleichenbacher has also given a chosen ciphertext attack on RSA encryption when using a fixed padding scheme [67]. More precisely, suppose a message m is padded as in the figure below to form an integer x, and is then encrypted as $\mathsf{c} = x^e \pmod N$.

00 02	non-zero padding string	00	m

Bleichenbacher supposes an attacker has access to an oracle that determines, given an integer c, whether the corresponding e-th root x has binary expansion in this form. Such an oracle is provided by a decryption oracle that either outputs m or $\perp$. Error messages from a server may also provide such an oracle.

We do not have space to give the details. The basic idea is that, given a challenge c, one computes $\mathsf{c}' = \mathsf{c}r^e \pmod N$ for various integers r and determines intervals containing the message according to the error response. The attack eventually reveals the message (after perhaps a million queries to the oracle).

24.5 Attacks on RSA Parameters

In this section we briefly recall some attacks on certain choices of RSA public key.

24.5.1 Wiener Attack on Small Private Exponent RSA

One proposal to speed-up RSA decryption is to choose d to be a small integer. Key generation is performed by first choosing d and then setting $e = d^{-1} \pmod{\lambda(N)}$. This is called **small private exponent RSA**.[10] We present the famous **Wiener attack**, which is a polynomial-time attack on private exponents $d < N^{1/4}$.

Exercise 24.5.1. Give a brute-force attack on small private exponent RSA that tries each odd integer $d > 1$ in turn. What is the complexity of this attack?

[10]The reader should remember that, in practice, it is more efficient to use the Chinese remainder theorem to speed up RSA decryption than small private exponents.

We now sketch Wiener's idea [630]. We assume the key generation of Figure 24.1 is used, so that $N = pq$ where $p < q < 2p$. Consider the equation defining e and d

$$ed = 1 + k\varphi(N)$$

(a similar attack can be mounted using the equation $ed = 1 + k\lambda(N)$, see Exercise 24.5.5). Since $e < \varphi(N)$ we have $k < d$. Now $\varphi(N) = N + 1 - (p + q)$ and $\sqrt{N} \leq (p + q) < 3\sqrt{N}$ so $\varphi(N) = N - u$ where $0 \leq u = p + q - 1 \leq 3\sqrt{N}$. Rearranging gives

$$-ed + kN = (-1 + ku) < 3k\sqrt{N}. \tag{24.3}$$

If d is smaller than $\sqrt{N}/3$ then the right hand side is $< N$. Hence, one could try to find d by running the extended Euclidean algorithm on (e, N) and testing the coefficient of e to see if it is a candidate value for $\pm d$ (e.g., by testing whether $(x^e)^d \equiv x \pmod{N}$ for a random $1 < x < N$). Note that one must use the basic extended Euclidean algorithm rather than the faster variant of Algorithm 1. We now explain that this method is guaranteed to find d when it is sufficiently small.

Theorem 24.5.2. *Let $N = pq$ where $p < q < 2p$ are primes. Let $e = d^{-1} \pmod{\varphi(N)}$ where $0 < d < N^{1/4}/\sqrt{3}$. Then given (N, e) one can compute d in polynomial time.*

Proof: Using the notation above, $(d, k, uk - 1)$ is a solution to equation (24.3) with $0 < k < d$ and $0 \leq u < 3\sqrt{N}$.

The Euclidean algorithm finds all triples (s, t, r) satisfying $es + Nt = r$ with $|sr| < N$ and $|tr| < e$. Hence, if $|d(uk - 1)| < N$ then the required solution will be found. If $0 < d < N^{1/4}/\sqrt{3}$ then

$$|duk| < d^2 u < \frac{N^{1/2}}{3} 3\sqrt{N} = N$$

which completes the proof. □

Example 24.5.3. Let $N = 86063528783122081$ with $d = 8209$. One computes that $e = 14772019882186053$.

One can check that

$$ed = 1 + 1409\varphi(N).$$

Running Euclid's algorithm with $r_{-1} = N$ and $r_0 = e$ and writing s_i, t_i be such that $r_i = s_i N + t_i e$ one finds the following table of values.

i	q	r_i	s_i	t_i
-1	$--$	86063528783122081	1	0
0	$--$	14772019882186053	0	1
1	5	12203429372191816	1	-5
2	1	2568590509994237	-1	6
3	4	1929067332214868	5	-29
4	1	639523177779369	-6	35
5	3	10497798876761	23	-134
6	60	9655245173709	-138	8075
7	1	842553703052	1409	-8209

One sees that d is found in only 7 steps.

Exercise 24.5.4. Consider the RSA public key $(N, e) = (11068562742977, 10543583750987)$. Use the Wiener attack to determine the private key.

Exercise 24.5.5. Show how to perform the Wiener attack when $\varphi(N)$ is replaced by $\lambda(N)$. What is the bound on the size of d for which the attack works?

Exercise 24.5.6. Let $(N, e) = (63875799947551, 4543741325953)$ be an RSA public key where $N = pq$ with $\gcd(p-1, q-1) > 2$ and small private exponent d such that $ed \equiv 1 \pmod{\lambda(N)}$. Use the Wiener attack to find d.

Exercise 24.5.7. Show that one can prevent the Wiener attack by adding a sufficiently large multiple of $\varphi(N)$ to e.

Wiener's result has been extended in several ways. Dujella [184] and Verheul and van Tilborg [621] show how to extend the range of d, while still using Euclid's algorithm. Their algorithms are exponential time. Boneh and Durfee [78] used lattices to extend the attack to $d < N^{0.284}$ and, with significant further work, extended the range to $d < N^{0.292}$. Blömer and May [71] give a simpler formulation of the Boneh-Durfee attack for $d < N^{0.284}$. Some unsuccessful attempts to extend Wiener's method to larger d are discussed by Suk [595] and Bauer [31].

24.5.2 Small CRT Private Exponents

As mentioned in Section 24.1.1, a common way to speed up RSA decryption is to use the Chinese remainder theorem. Indeed, one can choose the CRT private exponents d_p and d_q to be small (subject to $d_p \equiv d_q \pmod{\gcd(p-1, q-1)}$ and define e such that $ed_p \equiv 1 \pmod{p-1}$ and $ed_q \equiv 1 \pmod{q-1}$. Of course, one should take $d_p \neq d_q$, or else one can just apply the Wiener attack. We now show that these values cannot be taken to be too small.

Exercise 24.5.8. Give a brute-force attack on small private CRT exponents.

We now present a "birthday attack", which is attributed to Pinch in [492]. Let d_p be such that $ed_p \equiv 1 \pmod{p-1}$ and $ed_p \not\equiv 1 \pmod{q-1}$. Suppose we know that $1 < d_p < K$ and let $L = \lceil \sqrt{K} \rceil$. Then $d_p = d_0 + Ld_1$ where $0 \leq d_0, d_1 < L$ and, for a random integer $1 < \mathsf{m} < N$ one expects

$$\gcd(\mathsf{m}^{ed_0 - 1}\mathsf{m}^{Led_1} - 1, N) = p.$$

The problem is to detect this match. The idea is to use the method of Section 2.16 for evaluating polynomials. So, define

$$G(x) = \prod_{j=0}^{L-1} (\mathsf{m}^{ej-1}x - 1) \pmod{N}.$$

This polynomial has degree L and can be constructed using the method in the proof of Theorem 2.16.1 in $O(M(L)\log(L)M(\log(N)))$ bit operations. The polynomial $G(x)$ requires $L\log_2(N)$ bits of storage.

Now, compute $\mathsf{c} = \mathsf{m}^{Le} \pmod{N}$. We wish to evaluate $G(\mathsf{c}^{d_1}) \pmod{N}$ for each of the candidate values $0 \leq d_1 < L$ (to obtain a list of L values). This can be performed using Theorem 2.16.1 in $O(L\log(L)^2\log(\log(L))M(\log(N)))$ bit operations. For each value $G(\mathsf{c}^{d_1}) \pmod{N}$ in the list we can compute

$$\gcd(G(\mathsf{c}^{d_1}), N)$$

to see if we have split N. The total running time of the attack is $\tilde{O}(\sqrt{K})$ bit operations.

Exercise 24.5.9. (Galbraith, Heneghan and McKee [220]) Suppose one chooses private CRT exponents of bit-length n and Hamming weight w. Use the ideas of this section together with those of Section 13.6 to give an algorithm to compute a CRT private exponent, given n and w, with complexity $O(\sqrt{w}W\log(W)^2\log(\log(W))M(\log(N)))$ bit operations where $W = \binom{n/2}{w/2}$.

When e is also small (e.g., when using the key generation method of Exercise 24.1.5) then there are lattice attacks on small CRT private exponents. We refer to Bleichenbacher and May [69] for details.

24.5.3 Large Common Factor of $p-1$ and $q-1$

Variants of RSA have been proposed for moduli $N = pq$ where there is some integer r greater than 2 such that both $r \mid (p-1)$ and $r \mid (q-1)$. For example, as follows from the solution to Exercise 24.5.5, one can prevent the Wiener attack by taking r large. We explain in this section why such variants of RSA must be used with caution.

First we remark, following McKee and Pinch [414], that r should not be considered as a secret. This is because r is a factor of $N-1$ and so the elliptic curve method or the Pollard rho factoring method can be used to compute a, usually short, list of possible values for r. Note that there is no way to determine the correct value of r from the list, but the attacks mentioned below can be repeated for each candidate value for r. Certainly, if r is small then it can be easily found this way. Even if r is large, since factoring $N-1$ in this setting is not harder than factoring N, it follows that the problem of computing r is not harder than the most basic assumption underlying the scheme.

Even if r is not known, as noted by McKee and Pinch [414], it cannot be too large: applying the Pollard rho method by iterating the function

$$x \mapsto x^{N-1} + 1 \pmod{N}$$

will produce a sequence that repeats modulo p after $O(\sqrt{p/r})$ terms, on average. Hence, if r is too large then the factorisation of N will be found even without knowing r.

We now explain a method to factor N when r is known. Suppose $N = pq$ where $p < q < 2p$ are primes. Write

$$p = xr + 1\,, \quad q = yr + 1.$$

Then

$$(N-1)/r = xyr + (x+y) = ur + v \tag{24.4}$$

where u and v $(0 \leq v < r)$ are known and x, y are unknown.

Exercise 24.5.10. Let the notation be as above. Show that if $r > \sqrt{3}N^{1/4}$ then one can determine x and y in polynomial-time.

Exercise 24.5.11. (McKee and Pinch [414]) Let the notation be as above and suppose that $r < \sqrt{3}N^{1/4}$. Write

$$x + y = v + cr\,, \quad xy = u - c$$

where $c \in \mathbb{N}$. Show that $c < 3N^{1/2}/r^2$. Then show that

$$(x-y)^2 = r^2c^2 + (2rv+4)c + v^2 - 4u.$$

Hence, show how to determine c by exhaustive search in $O(N^{1/2}\log(N)^2/r^2)$ bit operations.

Exercise 24.5.12. Let the notation be as above. Show that the exponent of $(\mathbb{Z}/N\mathbb{Z})^*$ divides xyr. Hence, deduce that

$$z^{ur} \equiv z^{xyr+cr} \equiv z^{cr} \pmod{N}$$

for every $z \in (\mathbb{Z}/N\mathbb{Z})^*$. Given r, show how to find c (and hence split N) in an expected $O(N^{1/4}M(\log(N))/r)$ bit operations using the Pollard kangaroo algorithm (one could also use baby-step-giant-step).

Exercise 24.5.13. Suppose $N = pq$ where p and q are 1536-bit primes such that $p-1$ and $q-1$ have a large common factor r. Show that, to ensure security against an attacker who can perform 2^{128} operations, one should impose the restriction $1 \leq r < 2^{640}$.

Exercise 24.5.14. Generalise the above attacks to the case where $r \mid (p+1)$ and $r \mid (q+1)$.

24.6 Digital Signatures Based on RSA and Rabin

There are numerous signature schemes based on RSA and Rabin. Due to lack of space we just sketch two schemes in the random oracle model. Hohenberger and Waters [292] have given an RSA signature scheme in the standard model whose security relies only on the Strong-RSA assumption.

24.6.1 Full Domain Hash

A simple way to design RSA signatures that are secure in the random oracle model is to assume each user has a hash function $H : \{0,1\}^* \to (\mathbb{Z}/N\mathbb{Z})^*$ where N is their public key.[11] Such a hash function is called a **full domain hash**, since the hash output is the entire domain of the RSA trapdoor permutation. Constructing such a hash function is not completely trivial; we refer to Section 3.6. The signature on a message m in this case is $\mathsf{s} = H(\mathsf{m})^d \pmod{N}$. These ideas were formalised by Bellare and Rogaway, but we present the slightly improved security result due to Coron.

Theorem 24.6.1. *RSA signatures with full domain hash (**FDH-RSA**) have UF-CMA security in the random oracle model (i.e., where the full domain hash function is replaced by a random oracle) if the RSA problem is hard.*

Proof: (Sketch) Let A be an perfect[12] adversary playing the UF-CMA game. We build a simulator that takes an instance (N, e, y) of the RSA problem and, using A as a subroutine, tries to solve the RSA problem.

The simulator in this case starts by running the adversary A on input (N, e). The adversary will make queries to the hash function H, and will make decryption queries. The adversary will eventually output a pair $(\mathsf{m}^*, \mathsf{s}^*)$ such that s^* is a valid signature on m^*. To explain the basic idea of the simulator we remark that if one could arrange that $H(\mathsf{m}^*) = y$ then $(\mathsf{s}^*)^e \equiv y \pmod{N}$ and the RSA instance is solved.

The simulator simulates the random oracle H in the following way. First, the simulator will maintain a list of pairs $(\mathsf{m}, H(\mathsf{m}))$ where m was a query to the random oracle and $H(\mathsf{m}) \in (\mathbb{Z}/N\mathbb{Z})^*$ was the value returned. This list is initially empty. For each query m to the random oracle the simulator first checks if m has already been queried and, if

[11] In practice one designs $H : \{0,1\}^* \to \{0, 1, \ldots, N-1\}$ since the probability that a random element of $\mathbb{Z}/N\mathbb{Z}$ does not lie in $(\mathbb{Z}/N\mathbb{Z})^*$ is negligible.

[12] The proof in the general case, where the adversary succeeds with non-negligible probability ϵ, requires minor modifications.

so, responds with the same value $H(\mathsf{m})$. If not, the simulator chooses a random element $1 < r < N$, computes $\gcd(r, N)$ (and if this is not 1 then factors N, solves the RSA instance, and halts), computes $z = r^e \pmod N$ and with some probability $1 - p$ (we determine p at the end of the proof) returns z as $H(\mathsf{m})$ and with probability p returns $yz \pmod N$. The information $(\mathsf{m}, H(\mathsf{m}), r)$ is stored.

When the simulator is asked by the adversary to sign a message m it performs the following: First it computes $H(\mathsf{m})$ and the corresponding value r. If $H(\mathsf{m}) = r^e \pmod N$ then the simulator returns $\mathsf{s} = r$. If $H(\mathsf{m}) = yr^e \pmod N$ then the simulator fails.

Eventually, the adversary outputs a pair $(\mathsf{m}^*, \mathsf{s}^*)$. If $H(\mathsf{m}^*) = yr^e \pmod N$ where r is known to the simulator, and if $(\mathsf{s}^*)^e \equiv H(\mathsf{m}^*) \pmod N$, then $y = (\mathsf{s}^* r^{-1})^e \pmod N$ and so the simulator returns $\mathsf{s}^* r^{-1} \pmod N$. Otherwise, the simulator fails.

To complete the proof it is necessary to argue that the simulator succeeds with non-negligible probability. If the adversary makes q_S signing queries then the probability that the simulator can answer all of them is $(1-p)^{q_S}$. The probability that the message m^* corresponds to a random oracle query that allows us to solve the RSA problem is p. Hence, the probability of success is (ignoring some other negligible factors) $(1-p)^{q_S} p$. Assume that $q_S \geq 1$ and that q_S is known (in practice, one can easily learn a rough estimate of q_S by experimenting with the adversary A). Choose $p = 1/q_S$ so that the probability of success is $(1 - 1/q_S)^{q_S} \frac{1}{q_S}$, which tends to $1/(eq_S)$ for large q_S (where $e = 2.71828\ldots$). Since a polynomial-time adversary can only make polynomially many signature queries the result follows. We refer to Coron [148] for all the details. □

One problem with the full domain hash RSA scheme is the major loss of security (by a factor of q_S) in Theorem 24.6.1. In other words, the reduction is not tight. This can be avoided by including an extra random input to the hash function. In other words, an RSA signature is $(\mathsf{s}_1, \mathsf{s}_2)$ such that $\mathsf{s}_2^e \equiv H(\mathsf{m} \| \mathsf{s}_1) \pmod N$. Then, when the simulator is asked to output a signature on message m, it can choose a "fresh" value s_1^* and define $H(\mathsf{m} \| \mathsf{s}_1^*) = (\mathsf{s}_2^*)^e \pmod N$ as above. This approach avoids previous queries to $H(\mathsf{m} \| \mathsf{s}_1)$ with high probability. Hence, the simulator can answer "standard" hash queries with $yr^e \pmod N$ and "special" hash queries during signature generation with $r^e \pmod N$. This scheme is "folklore", but the details are given in Appendix A of Coron [149]. The drawback is that the extra random value s_1 must be included as part of the signature. The **PSS** signature padding scheme was designed by Bellare and Rogaway [41] precisely to allow extra randomness in this way without increasing the size of the signature. We refer to [149] for a detailed analysis of RSA signatures using the PSS padding.

Exercise 24.6.2. Give a security proof for the RSA full domain hash signature scheme with verification equation $H(\mathsf{m} \| \mathsf{s}_1) = \mathsf{s}_2^e \pmod N$.

The above results are all proved in the random oracle model. Paillier [475] has given some evidence that full domain hash RSA and RSA using PSS padding cannot be proved secure in the standard model. Theorem 1 of [475] states that if one has a "black box" reduction from the RSA problem to selective forgery for a signature scheme under a passive attack, then under an adaptive chosen message attack one can, in polynomial-time, forge any signature for any message.

24.6.2 Secure Rabin-Williams Signatures in the Random Oracle Model

In this section we give a tight security result, due to Bernstein [47], for Rabin signatures. We assume throughout that $N = pq$ is a **Williams integer**; in other words, a product of primes $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$ (such integers were discussed in Section 24.2.1).

We assume that $H : \{0,1\}^* \to \{0,1\}^\kappa$ is a cryptographic hash function (which will be modelled as a random oracle) where $2^\kappa < N < 2^{\kappa+O(\log(\kappa))}$.

Exercise 24.6.3. Suppose $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$ are primes and $N = pq$. Then $(\frac{-1}{p}) = (\frac{-1}{q}) = (\frac{2}{p}) = -1$ while $(\frac{2}{q}) = 1$. Show that, for any integer $h \in (\mathbb{Z}/N\mathbb{Z})^*$, there are unique integers $e \in \{1,-1\}$ and $f \in \{1,2\}$ such that efh is a square modulo N.

The signature scheme for public key N is as follows. For a message $\mathsf{m} \in \{0,1\}^*$ one computes $H(\mathsf{m})$ and interprets it as an integer modulo N (with overwhelming probability, $H(\mathsf{m}) \in (\mathbb{Z}/N\mathbb{Z})^*$). The signer determines the values e and f as in Exercise 24.6.3 and determines the four square roots s_1, s_2, s_3, s_4 satisfying $s_i^2 \equiv H(\mathsf{m})ef \pmod N$. The signer then deterministically chooses one of the values s_i (for example, by ordering the roots as integers $s_1 < s_2 < s_3 < s_4$ and then generating an integer $i \in \{1,2,3,4\}$ using a pseudorandom number generator with a secret key on input m). The signature is the triple $\mathsf{s} = (e, f, (ef)^{-1}s_i \pmod N)$. It is crucially important that, if one signs the same message twice, then the same signature is output. To verify a signature $\mathsf{s} = (e, f, s)$ for public key N and message m one computes $H(\mathsf{m})$ and then checks that $efs^2 \equiv H(\mathsf{m}) \pmod N$.

Exercise 24.6.4. Show that if a signer outputs two signatures (e_1, f_1, s_1) and (e_2, f_2, s_2) for the same message m such that $s_1 \not\equiv \pm s_2 \pmod N$ then one can factor the modulus.

Exercise 24.6.5. Show that it is not necessary to compute the Jacobi symbol $(\frac{H(\mathsf{m})}{N})$ when generating Rabin-Williams signatures as above. Instead, one can compute $H(\mathsf{m})^{(p+1)/4} \pmod p$ and $H(\mathsf{m})^{(q+1)/4} \pmod q$, as is needed to compute the s_i, and determine e and f with only a little additional computation.

Theorem 24.6.6. *The Rabin-Williams signature scheme sketched above has UF-CMA security in the random oracle model (i.e., if H is replaced by a random oracle) if factoring Williams integers is hard and if the pseudorandom generator is indistinguishable from a random function.*

Proof: (Sketch) Let A be a perfect adversary against the Rabin-Williams signature scheme and let N be a Williams integer to be factored. The simulator runs the adversary A on N.

The simulator must handle the queries made by A to the random oracle. To do this it maintains a list of hash values, which is initially empty. When A queries H on m the simulator first checks whether m appears on the list of hash values, and, if it does, responds with the same value as previously. If H has not been previously queried on m the simulator chooses random $s \in (\mathbb{Z}/N\mathbb{Z})^*$, $e \in \{-1,1\}$, $f \in \{1,2\}$ and computes $h = efs^2 \pmod N$. If $0 \leq h < 2^\kappa$ then return h and store (m, e, f, s, h) in the list. If h is too big then repeat with a different choice for (s, e, f). Since $N < 2^{\kappa+O(\log(\kappa))}$ the expected number of trials is polynomial in $\log(N)$.

When A makes a signature query on m the simulator first queries $H(\mathsf{m})$ and gets the values (e, f, s) from the hash list such that $H(\mathsf{m}) \equiv efs^2 \pmod N$. The simulator can therefore answer with (e, f, s), which is a valid signature. (It is necessary to show that the values (e, f, s) output in this way are indistinguishable from the values output in the real cryptosystem, and this requires that the pseudorandom choice of s from among the four possible roots be computationally indistinguishable from random; note that the adversary cannot detect whether or not a pseudorandom generator has actually been used since it does not know the secret key for the generator.)

Finally, A outputs a signature (e^*, f^*, s^*) on a message m^*. Recalling the values (e, f, s) from the construction of $H(\mathsf{m}^*)$ we have $e^* = e$, $f^* = f$ and $(s^*)^2 \equiv s^2 \pmod N$.

With probability 1/2 we can factor N as $\gcd(N, s^* - s)$. We refer to Section 6 of Bernstein [47] for the full details. □

Exercise 24.6.7. Show that if one can find a collision for the hash function H in Bernstein's variant of Rabin-Williams signatures and one has access to a signing oracle then one can factor N with probability 1/2.

Exercise 24.6.8. Suppose the pseudorandom function used to select the square root in Rabin-Williams signatures is a function of $H(\mathsf{m})$ rather than m. Show that, in contrast to Exercise 24.6.7, finding a collision in H no longer leads to an algorithm to split N. On the other hand, show that if one can compute a preimage for H and one has access to a signing oracle then one can factor N with probability 1/2.

Exercise 24.6.9. Adapt the proof of Theorem 24.6.6 to the case where H has full domain output.

Exercise 24.6.10. Adapt the proof of Theorem 24.6.1 to the case where $H : \{0,1\}^* \to \{0,1\}^\kappa$ where $2^\kappa < N < 2^{\kappa + O(\log(\kappa))}$.

24.6.3 Other Signature and Identification Schemes

Example 24.6.11. Let (N, e) be an RSA public key for a trusted authority, where e is a large prime. Shamir [547] proposed the following identity-based signature scheme. A user with identity $\mathsf{id} \in \{0,1\}^*$ has a corresponding public key $H_1(\mathsf{id}) \in (\mathbb{Z}/N\mathbb{Z})^*$, where H_1 is a cryptographic hash function. The user obtains their private key s_{id} such that

$$s_{\mathsf{id}}^e \equiv H_1(\mathsf{id}) \pmod{N}$$

from the trusted authority.

To sign a message $\mathsf{m} \in \{0,1\}^*$ the user chooses a random integer $1 < r < N$, computes $\mathsf{s}_1 = r^e \pmod{N}$, then computes $\mathsf{s}_2 = s_{\mathsf{id}} r^{H_2(\mathsf{m} \| \mathsf{s}_1)} \pmod{N}$ where $H_2 : \{0,1\}^* \to \{0, 1, \ldots, N-1\}$ is a cryptographic hash function and s_1 is represented as a binary string. The signature is $(\mathsf{s}_1, \mathsf{s}_2)$.

To verify a signature one checks that

$$\mathsf{s}_2^e \equiv H_1(\mathsf{id}) \mathsf{s}_1^{H_2(\mathsf{m} \| \mathsf{s}_1)} \pmod{N}.$$

Exercise 24.6.12. Show that outputs $(\mathsf{s}_1, \mathsf{s}_2)$ of the Shamir signature algorithm do satisfy the verification equation.

The security of Shamir signatures was analysed by Bellare, Namprempre and Neven [35] (also see Section 4 of [335]). They show, in the random oracle model, that the scheme is secure against existential forgery if the RSA problem is hard.

Exercise 24.6.13. Show how to break the Shamir signature scheme under a known message attack if e is small (for example, $e = 3$).

Exercise 24.6.14. Consider the following modified version of the Shamir identity-based signature scheme: The verification equation for signature $(\mathsf{s}_1, \mathsf{s}_2)$ on message m and identity id is

$$\mathsf{s}_2^e \equiv H_1(\mathsf{id}) \mathsf{s}_1^{H_2(\mathsf{m})} \pmod{N}.$$

Show how the user with private key s_{id} can generate signatures. Give a selective forgery under a known message attack for this scheme.

Exercise 24.6.15. Consider the following modified version of the Shamir identity-based signature scheme: The verification equation for signature s on message m and identity id is

$$\mathsf{s}^e \equiv H_1(\mathsf{id})^{H_2(\mathsf{m})} \pmod{N}.$$

Show how the user with private key s_{id} can generate signatures. Show how to compute the private key for this scheme under a known message attack.

We now briefly present two interactive identification schemes that are convenient alternatives to RSA and Rabin signatures for constrained devices. The notion of an identification scheme was sketched in Section 22.1.1; recall that it is an interactive protocol between a prover and a verifier.

Example 24.6.16. (Feige, Fiat and Shamir [201]) A prover has public key $(N, v_1, \ldots, v_k)$, where $N = pq$ is an RSA modulus and $1 < v_j < N$ for $1 \leq j \leq k$. The private key is a list of integers $u_1, \ldots, u_k$ such that $v_j \equiv u_j^2 \pmod{N}$ for $1 \leq j \leq k$. The identification protocol is as follows: The prover chooses a random integer $1 < r < N$ and send $\mathsf{s}_1 = r^2 \pmod{N}$ to the verifier. The verifier sends a challenge $c = (c_1, \ldots, c_k) \in \{0,1\}^k$. The prover computes

$$\mathsf{s}_2 = r \prod_{j=1}^{k} u_j^{c_j} \pmod{N}$$

and sends it to the verifier. The verifier checks that

$$\mathsf{s}_2^2 \equiv \mathsf{s}_1 \prod_{j=1}^{k} v_j^{c_j} \pmod{N}.$$

One can try to impersonate a user by guessing the challenge c and defining s_1 accordingly; this succeeds with probability $1/2^k$. The protocol can be repeated a number of times if necessary. For example, one might choose $k = 20$ and repeat the protocol 4 times.

The point is that both signing and verification are only a small number of modular multiplications (in contrast to Rabin signatures, for which signing requires computing two large exponentiations). The security is based on factoring (see Exercise 24.6.17).

The public key can be shortened by choosing $v_1, \ldots, v_k$ to be the first k primes. Alternatively, the scheme can be made identity-based by defining $v_1, \ldots, v_k$ as a function of the identity of a user; the user can get the values u_i from the trusted authority who knows the factorisation of N. The identification scheme can be turned into a signature scheme (either public key or identity-based) by choosing the value c as the output of a hash function $H(\mathsf{m} \| \mathsf{s}_1)$; but then k should be taken to be very large. For further discussion of these schemes see Sections 10.4.2 and 11.4.1 of Menezes, van Oorschot and Vanstone [418].

Exercise 24.6.17. Let A be an algorithm that takes as input a public key for the Feige-Fiat-Shamir scheme, outputs a value s_1, receives two distinct challenges c_1 and c_2 and outputs values $\mathsf{s}_{2,1}$ and $\mathsf{s}_{2,2}$ satisfying the verification equation for c_1 and c_2 respectively. Show how to use A to compute square roots modulo N.

Example 24.6.18. (Guillou and Quisquater [271]) A prover has public key (N, e, u) where $N = pq$ is an RSA modulus, e is an RSA exponent (i.e., $\gcd(e, \varphi(N)) = 1$) and $1 < u < N$ is a randomly chosen integer. The private key is an integer s such that $s^e \equiv u \pmod{N}$. The identification protocol is as follows: The prover chooses a random integer $1 < r < N$ and sends $\mathsf{s}_1 = r^e \pmod{N}$ to the verifier. The verifier sends a

challenge $0 \leq c < 2^k$ to the prover, who replies with $\mathsf{s}_2 = rs^c \pmod N$. The verifier checks that

$$\mathsf{s}_2^e \equiv \mathsf{s}_1 u^c \pmod N.$$

When e and c are small then both the prover and verifier have easy computations (in contrast with RSA, where at least one party must perform a large exponentiation). Hence this scheme can be more suitable than RSA in constrained environments. The security depends on the RSA problem (see Exercise 24.6.19).

One can try to impersonate a user by guessing the challenge c and defining s_1 accordingly; this succeeds with probability $1/2^k$. The protocol can be repeated a number of times if necessary.

The scheme can be made identity-based by replacing u with $H_1(\mathsf{id})$. Each user can get their private key s_{id} such that $s_{\mathsf{id}}^e \equiv H_1(\mathsf{id}) \pmod N$ from the trusted authority. The scheme can be turned into a signature scheme (either public key or identity-based) by setting $c = H(\mathsf{m} \| \mathsf{s}_1)$; but then k should be sufficiently large. A variant with lower bandwidth is to send only some bits of s_1 and change the verification equation to checking that the appropriate bits of $\mathsf{s}_2^e u^{-c} \pmod N$ equal those of s_1. For further discussion of these schemes see Sections 10.4.3 and 11.4.2 of Menezes, van Oorschot and Vanstone [418].

Exercise 24.6.19. Let A be an algorithm that takes as input a public key for the Guillou-Quisquater scheme, outputs a value s_1, receives two distinct challenges c_1 and c_2 and outputs values $\mathsf{s}_{2,1}$ and $\mathsf{s}_{2,2}$ satisfying the verification equation for c_1 and c_2 respectively. Show how to use A to solve the RSA problem.

24.7 Public Key Encryption Based on RSA and Rabin

24.7.1 Padding Schemes for RSA and Rabin

To prevent algebraic attacks such as those mentioned in Sections 1.2 and 24.4 it is necessary to use randomised padding schemes for encryption with RSA. Three goals of padding schemes for RSA are listed below.

1. To introduce randomness into the message and expand short messages to full size.
2. To ensure that algebraic relationships among messages do not lead to algebraic relationships between the corresponding ciphertexts.
3. To ensure that random elements of $\mathbb{Z}_N^*$ do not correspond to valid ciphertexts. This means that access to a decryption oracle in CCA attacks is not useful.

Example 24.7.1. Consider the following naive padding scheme when using 3072-bit RSA moduli: suppose messages are restricted to be at most 256 bits, and suppose a random 2815-bit value is r appended to the message to bring it to full length (i.e., the value input to the RSA function is $\mathsf{m} + 2^{256}r$). This certainly adds randomness and destroys many algebraic relationships. However, there is an easy CCA attack on the OWE-security of RSA with this padding scheme.

To see this, suppose $2^{3071} < N < 2^{3072}$ and let c be the ciphertext under attack. With probability $1/2$ the most significant bit of r is zero and so $\mathsf{c}' = \mathsf{c}2^e \pmod N$ is a valid padding of $2\mathsf{m}$ (except that the most significant bit of m is lost). Hence, by decrypting c' one determines all but the most significant bit of m. Similarly, if the least significant bit of m is zero then one can make a decryption query on $\mathsf{c}' = 2^{-e}\mathsf{c} \pmod N$.

Exercise 24.7.2. Consider the situation of Example 24.7.1 again. Find a CCA attack on RSA with the padding scheme $1+2\mathsf{m}+2^{257}r+2^{3071}$ where $0 \leq \mathsf{m} < 2^{256}$ and $0 \leq r < 2^{2813}$.

24.7.2 OAEP

In this section we present the **OAEP** (Optimal Asymmetric Encryption Padding) scheme, which was developed by Bellare and Rogaway [40] (for more details see Section 5.9.2 of Stinson [592]). The word "optimal" refers to the length of the padded message compared with the length of the original message: the idea is that the additional bits in an OAEP padding of a message are as small as can be.

The padding scheme takes as input an n-bit message m and outputs a κ-bit binary string S that can then be encrypted (in the case of RSA one encrypts by interpreting S as an element of $\mathbb{Z}_N^*$ and raising to the power e modulo N). Similarly, to decrypt a ciphertext c corresponding to an RSA-OAEP message one computes $\mathsf{c}^d \pmod N$, interprets this number as a bitstring S, and then unpads to get m or $\perp$. Figure 24.3 describes the OAEP scheme in detail. As usual, $a\|b$ denotes the concatenation of two binary strings and $a \oplus b$ denotes the bitwise XOR of two binary strings of the same length.

System Parameters: Suppose we are using $(\kappa+1)$-bit RSA moduli (e.g., $\kappa = 3071$). Let κ_0 and κ_1 be chosen so that no adversary can perform 2^{κ_i} operations, e.g. $\kappa_0 = \kappa_1 = 128$. Set $n = \kappa - \kappa_0 - \kappa_1$. Messages are defined to be n-bit strings.
Let G be a cryptographic hash function mapping κ_0 bit strings to $n+\kappa_1$ bit strings and H be a cryptographic hash function from $n+\kappa_1$ bit strings to κ_0 bit strings.

Pad: Let m be an n-bit string.

1. Choose a random κ_0-bit string R.
2. Set $S_1 = (m\|0^{\kappa_1}) \oplus G(R)$, where 0^{κ_1} denotes a κ_1-bit string of zeroes.
3. Set $S_2 = R \oplus H(S_1)$.
4. Set $S = S_1\|S_2$.

Unpad: Given a κ-bit string S one calls the low κ_0 bits S_2 and the high $n+\kappa_1$ bits S_1.

1. Compute $R = S_2 \oplus H(S_1)$.
2. Compute $S_3 = S_1 \oplus G(R)$.
3. Check whether the low κ_1 bits of S_3 are all zero, if not output $\perp$ and halt.
4. Obtain m as the top n bits of S_3.

Figure 24.3: OAEP.

The RSA-OAEP scheme does achieve the three goals of padding schemes mentioned earlier. First, the padding scheme is randomised and has full length. Second, since S_1 and S_2 are both XORs with outputs of hash functions, the bitstring S "looks random" and algebraic relationships among messages do not lead to algebraic relationships among their paddings. Third, if you have a decryption oracle and you send it a random element of $\mathbb{Z}_N^*$ then it will output $\perp$ with high probability.

The security of RSA-OAEP has a complicated history. Bellare and Rogaway [40] gave an IND-CCA security result, assuming that the RSA problem is hard, in the random oracle model, but Shoup [555] found a flaw in their security proof (though not an attack on their scheme). Shoup also gave a variant of OAEP (called OAEP+) together with a security proof in the random oracle model. Fujisaki, Okamoto, Pointcheval and Stern [215] were able to give a proof of the security of RSA using OAEP in the random oracle model by exploiting the random self-reducibility of RSA. The reader is referred to these papers,

and the excellent survey by Gentry [252], for the details.

24.7.3 Rabin-SAEP

Boneh [74] has considered a padding scheme (which he calls **SAEP**) that is simpler than OAEP and is suitable for encrypting short messages with Rabin. Note that the restriction to short messages is not a serious problem in practice, since public key encryption is mainly used to transport symmetric keys; nevertheless, this restriction means that SAEP is not an "optimal" padding. The scheme can also be used for RSA with extremely short public exponents (such as $e = 3$). We sketch the proof of security of Rabin encryption using this padding, as it is relatively straightforward and it is also a nice application of some of the cryptanalysis techniques already seen in Section 24.4.

Let $\kappa \in \mathbb{N}$ be a security parameter (for example, $\kappa = 3070$). Suppose $N = pq$ is an RSA modulus such that $2^{\kappa+1} < N < 2^{\kappa+1} + 2^{\kappa}$. We will also assume that $p \equiv q \equiv 3 \pmod 4$. Suppose $0 < \kappa_0, \kappa_1 < \kappa_0 + \kappa_1 < \kappa$ (later we will insist that $\kappa_1 > (\kappa + 2)/2$ and $0 < n = \kappa - \kappa_0 - \kappa_1 < \kappa/4$). Let $H : \{0,1\}^{\kappa_1} \to \{0,1\}^{n+\kappa_0}$ be a cryptographic hash function. The SAEP padding of a message $\mathsf{m} \in \{0,1\}^n$ is as follows:

1. Set $S_0 = \mathsf{m} \| 0^{\kappa_0}$.
2. Choose a random element $R \in \{0,1\}^{\kappa_1}$.
3. Set $S_1 = S_0 \oplus H(R)$.
4. Output $S = S_1 \| R$.

To unpad an SAEP bitstring S one first writes S as $S_1 \| R$ where $R \in \{0,1\}^{\kappa_1}$, then computes $S_0 = S_1 \oplus H(R)$, then writes $S_0 = \mathsf{m} \| S_2$ where $S_2 \in \{0,1\}^{\kappa_0}$. If S_2 is not the all zero string then return $\perp$, else return m.

Rabin-SAEP encryption proceeds by taking a message $\mathsf{m} \in \{0,1\}^n$, padding it as above, interpreting the bitstring as an integer $0 \leq x < 2^{\kappa} < N/2$, and computing $\mathsf{c} = x^2 \pmod N$. As usual, with overwhelming probability we have $\gcd(x, N) = 1$, so we assume that this is the case.

To decrypt the ciphertext c one computes the four square roots $1 \leq x_1, \ldots, x_4 < N$ of c modulo N in the usual way. Writing these such that $x_3 = N - x_1, x_4 = N - x_2$ it follows that at exactly two of them are less than $N/2$. Hence, at most two are less than 2^{κ}. For each root x such that $x < 2^{\kappa}$ perform the unpad algorithm to get either $\perp$ or a message m. If there are two choices for x, and either both give $\perp$ or both give messages, then output $\perp$. Otherwise, output m. An integer c is said to be a **valid ciphertext** if it decrypts to a message m, otherwise it is an **invalid ciphertext**.

Exercise 24.7.3. Show that if S is the output of the pad algorithm on $\mathsf{m} \in \{0,1\}^n$ then m is the output of unpad on S. Then show that if c is a Rabin-SAEP encryption of a message $\mathsf{m} \in \{0,1\}^n$ then the decryption algorithm on c outputs m with overwhelming probability.

We will now study the security of the scheme. Intuitively, a CCA attacker of the Rabin-SAEP scheme either computes at least one square root of the challenge ciphertext c^*, or else computes a ciphertext c related to c^* in the sense that if c^* is an encryption of m then c is an encryption of $\mathsf{m} \oplus z$ for some bitstring z. In this latter case, there is a square root of c that differs from the desired square root of c^* only in some of the most significant n bits. The proof of Theorem 24.7.5 shows how either situation leads to the factorisation of N.

Lemma 24.7.4. *Let $\kappa \in \mathbb{N}$ (with $\kappa > 10$). Let $N = pq$, where $p \equiv q \equiv 3 \pmod 4$ are prime. Suppose further that $2^{\kappa+1} < N < 2^{\kappa+1} + 2^{\kappa}$. Let $y = x^2 \pmod N$ where $0 < x < 2^{\kappa}$ is randomly chosen. Then there is an integer $0 < x' < 2^{\kappa}$ such that $x' \neq x$ but $y \equiv (x')^2 \pmod N$ with probability at least $1/3$.*

Proof: We know that $2^{\kappa} < N/2 < \frac{3}{2}2^{\kappa}$.

Let $A = \{0 < x < 2^{\kappa} : \gcd(x, N) = 1$ and $x^2 \pmod N$ has exactly one square root in the range$\}$ and $B = \{0 < x < 2^{\kappa} : \gcd(x, N) = 1$ and $x^2 \pmod N$ has exactly two square roots in the range$\}$. Note that $\#A + \#B \geq 2^{\kappa} - p - q + 1$.

Since every such $y = x^2 \pmod N$ has exactly two square roots between 0 and $N/2$, it follows that for each $x \in A$ then the other square root x' satisfies $2^{\kappa} \leq x' < N/2$. Hence, $\#A < N/2 - 2^{\kappa}$ and so $\#B > 2^{\kappa+1} - N/2 - p - q$.

Finally, the probability of having two roots is

$$\frac{\#B}{2^{\kappa}} > 2 - \frac{N}{2^{\kappa+1}} - \frac{p+q}{2^{\kappa}} > \frac{1}{2} - \frac{p+q}{2^{\kappa}},$$

which is $1/2 - \epsilon$ for some small $\epsilon > 0$, and certainly greater than $1/3$ when $p, q > 2^5$. □

Theorem 24.7.5. *Let $N = pq$ be a public key for the Rabin-SAEP encryption scheme. Suppose $0 < \kappa_0, \kappa_1 < \kappa$ are parameters such that $\kappa_1 > (\kappa+2)/2$ and $n = \kappa - \kappa_0 - \kappa_1 < \kappa/4$. If factoring Blum integers is hard then Rabin-SAEP has IND-CCA security in the random oracle model (i.e., when the hash function H is replaced by oracle access to a random function).*

Proof: (Sketch) Let A be an adversary against IND-CCA security of Rabin-SAEP in the random oracle model. We build a simulator that takes as input an integer $N = pq$ and attempts to factor it. The simulator will run A on the public key N.

The adversary A makes queries to the hash function oracle, decryption queries, and, at some point, gives two messages m_0 and m_1 and requests a challenge ciphertext c^* that is an encryption of m_b where $b \in \{0, 1\}$. The adversary eventually outputs a guess for the bit b. The simulator has to respond to these queries.

To respond to the request for the challenge ciphertext the simulator will choose a random $0 < a^{\dagger} < 2^{\kappa}$ and compute $\mathsf{c}^* = (a^{\dagger})^2 \pmod N$. By Lemma 24.7.4, with probability at least $1/3$ there is a second value $0 < a^* < 2^{\kappa}$ such that $\mathsf{c}^* \equiv (a^*)^2 \pmod N$. The entire security proof is designed so that the simulator has a chance to learn the value a^*. Once the simulator knows a^* it can factor N by computing $\gcd(N, a^{\dagger} - a^*)$. Without loss of generality, $a^{\dagger}$ is chosen at the start of the simulation.

Let $r^{\dagger}$ and r^* be the κ_1 least significant bits of $a^{\dagger}$ and a^* respectively. Note that $r^{\dagger}$ is known to the simulator but r^* is not. The question of whether c^* is a valid ciphertext, and if so, whether it encrypts message m_0 or m_1, depends entirely on the values $H(r^{\dagger})$, $H(r^*)$, $a^{\dagger}$ and a^*. Surprisingly, it is not necessary for the simulator to ensure that c^* is a valid encryption of either m_0 or m_1. The crux of the proof is the observation that, in order to be able to answer the above questions, one has to perform some operations involving r^*. For the remainder of the proof we assume that the value $H(r^{\dagger})$ is such that $a^{\dagger}$ does not correspond to a correct SAEP padding of a message. Further, it may help the reader to imagine that the value of H on r^* is such that $x^* \oplus H(r^*)$ (where $a^* = x^* \| r^*$) has its κ_0 least significant bits equal to zero.[13]

Boneh shows that either A makes a query to the hash function H on r^*, or A makes a query to the decryption oracle with a ciphertext c that is an encryption using the value r^*. These observations are exploited as follows.

[13] As we will see, the point is that this computation need never be performed, since as soon as r^* is queried to H the simulator wins and the game is over.

- If c is a ciphertext such that a corresponding value r has been queried to H, then the polynomial $F(y) = (y2^{\kappa_1} + r)^2 - \mathsf{c}$ has a root modulo N with $0 \leq y < \sqrt{N}$, and this can be efficiently found using Coppersmith's method (see Theorem 19.1.9; it is easy to make $F(y)$ monic before applying the theorem). For each decryption query on c one therefore repeats the above process for all values r that have been queried to H (we may assume at this point that $r \neq r^*$). A solution to this equation gives one of the roots of the ciphertext. In the case where the adversary is asking the simulator to decrypt a ciphertext that it has previously encrypted, then the simulator will respond correctly. We stress that if none of the values r queried to H correspond to the value c then there is not likely to be a small solution to the equation and Coppersmith's method does not provide any useful output.
- Alternatively, suppose c is a valid ciphertext that shares the value r^* with c^*. Let x be the corresponding square root of c, so that $\mathsf{c} = x^2 \pmod N$ and the κ_1 least significant bits of x equal r^*. Even though $H(r^*)$ has not yet been queried (otherwise, we have already factored N) if c^* and c are valid ciphertexts then we do not just have $x \equiv a^* \equiv r^* \pmod{2^{\kappa_1}}$ but $x \equiv a^* \pmod{2^{\kappa_0+\kappa_1}}$.

  Let z be such that $x = a^* + 2^{\kappa_0+\kappa_1}z$. Then $F_1(y) = y^2 - \mathsf{c}^*$ and $F_2(y,z) = (y + 2^{\kappa_0+\kappa_1}z)^2 - \mathsf{c}$ have a root y modulo N in common. Taking the resultant of $F_1(y)$ and $F_2(y,z)$ with respect to y gives a degree 4 polynomial $F(z)$ with a root $0 < z < N^{1/4}$. In such a situation, z can be computed by Coppersmith's theorem (again, it is easy to make the polynomial monic). Once z is computed one solves for y using the polynomial gcd and hence obtains the desired root a^* of c^*. These calculations will fail (in the sense that Coppersmith's algorithm does not output a small root) if c does not have a root x such that $x \equiv a^* \pmod{2^{\kappa_0+\kappa_1}}$.

All the main ideas are now in place, so we can finally describe the simulator. First we explain how the simulator handles queries to the oracle H.

1. The simulator creates a table of values $(r, H(r))$, which is initially set to have the single entry $(r^\dagger, H(r^\dagger))$ where $H(r^\dagger)$ is chosen uniformly at random.
2. If A queries the oracle H on a value r such that r already appears in the table, then the simulator returns the corresponding value $H(r)$.
3. If A queries the oracle H on a new value r then the simulator runs Coppersmith's algorithm on $F(y) = (y2^{\kappa_1} + r)^2 - \mathsf{c}^*$ in the hope of finding a root of c^*. If this succeeds then the root must be a^* (since if $r = r^\dagger$ we do not execute this step) and N is factored.
4. If r is new and Coppersmith's method does not yield a root of c^* then choose uniformly at random a value $H(r)$, add $(r, H(r))$ to the table, and return $H(r)$.

Now we explain how to handle decryption queries.

1. If A asks to decrypt a ciphertext c then, for each value r in the table of hash queries, run Coppersmith's algorithm on $F(y) = (y2^{\kappa_1} + r)^2 - \mathsf{c}$. If a square root of c is computed then perform the SAEP unpad algorithm and output the message or $\perp$ accordingly. Note that this is not exactly the same as the decryption algorithm, since it would check all square roots of c in the range of interest.
2. If step 1 does not succeed then compute the polynomial $F(z)$ as the resultant of $F_1(y) = y^2 - \mathsf{c}^*$ and $F_2(y,z) = (y + 2^{\kappa_0+\kappa_1}z)^2 - \mathsf{c}$ with respect to y as discussed above. If Coppersmith's method succeeds for $F(z)$ then the simulator can compute a^* and factor N.

3. If neither of these steps succeed then output $\perp$.

The main claim is that if A has a non-negligible probability of success then one of the above approaches for finding a^* succeeds with non-negligible probability. For complete details, and in particular, a careful analysis of the probabilities, we refer to Boneh [74]. □

Exercise 24.7.6. Prove the analogue of Theorem 24.7.5 when using SAEP padding with RSA and encryption exponent $e = 3$. Give the restriction on the sizes of n, κ_0 and κ_1 in this case.

24.7.4 Further Topics

Hybrid Encryption

It is standard in cryptography that encryption is performed using a **hybrid** system. A typical scenario is to use public key cryptography to encrypt a random session key $K_1 \| K_2$. Then the document is encrypted using a symmetric encryption scheme such as AES with the key K_1. Finally a MAC (message authentication code) with key K_2 of the symmetric ciphertext is appended to ensure the integrity of the transmission.

Encryption Secure in the Standard Model

Cramer and Shoup [160] have given an encryption scheme, using the universal hash proof systems framework based on the Paillier cryptosystem. Their scheme (using $N = pq$ where p and q are safe primes) has IND-CCA security in the standard model if the composite residuosity problem is hard (see Definition 24.3.4). We do not have space to present this scheme.

Hofheinz and Kiltz [291] have shown that the Elgamal encryption scheme of Section 23.1, when implemented in a certain subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$, has IND-CCA security in the random oracle model if factoring is hard, and in the standard model if a certain higher residuosity assumption holds.

Part VII

Advanced Topics in Elliptic and Hyperelliptic Curves

Chapter 25

Isogenies of Elliptic Curves

Isogenies are a fundamental object of study in the theory of elliptic curves. The definition and basic properties were given in Sections 9.6 and 9.7. In particular, they are group homomorphisms.

Isogenies are used in algorithms for point counting on elliptic curves and for computing class polynomials for the complex multiplication (CM) method. They have applications to cryptanalysis of elliptic curve cryptosystems. They also have constructive applications: prevention of certain side-channel attacks; computing distortion maps for pairing-based cryptography; designing cryptographic hash functions; relating the discrete logarithm problem on elliptic curves with the same number of points. We do not have space to discuss all these applications.

The purpose of this chapter is to present algorithms to compute isogenies from an elliptic curve. The most important result is Vélu's formulae, that compute an isogeny given an elliptic curve and a kernel subgroup G. We also sketch the various ways to find an isogeny given an elliptic curve and the j-invariant of an elliptic curve ℓ-isogenous to E. Once these algorithms are in place we briefly sketch Kohel's results, the isogeny graph, and some applications of isogenies. Due to lack of space we are unable to give proofs of most results.

Algorithms for computing isogenies on Jacobians of curves of genus 2 or more are much more complicated than in the elliptic case. Hence, we do not discuss them in this book.

25.1 Isogenies and Kernels

Let $E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$. Recall from Section 9.6 that a non-zero isogeny $\phi : E \to \widetilde{E}$ over $\Bbbk$ of degree d is a morphism of degree d such that $\phi(\mathcal{O}_E) = \mathcal{O}_{\widetilde{E}}$. Such a map is automatically a group homomorphism and has kernel of size dividing d.

Theorem 9.7.5 states that a separable isogeny $\phi : E \to \widetilde{E}$ over $\Bbbk$ may be written in the form

$$\phi(x, y) = (\phi_1(x), cy\phi_1(x)' + \phi_3(x)), \tag{25.1}$$

where $\phi_1(x), \phi_3(x) \in \Bbbk(x)$, where $\phi_1(x)' = d\phi_1(x)/dx$ is the (formal) derivative of the rational function $\phi_1(x)$, where $c \in \overline{\Bbbk}^*$ is a non-zero constant, and where (writing $\widetilde{a}_i$ for the coefficients of $\widetilde{E}$)

$$2\phi_3(x) = -\widetilde{a}_1\phi_1(x) - \widetilde{a}_3 + (a_1x + a_3)\phi_1(x)'.$$

Lemma 9.6.13 showed that if $\phi_1(x) = a(x)/b(x)$ in equation (25.1) then the degree of ϕ is $\max\{\deg_x(a(x)), \deg_x(b(x))\}$. The kernel of an isogeny ϕ with $\phi_1(x) = a(x)/b(x)$ is $\{\mathcal{O}_E\} \cup \{P = (x_P, y_P) \in E(\overline{\Bbbk}) : b(x_P) = 0\}$. The kernel of a separable isogeny of degree d has d elements.

Let E be an elliptic curve over a field $\Bbbk$ and G a finite subgroup of $E(\overline{\Bbbk})$ that is defined over $\Bbbk$. Theorem 9.6.19 states that there is a unique elliptic curve $\widetilde{E}$ (up to isomorphism) and a separable isogeny $\phi : E \to \widetilde{E}$ over $\Bbbk$ such that $\ker(\phi) = G$. We sometimes write $\widetilde{E} = E/G$. Let ℓ be a prime such that $\gcd(\ell, \mathrm{char}(\Bbbk)) = 1$. Since $E[\ell]$ is isomorphic (as a group) to the product of two cyclic groups, there are $\ell + 1$ different subgroups of $E[\ell]$ of order ℓ. It follows that there are $\ell + 1$ isogenies of degree ℓ, not necessarily defined over $\Bbbk$, from E to other curves (some of these isogenies may map to the same image curve).

As implied by Theorem 9.6.18 and discussed in Exercise 9.6.20, an isogeny is essentially determined by its kernel. We say that two separable isogenies $\phi_1, \phi_2 : E \to \widetilde{E}$ are **equivalent isogenies** if $\ker(\phi_1) = \ker(\phi_2)$.

Exercise 25.1.1. Let $\phi : E \to \widetilde{E}$ be a separable isogeny. Show that if $\lambda \in \mathrm{Aut}(\widetilde{E})$ then $\lambda \circ \phi$ is equivalent to ϕ. Explain why $\phi \circ \lambda$ is not necessarily equivalent to ϕ for $\lambda \in \mathrm{Aut}(E)$.

Theorem 25.1.2 shows that isogenies can be written as "chains" of prime-degree isogenies. Hence, in practice one can restrict to studying isogenies of prime degree. This observation is of crucial importance in the algorithms.

Theorem 25.1.2. *Let E and $\widetilde{E}$ be elliptic curves over $\Bbbk$ and let $\phi : E \to \widetilde{E}$ be a separable isogeny that is defined over $\Bbbk$. Then $\phi = \phi_1 \circ \cdots \circ \phi_k \circ [n]$ where $\phi_1, \ldots, \phi_k$ are isogenies of prime degree that are defined over $\Bbbk$ and $\deg(\phi) = n^2 \prod_{i=1}^{k} \deg(\phi_i)$.*

Proof: Theorem 9.6.19 states that ϕ is essentially determined by its kernel subgroup G and that ϕ is defined over $\Bbbk$ if and only if G is. We will also repeatedly use Theorem 9.6.18, that states that an isogeny $\phi : E \to \widetilde{E}$ defined over $\Bbbk$ factors as $\phi = \phi_2 \circ \phi_1$ (where $\phi_1 : E \to E_1$ and $\phi_2 : E_1 \to \widetilde{E}$ are isogenies over $\Bbbk$) whenever $\ker(\phi)$ has a subgroup $G = \ker(\phi_1)$ defined over $\Bbbk$.

First, let n be the largest integer such that $E[n] \subseteq G = \ker(\phi)$ and note that $\phi = \phi' \circ [n]$ where $[n] : E \to E$ is the usual multiplication by n map. Set $i = 1$, define $E_0 = E$ and set $G = G/E[n]$. Now, let $\ell \mid \#G$ be a prime and let $P \in G$ have prime order ℓ. There is an isogeny $\phi_i : E_{i-1} \to E_i$ of degree ℓ with kernel $\langle P \rangle$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Since $\sigma(P) \in G$ but $E[\ell] \not\subseteq G$ it follows that $\sigma(P) \in \langle P \rangle$ and so $\langle P \rangle$ is defined over $\Bbbk$. It follows that ϕ_i is defined over $\Bbbk$. Replace G by $\phi_i(G) \cong G/\langle P \rangle$ and repeat the argument. □

Exercise 25.1.3. How must the statement of Theorem 25.1.2 be modified if the requirement that ϕ be separable is removed?

Exercise 25.1.4. Let E be an ordinary elliptic curve. Let $\phi_1 : E \to E_1$ and $\phi_2 : E_1 \to E_2$ be non-zero separable isogenies over $\Bbbk$ of coprime degrees e and f respectively. Show that there is an elliptic curve $\widetilde{E}_1$ over $\Bbbk$, and a pair of non-zero separable isogenies $\psi_1 : E \to \widetilde{E}_1$ and $\psi_2 : \widetilde{E}_1 \to E_2$ of degrees f and e respectively, such that $\phi_2 \circ \phi_1 = \psi_2 \circ \psi_1$.

25.1.1 Vélu's Formulae

We now present explicit formulae, due to Vélu [617], for computing a separable isogeny from an elliptic curve E with given kernel G. These formulae work in any characteristic. As motivation for Vélu's formulae we now revisit Example 9.6.9.

Example 25.1.5. Let $E : y^2 = x^3 + x$ and consider the subgroup of order 2 generated by the point $(0, 0)$. From Example 9.2.4 we know that the translation by $(0, 0)$ map is given by

$$\tau_{(0,0)}(x, y) = \left(\frac{1}{x}, \frac{-y}{x^2} \right).$$

Hence, it follows that functions invariant under this translation map include

$$X = x + 1/x = (x^2 + 1)/x, \qquad Y = y - y/x^2 = y(x^2 - 1)/x^2.$$

One can compute that $X^3 = (x^6 + 3x^4 + 3x^2 + 1)/x^3$ and so

$$\begin{aligned} Y^2 &= y^2(x^2 - 1)^2/x^4 \\ &= (x^6 - x^4 - x^2 + 1)/x^3 \\ &= X^3 - 4X. \end{aligned}$$

It follows that the map

$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, y\frac{x^2 - 1}{x^2} \right)$$

is an isogeny from E to $\widetilde{E} : Y^2 = X^3 - 4X$.

We remark that ϕ can also be written as

$$\phi(x, y) = \left(\frac{y^2}{x^2}, y\frac{x^2 - 1}{x^2} \right)$$

and can be written projectively as

$$\begin{aligned} \phi(x : y : z) &= (x(x^2 + z^2) : y(x^2 - z^2) : x^2 z) \\ &= (y(x^2 + z^2) : xy^2 - x^2 z - z^3 : xyz) \\ &= (y^2 z : y(x^2 - z^2) : x^2 z) \\ &= (xy^2 : y(y^2 - 2xz) : x^3). \end{aligned}$$

Theorem 25.1.6. *(Vélu) Let E be an elliptic curve over $\Bbbk$ defined by the polynomial*

$$F(x, y) = x^3 + a_2 x^2 + a_4 x + a_6 - \left(y^2 + a_1 xy + a_3 y \right) = 0.$$

Let G be a finite subgroup of $E(\overline{\Bbbk})$. Let G_2 be the set of points in $G - \{\mathcal{O}_E\}$ of order 2 and let G_1 be such that $\#G = 1 + \#G_2 + 2\#G_1$ and

$$G = \{\mathcal{O}_E\} \cup G_2 \cup G_1 \cup \{-Q : Q \in G_1\}.$$

Write

$$F_x = \frac{\partial F}{\partial x} = 3x^2 + 2a_2x + a_4 - a_1y \quad \textit{and} \quad F_y = \frac{\partial F}{\partial y} = -2y - a_1x - a_3.$$

For a point $Q = (x_Q, y_Q) \in G_1 \cup G_2$ define the quantities

$$u(Q) = (F_y(Q))^2 = (-2y_Q - a_1x_Q - a_3)^2$$

and

$$t(Q) = \begin{cases} F_x(Q) & \text{if } Q \in G_2 \\ 2F_x(Q) - a_1F_y(Q) & \text{if } Q \in G_1. \end{cases}$$

Note that if $Q \in G_2$ then $F_y(Q) = 0$ and so $u(Q) = 0$.

Define

$$t(G) = \sum_{Q \in G_1 \cup G_2} t(Q) \quad \textit{and} \quad w(G) = \sum_{Q \in G_1 \cup G_2} (u(Q) + x_Q t(Q))$$

and set

$$A_1 = a_1,\ A_2 = a_2,\ A_3 = a_3,\ A_4 = a_4 - 5t(G),\ A_6 = a_6 - (a_1^2 + 4a_2)t(G) - 7w(G).$$

Then the map $\phi : (x, y) \mapsto (X, Y)$ where

$$X = x + \sum_{Q \in G_1 \cup G_2} \frac{t(Q)}{x - x_Q} + \frac{u(Q)}{(x - x_Q)^2}$$

and

$$Y = y - \sum_{Q \in G_1 \cup G_2} u(Q)\frac{2y + a_1x + a_3}{(x - x_Q)^3} + t(Q)\frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u(Q) - F_x(Q)F_y(Q)}{(x - x_Q)^2}$$

is a separable isogeny from E to

$$\widetilde{E} : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

with kernel G. Further, ϕ satisfies

$$\phi^*\left(\frac{dX}{2Y + A_1X + A_3}\right) = \frac{dx}{2y + a_1x + a_3}.$$

Proof: (Sketch) The basic idea (as used in Example 25.1.5) is that the function

$$X(P) = \sum_{Q \in G} x(P + Q)$$

on E is invariant under G (in the sense that $X = X \circ \tau_Q$ for all $Q \in G$) and so can be considered as "defined on E/G". To simplify some calculations sketched below it turns out to be more convenient to subtract the constant $\sum_{Q \in G - \{\mathcal{O}_E\}} x(Q)$ from X. (Note that $x(Q) = x_Q$.) Let $t_\infty = -x/y$ be a uniformizer on E at $\mathcal{O}_E$ (one could also take $t_\infty = x/y$, but this makes the signs more messy). The function x can be written as $t_\infty^{-2} - a_1t_\infty^{-1} - a_2 - a_3t_\infty - (a_1a_3 + a_4)t_\infty^2 - \cdots$ (for more details about the expansions of x, y and ω_E in terms of power series see Section IV.1 of Silverman [564]). It follows that $X = t_\infty^{-2} - a_1t_\infty^{-1} - \cdots$ and so $v_{\mathcal{O}_E}(X) = -2$.

One can also show that $y = -t_\infty^{-3} - a_1 t_\infty^{-2} - a_2 t_\infty^{-1} - \cdots$. The function $Y(P) = \sum_{Q \in G} y(P+Q)$ is invariant under G and has $v_{\mathcal{O}_E}(Y) = -3$. One can therefore show (see Section 12.3 of Washington [626]) that the subfield $\Bbbk(X,Y)$ of $\Bbbk(x,y)$ is the function field of an elliptic curve $\widetilde{E}$ (Washington [626] does this in Lemma 12.17 using the Hurwitz genus formula). The map $\phi : (x,y) \mapsto (X,Y)$ is therefore an isogeny of elliptic curves. By considering the expansions in terms of t_∞ one can show that the equation for the image curve is $Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$ where the coefficients A_i are as in the statement of the Theorem.

Now, let $\omega_E = dx/(2y + a_1x + a_3)$. One has $dx = (-2t_\infty^{-3} + a_1 t_\infty^{-2} + \cdots)dt_\infty$ and $2y + a_1x + a_3 = -2t_\infty^{-3} - a_1 t_\infty^{-2} + \cdots$ and so $\omega_E = (1 - a_1 t_\infty + \cdots)dt_\infty$. Similarly, $\phi^*(\omega_{\widetilde{E}}) = d(X \circ \phi)/(2Y \circ \phi + A_1 X \circ \phi + A_3) = d(t_\infty^{-2} + a_1 t_\infty^{-1} + \cdots)/(-2t_\infty^{-3} + \cdots) = (1 + \cdots)dt_\infty$. It follows that the isogeny is separable and that $\phi^*(\omega_{\widetilde{E}}) = f\omega_E$ for some function f. Further, $\mathrm{div}(\omega_E) = 0$ and $\mathrm{div}(\phi^*(\omega_{\widetilde{E}})) = \phi^*(\mathrm{div}(\omega_{\widetilde{E}})) = 0$ (by Lemma 8.5.36, since ϕ is unramified[1]) and so $\mathrm{div}(f) = 0$. It follows that f is a constant, and the power series expansions in terms of t_∞ imply that $f = 1$ as required.

Write the isogeny as $\phi(x,y) = (\phi_1(x), y\phi_2(x) + \phi_3(x))$. By Theorem 9.7.5 the isogeny is determined by $\phi_1(x)$ (for the case $\mathrm{char}(\Bbbk) = 2$ see Exercise 9.7.6). Essentially, one only has to prove Vélu's formula for $\phi_1(x)$; we do this now. First, change the definition of X to

$$X(P) = x_P + \sum_{Q \in G - \{\mathcal{O}_E\}} (x_{P+Q} - x_Q)$$

where P is a "generic point" (i.e., $P = (x_P, y_P)$ where x_P and y_P are variables) on the elliptic curve and $Q \in G - \{\mathcal{O}_E\}$. Let $F(x,y)$ be as in the statement of the Theorem and let $y = l(x)$ be the equation of the line through P and Q (so that $l(x) = \lambda(x - x_Q) + y_Q$ where $\lambda = (y_P - y_Q)/(x_P - x_Q)$). Define

$$F_1(x) = F(x, l(x)) = (x - x_Q)(x - x_P)(x - x_{P+Q}).$$

Further,

$$\frac{\partial F_1}{\partial x}(Q) = (x_Q - x_P)(x_Q - x_{P+Q})$$

and

$$\frac{\partial F_1}{\partial x} = \frac{\partial F}{\partial x} + \frac{\partial F}{\partial y}\frac{\partial l}{\partial x} = F_x + F_y \cdot \lambda.$$

Hence, $x_{P+Q} - x_Q = F_x(Q)/(x_P - x_Q) + (y_P - y_Q)F_y(Q)/(x_P - x_Q)^2$. One now considers two cases: When $[2]Q = \mathcal{O}_E$ then $F_y(Q) = 0$. When $[2]Q \neq \mathcal{O}_E$ then it is convenient to consider

$$x_{P+Q} - x_Q + x_{P-Q} - x_{-Q}.$$

Now, $x_{-Q} = x_Q$, $y_{-Q} = y_Q + F_y(Q)$, $F_x(-Q) = F_x(Q) - a_1F_y(Q)$ and $F_y(-Q) = -F_y(Q)$. The formula for $\phi_1(x)$ follows.

Now we sketch how to obtain the formula for the Y-coordinate of the isogeny in the case $\mathrm{char}(\Bbbk) \neq 2$. Note that $\phi_1(x) = x + \sum_Q [t(Q)/(x - x_Q) + u(Q)/(x - x_Q)^2]$ and so $\phi_1(x)' = 1 - \sum_Q [t(Q)/(x - x_Q)^2 + 2u_Q/(x - x_Q)^3]$. Using $\phi_3(x) = (-A_1\phi_1(x) - A_3 +$

[1] This was already discussed in Section 9.6. One can directly see that separable isogenies are unramified since if $\phi(P_1) = P_2$ then the set of pre-images under ϕ of P_2 is $\{P_1 + Q : Q \in \ker(\phi)\}$.

$(a_1x + a_3)\phi_1(x)')/2$ one computes

$$\begin{aligned} y\phi_2(x) + \phi_3(x) &= y\phi_1(x)' + \phi_3(x) \\ &= y\left(1 - \sum_Q t(Q)/(x-x_Q)^2 + 2u(Q)/(x-x_Q)^3\right) \\ &\quad -(a_1x+a_3)/2 - a_1\sum_Q [t(Q)/(x-x_Q)^2 + 2u(Q)/(x-x_Q)^3] \\ &\quad +(a_1x+a_3)/2 + (a_1x+a_3)\sum_Q [-t(Q)/(x-x_Q)^2 - 2u(Q)/(x-x_Q)^3] \\ &= y - \sum_Q \left[t(Q)\frac{y + a_1(x-x_Q) - y_Q}{(x-x_Q)^2} + u(Q)\frac{2y + a_1x + a_3}{(x-x_Q)^3} \right. \\ &\quad \left. + \frac{t(Q)((a_1x_Q + a_3)/2 + y_Q) + a_1u(Q)/2}{(x-x_Q)^2} \right]. \end{aligned}$$

It suffices to show that the numerator of the final term in the sum is equal to $a_1u(Q) - F_x(Q)F_y(Q)$. However, this follows easily by noting that $(a_1x_Q+a_3)/2+y_Q = -F_y(Q)/2$, $u(Q) = F_y(Q)^2$ and using the facts that $F_y(Q) = 0$ when $[2]Q = \mathcal{O}_E$ and $t(Q) = 2F_x(Q) - a_1F_y(Q)$ otherwise. □

Corollary 25.1.7. *Let E be an elliptic curve defined over $\Bbbk$ and G a finite subgroup of $E(\overline{\Bbbk})$ that is defined over $\Bbbk$. Then there is an elliptic curve $\widetilde{E} = E/G$ defined over $\Bbbk$ and an isogeny $\phi : E \to \widetilde{E}$ defined over $\Bbbk$ with $\ker(\phi) = G$.*

Proof: It suffices to show that the values $t(G)$, $w(G)$ and the rational functions X and Y in Theorem 25.1.6 are fixed by any $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. □

Corollary 25.1.8. *Let $\phi : E \to \widetilde{E}$ be a separable isogeny of odd degree ℓ between elliptic curves over $\Bbbk$. Write $\phi(x,y) = (\phi_1(x), \phi_2(x,y))$, where $\phi_1(x)$ and $\phi_2(x,y)$ are rational functions. Then $\phi_1(x,y) = u(x)/v(x)^2$, where $\deg(u(x)) = \ell$ and $\deg(v(x)) = (\ell-1)/2$. Also, $\phi_2(x,y) = (yw_1(x)+w_2(x))/v(x)^3$, where $\deg(w_1(x)) \leq 3(\ell-1)/2$ and $\deg(w_2(x)) \leq (3\ell-1)/2$.*

Exercise 25.1.9. Prove Corollary 25.1.8.

Definition 25.1.10. An isogeny $\phi : E \to \widetilde{E}$ is **normalised** if $\phi^*(\omega_{\widetilde{E}}) = \omega_E$.

Vélu's formulae give a normalised isogeny. Note that normalised isogenies are incompatible with Theorem 9.7.2 (which, for example, implies $[m]^*(\omega_E) = m\omega_E$). For this reason, in many situations one needs to take an isomorphism from $\widetilde{E}$ to obtain the desired isogeny. Example 25.1.12 shows how this works.

Exercise 25.1.11. Let $\phi : E \to \widetilde{E}$ be an isogeny given by rational functions as in equation (25.1). Show that ϕ is normalised if and only if $c = 1$.

Example 25.1.12. Let $E : y^2 + xy + 3y = x^3 + 2x^2 + 4x + 2$ over $\mathbb{F}_{311}$. Then

$$E[2] = \{\mathcal{O}_E, (-1,-1), (115,252), (117,251)\} \subset E(\mathbb{F}_{311}).$$

Let $G = E[2]$. Applying the Vélu formulae one computes $t(G) = 8$, $w(G) = 306$, $A_1 = 1, A_2 = 2, A_3 = 3, A_4 = 275$ and $A_6 = 276$. One can check that E and

$$\widetilde{E} : Y^2 + XY + 3Y = X^3 + 2X^2 + 275X + 276$$

have the same j-invariant, but they are clearly not the same Weierstrass equation. Hence, the Vélu isogeny with kernel $E[2]$ is not the isogeny $[2] : E \to E$.

To recover the map [2] one needs to find a suitable isomorphism from $\widetilde{E}$ to E. The isomorphism will have the form $(X, Y) \mapsto (u^2X + r, u^3Y + su^2X + t)$ where we must have $u = 1/2$ to have the correct normalisation for the action of the isogeny on the invariant differential (see Exercise 25.1.13). One can verify that taking $r = 291$, $s = 233$ and $t = 67$ gives the required isomorphism from $\widetilde{E}$ to E and that the composition of the Vélu isogeny and this isomorphism is the map [2].

Exercise 25.1.13. Show that if $\phi : (x, y) \mapsto (u^2x + r, u^3y + su^2x + t)$ is an isomorphism from E to $\widetilde{E}$ then $\phi^*(\omega_{\widetilde{E}}) = \frac{1}{u}\omega_E$.

Exercise 25.1.14. Determine the complexity of constructing and computing the Vélu isogeny. More precisely, show that if $d = \#G$ and $G \subset E(\mathbb{F}_{q^n})$ then $O(dM(n, q))$ bit operations are sufficient, where $M(n, q) = M(n \log(nq))$ is the number of bit operations to multiply two degree n polynomials over $\mathbb{F}_q$.

Further, show that if d is an odd prime then $n \leq d - 1$ and so the complexity can be written as $O(d^{2+\epsilon} \log(q)^{1+\epsilon})$ bit operations.

Example 25.1.15. Consider $E : y^2 = x^3 + 2x$ over $\mathbb{F}_{37}$, with $j = 26 \equiv 1728 \pmod{37}$. We have $\#E(\mathbb{F}_{37}) = 2 \cdot 5^2$ so there is a unique point $(0, 0)$ of order 2 over $\mathbb{F}_{37}$ giving a 2-isogeny from E. Using Vélu's formulae one determines that the image of this isogeny is $E_1 : y^2 = x^3 + 29x$, which also has j-invariant 26 and is isomorphic to E over $\mathbb{F}_{37}$.

Now consider the other points of order 2 on E. Let $\alpha \in \mathbb{F}_{37^2}$ satisfy $\alpha^2 = -2$. The isogeny ϕ_2 with kernel $\{\mathcal{O}_E, (\alpha, 0)\}$ maps to $E_2 : y^2 = x^3 + 28\alpha x$, while the isogeny ϕ_3 with kernel $\{\mathcal{O}_E, (-\alpha, 0)\}$ maps to $E_3 : y^2 = x^3 - 28\alpha x$. Note that there is an isomorphism $\psi : E_2 \to E_3$ over $\mathbb{F}_{37^2}$. We have $\hat{\phi_2} \circ \phi_2 = \hat{\phi_3} \circ \phi_3 = [2]$ on E. One can also consider $\hat{\phi_3} \circ \psi \circ \phi_2$ on E, which must be an element of $\mathrm{End}(E) = \mathbb{Z}[i]$ of degree 4. One can show that it is $i[2]$ where $i(x, y) = (-x, 31y)$. Hence, [2] and $\hat{\phi_3} \circ \psi \circ \phi_2$ are equivalent isogenies.

Kohel [350] and Dewaghe [171] independently gave formulae for the Vélu isogeny in terms of the coefficients of the polynomial defining the kernel, rather than in terms of the points in the kernel. We give these formulae in Lemma 25.1.16 for the case where G has odd order (they are also given in Section 2.4 of [350]). Since a $\Bbbk$-rational subgroup of an elliptic curve can have points defined over an extension of $\Bbbk$, working with the coefficients of the polynomial can be more efficient than working with the points in G.

Lemma 25.1.16. *Let $E : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$. Let G be a cyclic subgroup of $E(\overline{\Bbbk})$ of odd order $2d + 1$. Let $G_1 \subseteq G$ be such that $\#G_1 = d$ and $G = \{\mathcal{O}_E\} \cup G_1 \cup \{-Q : Q \in G_1\}$. Define*

$$\psi(x) = \prod_{Q \in G_1} (x - x_Q) = x^d - s_1x^{d-1} + s_2x^{d-2} + \cdots + (-1)^d s_d \tag{25.2}$$

where the s_i are the i-th symmetric polynomials in the roots of $\psi(x)$ (equivalently, in the x-coordinates of elements of G_1). Define $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$. Then there is an isogeny $\phi : E \to \widetilde{E}$, with $\ker(\phi) = G$, of the form $\phi(x, y) = (A(x)/\psi(x)^2, B(x, y)/\psi(x)^3)$ where $A(x)$ and $B(x, y)$ are polynomials. Indeed,

$$\frac{A(x)}{\psi(x)^2} = (2d+1)x - 2s_1 - (4x^3 + b_2x^2 + 2b_4x + b_6)(\psi(x)'/\psi(x))' - (6x^2 + b_2x + b_4)(\psi(x)'/\psi(x)).$$

The proof of Lemma 25.1.16 is given as a sequence of exercises.

Exercise 25.1.17. Let the notation be as in Lemma 25.1.16. Let $F_x(Q)$, $F_y(Q)$, $t(Q)$ and $u(Q)$ be as in Theorem 25.1.6. Show that

$$t(Q) = 6x_Q^2 + b_2 x_Q + b_4 \quad \text{and} \quad u(Q) = 4x_Q^3 + b_2 x_Q^2 + 2b_4 x_Q + b_6.$$

Exercise 25.1.18. Let the notation be as in Lemma 25.1.16. Let $F_x(Q)$, $F_y(Q)$, $t(Q)$ and $u(Q)$ be as in Theorem 25.1.6. Show that

$$\begin{aligned}
\frac{x_Q}{x - x_Q} &= \frac{x}{x - x_Q} - 1, \\
\frac{x_Q}{(x - x_Q)^2} &= \frac{x}{(x - x_Q)^2} - \frac{1}{(x - x_Q)}, \\
\frac{x_Q^2}{(x - x_Q)} &= \frac{x^2}{x - x_Q} - x - x_Q, \\
\frac{x_Q^2}{(x - x_Q)^2} &= \frac{x^2}{(x - x_Q)^2} - \frac{2x}{(x - x_Q)} + 1, \\
\frac{x_Q^3}{(x - x_Q)^2} &= \frac{x^3}{(x - x_Q)^2} - \frac{3x^2}{(x - x_Q)} + 2x + x_Q.
\end{aligned}$$

Exercise 25.1.19. Let the notation be as in Lemma 25.1.16. For $1 \leq i \leq 3$ define

$$S_i = \sum_{Q \in G_1} \frac{1}{(x - x_Q)^i}.$$

Show that $S_1 = \psi(x)'/\psi(x)$ and that $S_2 = -(\psi'(x)/\psi(x))' = ((\psi(x)')^2 - \psi(x)\psi(x)'')/\psi(x)^2$.

Exercise 25.1.20. Complete the proof of Lemma 25.1.16.

Exercise 25.1.21. Determine the complexity of using Lemma 25.1.16 to compute isogenies over finite fields. More precisely, show that if $G \subseteq E(\mathbb{F}_{q^n})$ is defined over $\mathbb{F}_q$ and $d = \#G$ then one can compute $\psi(x)$ in $O(d^2)$ operations in $\mathbb{F}_{q^n}$. Once $\psi(x) \in \mathbb{F}_q[x]$ is computed show that one can compute the polynomials $A(x)$ and $B(x, y)$ for the isogeny in $O(d)$ operations in $\mathbb{F}_q$.

25.2 Isogenies from j-invariants

Vélu's formulae require that one knows the kernel of the desired isogeny. But in some applications one wants to take a $\Bbbk$-rational isogeny of a given degree d (assuming such an isogeny exists) from E to another curve $\widetilde{E}$ (where $\widetilde{E}$ may or may not be known), and one does not know a specific kernel. By Theorem 25.1.2 one can restrict to the case when $d = \ell$ is prime. We usually assume that ℓ is odd, since the case $\ell = 2$ is handled by points of order 2 and Vélu's formulae.

One solution is to choose a random point $P \in E[\ell]$ that generates a $\Bbbk$-rational subgroup of order ℓ. To find such a point, compute the ℓ-division polynomial (which has degree $(\ell^2 - 1)/2$ when ℓ is odd) and find irreducible factors of it in $\Bbbk[x]$ of degree up to $(\ell - 1)/2$. Roots of such factors are points of order ℓ, and one can determine whether or not they generate a $\Bbbk$-rational subgroup by computing all points in the subgroup. Roots of factors of degree $d > (\ell - 1)/2$ cannot give rise to $\Bbbk$-rational subgroups of order ℓ. This approach is expensive when ℓ is large for a number of reasons. For a start, finding roots of degree at most $(\ell - 1)/2$ of a polynomial of degree $(\ell^2 - 1)/2$ in $\mathbb{F}_q[x]$ takes $\Omega(\ell^3 \log(\ell) \log(q))$ bit operations.

A more elegant approach is to use the ℓ-th modular polynomial. It is beyond the scope of this book to present the theory of modular functions and modular curves (some basic references are Sections 5.2 and 5.3 of Lang [366] and Section 11.C of Cox [157]). The fundamental fact is that there is a symmetric polynomial, called the **modular polynomial**[2] $\Phi_\ell(x,y) \in \mathbb{Z}[x,y]$ such that if E is an elliptic curve over a field $\Bbbk$ and $\widetilde{E}$ is an elliptic curve over $\Bbbk$ then there is a separable isogeny of degree ℓ (where $\gcd(\ell, \mathrm{char}(\Bbbk)) = 1$) with cyclic kernel from E to $\widetilde{E}$ if and only if $\Phi_\ell(j(E), j(\widetilde{E})) = 0$ (see Theorem 5, Section 5.3 of Lang [366]). The modular polynomial $\Phi_\ell(x,y)$ is a singular model for the modular curve $X_0(\ell)$ over $\mathbb{Q}$. This modular curve is a moduli space in the sense that a (non-cusp) point of $X_0(\ell)(\Bbbk)$ corresponds to a pair (E,G) where E is an elliptic curve over $\Bbbk$ and where G is a cyclic subgroup of E, defined over $\Bbbk$, of order ℓ. Note that it is possible to have an elliptic curve E together with two distinct cyclic subgroups G_1 and G_2 of order ℓ such that the image curves E/G_1 and E/G_2 are isomorphic; in this case (E,G_1) and (E,G_2) are distinct points of $X_0(\ell)$ but correspond to a repeated root of $\Phi_\ell(j(E),y)$ (it follows from the symmetry of $\Phi_\ell(x,y)$ that this is a singular point on the model). In other words, a repeated root of $\Phi_\ell(j(E),y)$ corresponds to non-equivalent ℓ-isogenies from E to some elliptic curve $\widetilde{E}$.

Since there are $\ell+1$ cyclic subgroups of $E[\ell]$ it follows that $\Phi_\ell(j(E),y)$ has degree $\ell+1$. Indeed, $\Phi_\ell(x,y) = x^{\ell+1} + y^{\ell+1} - (xy)^\ell + \cdots$ with all other terms of lower degree (see Theorem 11.18 of Cox [157] or Theorem 3 of Section 5.2 of Lang [366]). The coefficients of $\Phi_\ell(x,y)$ are large (as seen in Example 25.2.1, even when $\ell = 2$ the coefficients are large).

Example 25.2.1.

$$\begin{aligned}\Phi_2(x,y) &= x^3 + y^3 - x^2y^2 + 1488(x^2y + xy^2) - 162000(x^2 + y^2) \\ &\quad +40773375xy + 8748000000(x+y) - 157464000000000.\end{aligned}$$

Let ℓ be prime. Cohen [138] showed that the number of bits in the largest coefficient of $\Phi_\ell(x,y)$ is $O(\ell \log(\ell))$ (see Bröker and Sutherland [110] for a more precise bound). Since there are roughly ℓ^2 coefficients it follows that $\Phi_\ell(x,y)$ can be written down using $O(\ell^3 \log(\ell))$ bits, and it is believed that this space requirement cannot be reduced. Hence, one expects to perform at least $O(\ell^3 \log(\ell)) = O(\ell^{3+\epsilon})$ bit operations[3] to compute $\Phi_\ell(x,y)$. Indeed, using methods based on modular functions one can conjecturally[4] compute $\Phi_\ell(x,y)$ in $O(\ell^{3+\epsilon})$ bit operations (see Enge [194]). Using modular functions other than the j-function can lead to polynomials with smaller coefficients, but this does not affect the asymptotic complexity.

The fastest method to compute modular polynomials is due to Bröker, Lauter and Sutherland [109]. This method exploits some of the ideas explained later in this chapter (in particular, isogeny volcanoes). The method computes $\Phi_\ell(x,y)$ modulo small primes and then determines $\Phi_\ell(x,y)$ by the Chinese remainder theorem. Under the Generalized Riemann Hypothesis (GRH) the complexity is $O(\ell^3 \log(\ell)^3 \log(\log(\ell)))$ bit operations. For the rest of the chapter we abbreviate the cost as $O(\ell^{3+\epsilon})$ bit operations. The method can also be used to compute $\Phi_\ell(x,y)$ modulo p, in which case the space requirements are $O(\ell^2 \log(\ell)^2 + \ell^2 \log(p))$ bits.

The upshot is that, given an elliptic curve E over $\Bbbk$, the j-invariants of elliptic curves $\widetilde{E}$ that are ℓ-isogenous over $\Bbbk$ (where $\gcd(\ell, \mathrm{char}(\Bbbk)) = 1$) are given by the roots of

[2]The reader should not confuse the modular polynomial $\Phi_\ell(x,y)$ with the cyclotomic polynomial $\Phi_m(x)$.

[3]Recall that a function $f(\ell)$ is $O(\ell^{3+\epsilon})$ if, for every $\epsilon > 0$, there is some $C(\epsilon), L(\epsilon) \in \mathbb{R}_{>0}$ such that $f(\ell) < C(\epsilon)\ell^{3+\epsilon}$ for all $\ell > L(\epsilon)$.

[4]Enge needs an assumption that rounding errors do not affect the correctness of the output.

$\Phi_\ell(j(E), y)$ in $\Bbbk$. When E is ordinary, Theorem 25.4.6 implies that $\Phi_\ell(j(E), y)$ has either $0, 1, 2$ or $\ell + 1$ roots in $\Bbbk$ (counted with multiplicities).

Exercise 25.2.2. Given the polynomial $\Phi_\ell(x, y)$ and a value $j \in \mathbb{F}_q$ show that one can compute $F(y) = \Phi_\ell(j, y) \in \mathbb{F}_q[y]$ in $O(\ell^2(\ell \log(\ell) \log(q) + M(\log(q))))$ bit operations. Show also that one can then compute the roots $\tilde{j} \in \mathbb{F}_q$ of $F(y) = \Phi_\ell(j(E), y)$ (or determine that there are no roots) in expected time bounded by $O(\ell^2 \log(\ell) \log(q))$ field operations (which is $O(\ell^{2+\epsilon} \log(q)^3)$ bit operations).

For the rest of this section we consider algorithms to compute an ℓ-isogeny $\phi : E \to \widetilde{E}$ given an elliptic curve E and the j-invariant of $\widetilde{E}$.

Exercise 25.2.3. Let E be an elliptic curve over $\mathbb{F}_q$ and let E' over $\mathbb{F}_q$ be a twist of E. Show that there is an $\mathbb{F}_q$-rational isogeny of degree ℓ from E (to some elliptic curve) if and only if there is an $\mathbb{F}_q$-rational isogeny of degree ℓ from E'. Show that $\mathrm{End}(E) \cong \mathrm{End}(E')$ (where $\cong$ denotes ring isomorphism).

25.2.1 Elkies' Algorithm

Let $\ell > 2$ be a prime and let E be an elliptic curve over $\Bbbk$ where $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) > \ell + 2$. Assume $j(E) \neq 0, 1728$ (for the case $j(E) \in \{0, 1728\}$ one constructs isogenies using the naive method or the methods of the following sections). Let $\tilde{j} \in \Bbbk$ be such that $\Phi_\ell(j(E), \tilde{j}) = 0$. We also assume that $\tilde{j}$ is a simple root of $\Phi_\ell(j(E), y)$ (more precisely, $(\partial\Phi_\ell(x, y)/\partial x)(j, \tilde{j}) \neq 0$ and $(\partial\Phi_\ell(x, y)/\partial y)(j, \tilde{j}) \neq 0$); see page 248 of Schoof [530] for a discussion of why this condition is not too severe.

Elkies gave a method to determine an explicit equation for an elliptic curve $\widetilde{E}$, such that $j(\widetilde{E}) = \tilde{j}$, and a polynomial giving the kernel of an ℓ-isogeny from E to $\widetilde{E}$. Elkies' original motivation (namely, algorithms for point counting) only required computing the kernel polynomial of the isogeny, but as we have seen, from this information one can easily compute the rational functions describing the isogeny. The method also works when $\ell > 2$ is composite, but that is not of practical relevance. The condition that $\mathrm{char}(\Bbbk)$ not be small (if it is non-zero) is essential.

We use the same notation as in Lemma 25.1.16: $\psi(x)$ is the polynomial of degree $(\ell - 1)/2$ whose roots are the x-coordinates of affine points in the kernel G of the isogeny and s_i are the i-th symmetric polynomials in these roots. We also define

$$p_i = \sum_{P \in G - \{\mathcal{O}_E\}} x_P^i$$

so that $p_1 = 2s_1$ and $p_2 = 2(s_1^2 - 2s_2)$ (these are Newton's formulae; see Lemma 10.7.6). While the value $\tilde{j}$ specifies the equation for the isogenous curve $\widetilde{E}$ (up to isomorphism) it does not, in general, determine the isogeny (see pages 37 and 44 of Elkies [193] for discussion). It is necessary to have some extra information, and for this the coefficient p_1 suffices and can be computed using partial derivatives of the modular polynomial (this is why the condition on the partial derivatives is needed).

The explanation of Elkies' algorithm requires theory that we do not have space to present. We refer to Schoof [530] for a good summary of the details (also see Elkies [193] for further discussion). The basic idea is to use the fact (Deuring lifting theorem) that the isogeny lifts to an isogeny between elliptic curves over $\mathbb{C}$. One can then interpret the ℓ-isogeny in terms of Tate curves[5] $\mathbb{C}^*/q^{\mathbb{Z}}$ (we have not presented the Tate curve in this

[5]The notation q here refers to $q(z) = \exp(2\pi i z)$ and not a prime power.

book; see Section C.14 of [564] or Section 5.3 of [565]) as a map from $q(z)$ to $q(z)^\ell$. As discussed on page 40 of Elkies [193], this isogeny is not normalised. There are a number of relations between the modular j-function, certain Eisenstein series, the equation of the elliptic curve (in short Weierstrass form) and the kernel polynomial of the isogeny. These relations give rise to formulae that must also hold over $\Bbbk$. Hence, one can work entirely over $\Bbbk$ and obtain the kernel polynomial.

The details of this approach are given in Sections 7 and 8 of Schoof [530]. In particular: Theorem 7.3 shows how to get j' (derivative); Proposition 7.1 allows one to compute the coefficients of the elliptic curve; Proposition 7.2 gives the coefficient p_1 of the kernel polynomial (which is a function of values specified in Proposition 7.1 and Theorem 7.3). The coefficients of the kernel polynomial are related to the coefficients of the series expansion of the Weierstrass ζ-function (see Theorem 8.3 of [530]).

The algorithm is organised as follows (see Algorithm 28). One starts with an ordinary elliptic curve $E : y^2 = x^3 + Ax + B$ over $\Bbbk$ and $j = j(E)$. We assume that $j \notin \{0, 1728\}$ and $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(k) > \ell + 2$. Let $\phi_x = (\frac{\partial \Phi_\ell}{\partial x})(j, \tilde{\jmath})$, $\phi_y = (\frac{\partial \Phi_\ell}{\partial y})(j, \tilde{\jmath})$, $\phi_{xx} = (\frac{\partial^2 \Phi_\ell}{\partial x^2})(j, \tilde{\jmath})$, $\phi_{yy} = (\frac{\partial^2 \Phi_\ell}{\partial y^2})(j, \tilde{\jmath})$ and $\phi_{xy} = (\frac{\partial^2 \Phi_\ell}{\partial x \partial y})(j, \tilde{\jmath})$. One computes the derivative j' and the corresponding values for E_4 and E_6. Given $\tilde{\jmath}$ one computes $\tilde{\jmath}'$ and then the coefficients $\tilde{A}$ and $\tilde{B}$ of the image curve $\tilde{E}$. Finally one computes p_1, from which it is relatively straightforward to compute all the coefficients of the kernel polynomial $\psi(x)$.

Algorithm 28 Elkies' algorithm (Source code provided by Drew Sutherland)

INPUT: $A, B \in \Bbbk$, $\ell > 2$, $j, \tilde{\jmath} \in \Bbbk$
OUTPUT: $\tilde{A}, \tilde{B}, \psi(x)$

Compute ϕ_x, ϕ_y, ϕ_{xx}, ϕ_{yy} and ϕ_{xy} ▷ Compute $\tilde{A}$ and $\tilde{B}$
Let $m = 18B/A$, let $j' = mj$, and let $k = j'/(1728 - j)$
Let $\tilde{\jmath}' = -j'\phi_x/(\ell\phi_y)$, let $\tilde{m} = \tilde{\jmath}'/\tilde{\jmath}$, and let $\tilde{k} = \tilde{\jmath}'/(1728 - \tilde{\jmath})$
Let $\tilde{A} = \ell^4 \tilde{m}\tilde{k}/48$ and $\tilde{B} = \ell^6 \tilde{m}^2 \tilde{k}/864$
Let $r = -(j'^2\phi_{xx} + 2\ell j'\tilde{\jmath}'\phi_{xy} + \ell^2\tilde{\jmath}'^2\phi_{yy})/(j'\phi_x)$ ▷ Compute p_1
Let $p_1 = \ell(r/2 + (k - \ell\tilde{k})/4 + (\ell\tilde{m} - m)/3)$
Let $d = (\ell - 1)/2$ ▷ Compute the power sums t_n of the roots of $\psi(x)$
Let $t_0 = d$, $t_1 = p_1/2$, $t_2 = ((1-10d)A - \tilde{A})/30$, and $t_3 = ((1-28d)B - 42t_1A - \tilde{B})/70$
Let $c_0 = 0$, $c_1 = 6t_2 + 2At_0$, $c_2 = 10t_3 + 6At_1 + 4Bt_0$
for $n = 2$ to $d - 1$ **do**
    Let $s = \sum_{i=1}^{n-1} c_i c_{n-i}$
    Let
$$c_{n+1} = \frac{3s - (2n-1)(n-1)Ac_{n-1} - (2n-2)(n-2)Bc_{n-2}}{(n-1)(2n+5)}$$
end for
for $n = 3$ to $d - 1$ **do**
    Let
$$t_{n+1} = \frac{c_n - (4n-2)At_{n-1} - (4n-4)Bt_{n-2}}{4n+2}$$
end for
Let $s_0 = 1$ ▷ Compute the symmetric functions s_n of the roots of $\psi(x)$
for $n = 1$ to d **do**
    Let $s_n = \frac{-1}{n} \sum_{i=1}^{n} (-1)^i t_i s_{n-i}$
end for
return $\psi(x) = \sum_{i=0}^{d} (-1)^i s_i x^{d-i}$

Exercise 25.2.4. Show that Elkies' algorithm requires $O(d^2) = O(\ell^2)$ operations in $\mathbb{k}$.

Bostan, Morain, Salvy and Schost [93] have given algorithms (exploiting fast arithmetic on power series) based on Elkies' methods. The algorithms apply when the characteristic of the field is zero or is sufficiently large compared with ℓ. There is a slight difference in scope: Elkies' starts with only j-invariants whereas Bostan et al assume that one is given elliptic curves E and $\widetilde{E}$ in short Weierstrass form such that there is a normalised isogeny of degree ℓ over $\mathbb{k}$ from E to $\widetilde{E}$. In general, one needs to perform Elkies' method before one has such an equation for $\widetilde{E}$ and so the computations with modular curves still dominate the cost. Theorem 2 of [93] states that one can compute the rational functions giving the isogeny in $O(M(\ell))$ operations in $\mathbb{k}$ when $\mathrm{char}(\mathbb{k}) > 2\ell - 1$ and when the coefficient p_1 is known. Note that Bostan et al are not restricted to prime degree isogenies. An application of the result of Bostan et al is to determine whether there is a normalised isogeny from E to $\widetilde{E}$ *without* needing to compute modular polynomials. Lercier and Sirvent [384] (again, assuming one is given explicit equations for E and $\widetilde{E}$ such that there is a normalised ℓ-isogeny between them) have showed how to achieve a similarly fast method even when the characteristic of the field is small.

A number of calculations can fail when $\mathrm{char}(\mathbb{k})$ is non-zero but small compared with ℓ, due to divisions by small integers arising in the power series expansions for the modular functions. Algorithms for the case of small characteristic will be mentioned in Section 25.2.3.

25.2.2 Stark's Algorithm

Stark [581] gave a method to compute the rational function giving the x-coordinate of an endomorphism $\phi : E \to E$ corresponding to a complex number β (interpreting $\mathrm{End}(E)$ as a subset of $\mathbb{C}$). The idea is to use the fact that, for an elliptic curve E over the complex numbers given by short Weierstrass form,

$$\wp(\beta z) = \frac{A(\wp(z))}{B(\wp(z))} \tag{25.3}$$

where A and B are polynomials and where $\wp(z) = z^{-2} + 3G_4 z^2 + \cdots$ is the Weierstrass function (see Theorem VI.3.5 of Silverman [564]). This isogeny is not normalised (since $\wp(\beta z) = \beta^{-2} z^{-2} + \cdots$ it follows that the pullback of ω_E under ϕ is $\beta\omega_E$). Stark's idea is to express $\wp$ as a (truncated) power series in z; the coefficients of this power series are determined by the coefficients of the elliptic curve E. One computes A and B by taking the continued fraction expansion of the left hand side of equation (25.3). One can apply this algorithm to curves over finite fields by applying the Deuring lifting theorem. Due to denominators in the power series coefficients of $\wp(z)$ the method only works when $\mathrm{char}(\mathbb{k}) = 0$ or $\mathrm{char}(\mathbb{k})$ is sufficiently large. Stark's paper [581] gives a worked example in the case $\beta = \sqrt{-2}$.

The idea generalises to normalised isogenies $\phi : E \to \widetilde{E}$ by writing $\wp_{\widetilde{E}}(z) = A(\wp_E(z))/B(\wp_E(z))$ where now the power series for $\wp_E(z)$ and $\wp_{\widetilde{E}}(z)$ are different since the elliptic curve equations are different. Note that it is necessary to have actual curve equations for the normalised isogeny, not just j-invariants. We refer to Section 6.2 of Bostan, Morain, Salvy and Schost [93] for further details and complexity estimates.

25.2.3 The Small Characteristic Case

As we have seen, the Elkies and Stark methods require the characteristic of the ground field to be either zero or relatively large since they use lifting to short Weierstrass forms

over $\mathbb{C}$ and since the power series expansions have rational coefficients that are divisible by various small primes. Hence, there is a need for algorithms that handle the case when $\mathrm{char}(\Bbbk)$ is small (especially, $\mathrm{char}(\Bbbk) = 2$). A number of such methods have been developed by Couveignes, Lercier, Morain and others. We briefly sketch Couveignes' "second method" [155].

Let p be the characteristic of the field. We assume that p is "small" (in the sense that an algorithm performing p operations is considered efficient). Let E and $\widetilde{E}$ be ordinary[6] elliptic curves over $\mathbb{F}_{p^m}$.

The basic idea is to use the fact that if $\phi : E \to \widetilde{E}$ is an isogeny of odd prime degree $\ell \neq p$ (isogenies of degree p are easy: they are either Frobenius or Verschiebung) then ϕ maps points of order p^k on E to points of order p^k on $\widetilde{E}$. Hence, one can try to determine the rational functions describing ϕ by interpolation from their values on $E[p^k]$. One could interpolate using any torsion subgroup of E, but using $E[p^k]$ is the best choice since it is a cyclic group and so there are only $\varphi(p^k) = p^k - p^{k-1}$ points to check (compared with $\varphi(n^2)$ if using $E[n]$). The method can be applied to any elliptic curve $\widetilde{E}$ in the isomorphism class, so in general it will not return a normalised isogeny.

Couveignes' method is as follows: First, compute points $P \in E[p^k] - E[p^{k-1}]$ and $\widetilde{P} \in \widetilde{E}[p^k] - \widetilde{E}[p^{k-1}]$ over $\overline{\mathbb{F}}_p$ and guess that $\phi(P) = \widetilde{P}$. Then try to determine the rational function $\phi_1(x) = u(x)/v(x)$ by interpolating $\phi_1(x([i]P)) = x([i]\widetilde{P})$; if this does not work then try another guess for $\widetilde{P}$. The interpolation is done as follows (we assume $p^k > 2\ell$). First, compute a polynomial $A(x)$ of degree d where $2\ell < d \leq p^k$ such that $A(x([i]P)) = x([i]\widetilde{P})$ for $1 \leq i \leq d$. Also compute $B(x) = \prod_{i=1}^{d}(x - x([i]P))$. If the guess for $\widetilde{P}$ is correct then $A(x) \equiv u(x)/v(x) \pmod{B(x)}$ where $\deg(u(x)) = \ell, \deg(v(x)) = \ell - 1$ and $v(x)$ is a square. Writing this equation as $A(x)v(x) = u(x) + B(x)w(x)$ it follows that $u(x)$ and $v(x)$ can be computed using Euclid's algorithm. The performance of the algorithm depends on the method used to determine points in $E[p^k]$, but is dominated by the fact that these points lie in an extension of the ground field of large degree, and that one expects to try around $\frac{1}{2}p^k \approx \ell$ choices for $\widetilde{P}$ before hitting the right one. The complexity is polynomial in ℓ, p and m (where E is over $\mathbb{F}_{p^m}$). When $p = 2$ the fastest method was given by Lercier [382]. For further details we refer to the surveys by Lercier and Morain [383] and De Feo [202].

25.3 Isogeny Graphs of Elliptic Curves over Finite Fields

Let E be an elliptic curve over $\mathbb{F}_q$. The $\mathbb{F}_q$-**isogeny class** of E is the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ that are isogenous over $\mathbb{F}_q$ to E. Tate's isogeny theorem states that two elliptic curves E and $\widetilde{E}$ over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if $\#E(\mathbb{F}_q) = \#\widetilde{E}(\mathbb{F}_q)$ (see Theorem 9.7.4 for one implication).

We have seen in Sections 9.5 and 9.10 that the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ is roughly $2q$ and that there are roughly $4\sqrt{q}$ possible values for $\#E(\mathbb{F}_q)$. Hence, if isomorphism classes were distributed uniformly across all group orders one would expect around $\frac{1}{2}\sqrt{q}$ elliptic curves in each isogeny class. The theory of complex multiplication gives a more precise result (as mentioned in Section 9.10.1). We

[6]The restriction to ordinary curves is not a significant problem. In practice we are interested in elliptic curves over $\mathbb{F}_{p^m}$ where m is large, whereas supersingular curves are all defined over $\mathbb{F}_{p^2}$. Indeed, for small p there are very few supersingular curves, and isogenies of small degree between them can be computed by factoring division polynomials and using Vélu's formulae.

denote by π_q the q-power Frobenius map; see Section 9.10 for its properties. The number of $\mathbb{F}_q$-isomorphism classes of ordinary elliptic curves over $\mathbb{F}_q$ with $q+1-t$ points is the Hurwitz class number of the ring $\mathbb{Z}[\pi_q] = \mathbb{Z}[(t+\sqrt{t^2-4q})/2]$. This is the sum of the ideal class numbers $h(\mathcal{O})$ over all orders $\mathbb{Z}[\pi_q] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. It follows (see Remark 9.10.19) that there are $O(q^{1/2}\log(q)\log(\log(q)))$ elliptic curves in each isogeny class. For supersingular curves see Theorem 9.11.12.

Definition 25.3.1. Let E be an elliptic curve over a field $\Bbbk$ of characteristic p. Let $S \subseteq \mathbb{N}$ be a finite set of primes. Define

$$X_{E,\Bbbk,S}$$

to be the (directed) graph[7] with vertex set being the $\Bbbk$-isogeny class of E. Vertices are typically labelled by $j(\widetilde{E})$, though we also speak of "the vertex $\widetilde{E}$".[8] There is a (directed) edge $(j(E_1), j(E_2))$ labelled by ℓ for each equivalence class of ℓ-isogenies from E_1 to E_2 defined over $\Bbbk$ for some $\ell \in S$. We usually treat this as an undirected graph, since for every ℓ-isogeny $\phi : E_1 \to E_2$ there is a dual isogeny $\widehat{\phi} : E_2 \to E_1$ of degree ℓ (though see Remark 25.3.2 for an unfortunate, though rare, complication).

Remark 25.3.2. Edges in the isogeny graph correspond to equivalence classes of isogenies. It can happen that two non-equivalent isogenies from $E_1 \to E_2$ have equivalent dual isogenies from $E_2 \to E_1$. It follows that there are two directed edges in the graph from E_1 to E_2 but only one directed edge from E_2 to E_1. (Note that this does not contradict the fact that isogenies satisfy $\widehat{\widehat{\phi}} = \phi$, as we are speaking here about isogenies up to equivalence.) Such an issue was already explained in Exercise 25.1.1; it only arises if $\#\mathrm{Aut}(E_2) > 2$ (i.e., if $j(E_2) = 0, 1728$).

Definition 25.3.3. A (directed) graph is **k-regular** if every vertex has (out-)degree k (a loop is considered as having degree 1). A **path** in a graph is a sequence of (directed) edges between vertices, such that the end vertex of one edge is the start vertex of the next. We will also describe a path as a sequence of vertices. A graph is connected if there is a path from every vertex to every other vertex. The **diameter** of a connected graph is the maximum, over all pairs v_1, v_2 of vertices in the graph, of the length of the shortest path from v_1 to v_2.

There are significant differences (both in the structure of the isogeny graph and the way it is used in applications) between the ordinary and supersingular cases. So we present them separately.

25.3.1 Ordinary Isogeny Graph

Fix an ordinary elliptic curve E over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = q+1-t$. The isogeny graph of elliptic curves isogenous over $\mathbb{F}_q$ to E can be identified, using the theory of complex multiplication, with a graph whose vertices are ideal classes (in certain orders). The goal of this section is to briefly sketch this theory in the special case (the general case is given in Section 25.4) of the sub-graph where all elliptic curves have the same endomorphism ring, in which case the edges correspond to multiplication by prime ideals. We do not

[7] Some authors would use the name "multi-graph", since there can be loops and/or multiple edges between vertices.

[8] In the supersingular case one can label vertices as $j(\widetilde{E})$ without ambiguity only when $\Bbbk$ is algebraically closed: when $\Bbbk$ is finite then, in the supersingular case, one has two distinct vertices in the graph for $\widetilde{E}$ and its quadratic twist. For the ordinary case there is no ambiguity by Lemma 9.11.13 (also see Exercise 25.3.8).

have space to give all the details; good references for the background are Cox [157] and Lang [366].

The endomorphism ring of E (over $\overline{\mathbb{F}}_q$) is an order $\mathcal{O}$ in the quadratic imaginary field $K = \mathbb{Q}(\sqrt{t^2-4q})$. (We refer to Section A.12 for background on orders and conductors.) Let $\mathcal{O}_K$ be the ring of integers of K. Then $\mathbb{Z}[\pi_q] = \mathbb{Z}[(t+\sqrt{t^2-4q})/2] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ and if $\mathcal{O}_K = \mathbb{Z}[\theta]$ then $\mathcal{O} = \mathbb{Z}[c\theta]$ where c is the conductor of $\mathcal{O}$. The ideal class group $\mathrm{Cl}(\mathcal{O})$ is defined to be the classes of invertible $\mathcal{O}$-ideals that are prime to the conductor; see Section 7 of [157] or Section 8.1 of [366]. There is an explicit formula for the order $h(\mathcal{O})$ of the ideal class group $\mathrm{Cl}(\mathcal{O})$ in terms of the class number $h(\mathcal{O}_K)$ of the number field; see Theorem 7.24 of [157] or Theorem 8.7 of [366].

There is a one-to-one correspondence between the set of isomorphism classes of elliptic curves E over $\mathbb{F}_q$ with $\mathrm{End}(E) = \mathcal{O}$ and the set $\mathrm{Cl}(\mathcal{O})$. Precisely, to an invertible $\mathcal{O}$-ideal $\mathfrak{a}$ one associates the elliptic curve $E = \mathbb{C}/\mathfrak{a}$ over $\mathbb{C}$. An $\mathcal{O}$-ideal $\mathfrak{a}'$ is equivalent to $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ if and only if $\mathbb{C}/\mathfrak{a}'$ is isomorphic to E. One can show that $\mathrm{End}(E) = \mathcal{O}$. The theory of complex multiplication shows that E is defined over a number field (called the ring class field) and has good reduction modulo the characteristic p of $\mathbb{F}_q$. This correspondence is not canonical, since the reduction modulo p map is not well-defined (it depends on a choice of prime ideal above p in the ring class field).

Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal and $E = \mathbb{C}/\mathfrak{a}$. Let $\mathfrak{l}$ be an invertible $\mathcal{O}$-ideal and, interpreting $\mathfrak{l} \subseteq \mathrm{End}(E)$, consider the set $E[\mathfrak{l}] = \{P \in E(\mathbb{C}) : \phi(P) = \mathcal{O}_E \text{ for all } \phi \in \mathfrak{l}\}$. Since $\mathcal{O} \subseteq \mathbb{C}$ we can interpret $\mathfrak{l} \subseteq \mathbb{C}$, in which case

$$\begin{aligned} E[\mathfrak{l}] &\cong \{z \in \mathbb{C}/\mathfrak{a} : \alpha z \in \mathfrak{a}, \text{ for all } \alpha \in \mathfrak{l}\} \\ &\cong \mathfrak{l}^{-1}\mathfrak{a}/\mathfrak{a}. \end{aligned}$$

It follows that $\#E[\mathfrak{l}]$ is equal to the norm of the ideal $\mathfrak{l}$. The identity map on $\mathbb{C}$ induces the isogeny

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{l}^{-1}\mathfrak{a}$$

with kernel $\mathfrak{l}^{-1}\mathfrak{a}/\mathfrak{a} \cong E[\mathfrak{l}]$. The above remarks apply to elliptic curves over $\mathbb{C}$, but the theory reduces well to elliptic curves over finite fields, and indeed, every isogeny from E to an elliptic curve $\widetilde{E}$ with $\mathrm{End}(E) = \mathrm{End}(\widetilde{E})$ arises in this way. This shows that, not only do ordinary elliptic curves correspond to ideals in $\mathcal{O}$, but so do their isogenies.

Exercise 25.3.4. Show that if $\mathfrak{l} = (\ell)$ where $\ell \in \mathbb{N}$ then the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{l}^{-1}\mathfrak{a}$ is $[\ell]$.

Exercise 25.3.5. Suppose the prime ℓ splits in $\mathcal{O}$ as $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$ in $\mathcal{O}$. Let $\phi : E \to \widetilde{E}$ correspond to the ideal $\mathfrak{l}_1$. Show that $\widehat{\phi}$ corresponds to $\mathfrak{l}_2$.

Let ℓ be a prime. Then ℓ splits in $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if the minimal polynomial of θ factors modulo ℓ with two linear factors. If D is the discriminant of K then ℓ splits if and only if the Kronecker symbol satisfies $(\frac{D}{\ell}) = +1$. Note that the Kronecker symbol is the Legendre symbol when ℓ is odd and

$$(\tfrac{D}{2}) = \begin{cases} 0 & D \equiv 0 \pmod 4, \\ 1 & D \equiv 1 \pmod 8, \\ -1 & D \equiv 5 \pmod 8. \end{cases} \tag{25.4}$$

Let E be an elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}(E) = \mathcal{O}$ and let ℓ be coprime to the conductor of $\mathcal{O}$. There are $1 + (\frac{D}{\ell})$ prime ideals $\mathfrak{l}$ above ℓ, and so there are this many isogenies of degree ℓ from E. It follows that there are ℓ-isogenies in the isogeny graph for roughly half the primes ℓ.[9]

[9] Of course, there are still $\ell + 1$ isogenies of degree ℓ for each ℓ, but the rest of them are not to curves $\widetilde{E}$ such that $\mathrm{End}(\widetilde{E}) = \mathcal{O}$.

Let E be an elliptic curve over $\mathbb{F}_q$ corresponding to an $\mathcal{O}$-ideal $\mathfrak{a}$. Let $S \subseteq \mathbb{N}$ be a finite set of primes that are all co-prime to the conductor. Let G be the component of E in the isogeny graph $X_{E,\mathbb{F}_q,S}$ of Definition 25.3.1. Let $S' = \{\mathfrak{l}_1, \ldots, \mathfrak{l}_k\}$ be the set of classes of invertible $\mathcal{O}$-ideals above primes $\ell \in S$ and let $\langle S' \rangle$ be the subgroup of $\mathrm{Cl}(\mathcal{O})$ generated by S'. From the above discussion it follows that G can be identified with the graph whose vertices are the $\mathcal{O}$-ideal classes in the coset $\mathfrak{a}\langle S' \rangle$ and such that, for each $\mathfrak{b} \in \mathfrak{a}\langle S' \rangle$ and each $\mathfrak{l}_i \in S'$ there is an edge between $\mathfrak{b}$ and $\mathfrak{l}_i^{-1}\mathfrak{b}$. Since ideal class groups are well-understood, this correspondence illuminates the study of the isogeny graph. For example, an immediate corollary is that the graph of elliptic curves E with $\mathrm{End}(E) = \mathcal{O}$ is connected if and only if S' generates $\mathrm{Cl}(\mathcal{O})$. A well-known result of Bach states that (assuming the Riemann hypothesis for the Dedekind zeta function of K and Hecke L-functions for characters of $\mathrm{Cl}(\mathcal{O}_K)$) the group $\mathrm{Cl}(\mathcal{O}_K)$ is generated by prime ideals of norm less than $6\log(|\Delta_K|)^2$ (see page 376 of [20]) where Δ_K is the discriminant of $\mathcal{O}_K$. Another immediate corollary is that the graph is regular (i.e., every vertex has the same degree).

Remark 25.3.6. We stress that there is no canonical choice of $\mathcal{O}$-ideal $\mathfrak{a}$ corresponding to an elliptic curve E with $\mathrm{End}(E) = \mathcal{O}$. However, given a pair $(E, \widetilde{E})$ of isogenous elliptic curves with $\mathrm{End}(E) = \mathrm{End}(\widetilde{E}) = \mathcal{O}$ the ideal class corresponding to the isogeny between them is well-defined. More precisely, if E is identified with $\mathbb{C}/\mathfrak{a}$ for some $\mathcal{O}$-ideal $\mathfrak{a}$ then there is a unique ideal class represented by $\mathfrak{b}$ such that $\widetilde{E}$ is identified with $\mathbb{C}/\mathfrak{b}^{-1}\mathfrak{a}$. The only algorithm known to find such an ideal $\mathfrak{b}$ is to compute an explicit isogeny from E to $\widetilde{E}$ (using algorithms presented later in this chapter) and then determine the corresponding ideal. If one could determine $\mathfrak{b}$ efficiently from E and $\widetilde{E}$ then navigating the ordinary isogeny graph would be much easier.

Exercise 25.3.7. Let E_1 be an elliptic curve with $\mathrm{End}(E_1) = \mathcal{O}$. Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}$ above ℓ. Suppose $\mathfrak{l}$ has order d in $\mathrm{Cl}(\mathcal{O})$. Show that there is a cycle $E_1 \to E_2 \to \cdots \to E_d \to E_1$ of ℓ-isogenies.

Exercise 25.3.8. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ and let E' be the quadratic twist of E. Show that the graphs $X_{E,\mathbb{F}_q,S}$ and $X_{E',\mathbb{F}_q,S}$ are identical.

Remark 25.3.9. Let ℓ split in $\mathcal{O} = \mathbb{Z}[\theta] \subseteq \mathrm{End}(E)$ and let $\mathfrak{l}_1 = (\ell, a+\theta)$ and $\mathfrak{l}_2 = (\ell, b+\theta)$ be the corresponding prime ideals. Given an isogeny $\phi : E \to \widetilde{E}$ of degree ℓ one can determine whether ϕ corresponds to $\mathfrak{l}_1$ or $\mathfrak{l}_2$ as follows: Compute (using the Elkies method if only $j(E)$ and $j(\widetilde{E})$ are known) the polynomial determining the kernel of ϕ; compute an explicit point $P \in \ker(\phi)$; check whether $[a]P + \theta(P) = \mathcal{O}_E$ or $[b]P + \theta(P) = \mathcal{O}_E$, where θ is now interpreted as an element of $\mathrm{End}(E)$. This trick is essentially due to Couveignes, Dewaghe, and Morain (see Section 3.2 of [156]; also see pages 49-50 of Kohel [350] and Galbraith, Hess and Smart [221]).

Remark 25.3.10. The ideas mentioned above show that all elliptic curves over $\mathbb{F}_q$ with the same endomorphism ring are isogenous over $\mathbb{F}_q$. Combined with the results of Section 25.4 one can prove Tate's isogeny theorem, namely that any two elliptic curves over $\mathbb{F}_q$ with the same number of points are isogenous over $\mathbb{F}_q$.

More details about the structure of the ordinary isogeny graph will be given in Section 25.4. In particular, that section will discuss isogenies between elliptic curves whose endomorphism rings are different orders in the same quadratic field.

25.3.2 Expander Graphs and Ramanujan Graphs

Let X be a finite (directed) graph on vertices labelled $\{1, \ldots, n\}$. The **adjacency matrix** of X is the $n \times n$ integer matrix A with $A_{i,j}$ being the number of edges from vertex i to vertex j. The **eigenvalues of a finite graph** X are defined to be the eigenvalues of its adjacency matrix A. For the rest of this section we assume that all graphs are un-directed. Since the adjacency matrix of an un-directed graph is real and symmetric, the eigenvalues are real.

Lemma 25.3.11. *Let X be a k-regular graph. Then k is an eigenvalue, and all eigenvalues λ are such that $|\lambda| \leq k$.*

Proof: The first statement follows since $(1, 1, \ldots, 1)$ is an eigenvector with eigenvalue k. The second statement is also easy (see Proposition 1.1.2 of Davidoff, Sarnak and Valette [166] or Theorem 1 of Murty [446]). □

Let X be a k-regular graph. We denote by $\lambda(X)$ the maximum of the absolute values of all the eigenvalues that are not equal to $\pm k$. Alon and Boppana showed that the lim inf of $\lambda(X)$ over any family of k-regular graphs (as the number of vertices goes to ∞) is at least $2\sqrt{k-1}$ (see Theorem 1.3.1 of Davidoff, Sarnak and Valette [166], Theorem 3.2 of Pizer [481] or Theorem 10 of Murty [446]). The graph X is said to be **Ramanujan** if $\lambda(X) \leq 2\sqrt{k-1}$. Define $\lambda_1(X)$ to be the largest eigenvalue that is strictly less than k.

Let G be a finite group and S a subset of G such that $g \in S$ implies $g^{-1} \in S$ (we also allow S to be a multi-set). The **Cayley graph** of G is the graph X with vertex set G and an edge between g and gs for all $g \in G$ and all $s \in S$. Murty [446] surveys criteria for when a Cayley graph is a Ramanujan graph. If certain character sums are small then X may be a Ramanujan graph; see Section 2 of [446].

Definition 25.3.12. Let X be a graph and A a subset of vertices of X. The **vertex boundary** of A in X is

$$\delta_v(A) = \{v \in X - A : \text{ there is an edge between } v \text{ and a vertex in } A\}.$$

Let E_X be the set of edges (x, y) in X. The **edge boundary** of A in X is

$$\delta_e(A) = \{(x, y) \in E_X : x \in A \text{ and } y \in X - A\}.$$

Let $c > 0$ be real. A k-regular graph X with $\#X$ vertices is a **c-expander** if, for all subsets $A \subseteq X$ such that $\#A \leq \#X/2$,

$$\#\delta_v(A) \geq c\#A.$$

Exercise 25.3.13. Show that $\delta_v(A) \leq \delta_e(A) \leq k\delta_v(A)$.

Exercise 25.3.14. Let X be a k-regular graph with n vertices that is a c-expander. Show that if n is even then $0 \leq c \leq 1$ and if n is odd then $0 \leq c \leq (n+1)/(n-1)$.

Expander graphs have a number of theoretical applications; one important property is that random walks on expander graphs reach the uniform distribution quickly.

Let X be a k-regular graph. Then

$$\#\delta_e(A) \geq \frac{k - \lambda_1(X)}{2}\#A \tag{25.5}$$

when $\#A \leq \#X/2$ (see Theorem 1.3.1 of Davidoff, Sarnak and Valette [166] or Section 4 of Murty [446][10]). Hence $\#\delta_v(A) \geq (\frac{1}{2} - \lambda_1(X)/(2k))\#A$ and so Ramanujan graphs are expander graphs. Indeed, small values for $\lambda_1(X)$ give large expansion factors. We refer to [166, 446] for further details, and references.

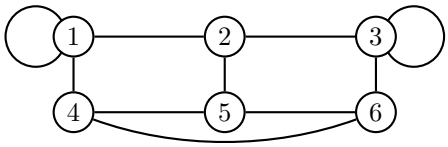


Figure 25.1: A 3-regular graph.

Exercise 25.3.15. Consider the 3-regular graph X in Figure 25.1. Determine the eigenvalues of X. Is this graph Ramanujan? Determine $\delta_v(\{1\})$, $\delta_v(\{1,2\})$ and $\delta_v(\{1,3\})$. Verify that $\#\delta_v(A) \geq \#A$ for all subsets A of vertices of X such that $\#A \leq 3$ and so X is an expander.

Exercise 25.3.16. For every $c > 0$ find an integer $n \in \mathbb{N}$, a graph X with n vertices, and a subset A of X such that $\#A \leq n/2$ but $\#\delta_v(A) < c\#A$. (Such a graph is very far from being an expander.)

Consider the ordinary isogeny graph of elliptic curves over $\mathbb{F}_q$ with $\mathrm{End}(E) = \mathcal{O}_K$, the ring of integers in $K = \mathbb{Q}(\sqrt{t^2 - 4q})$. This was shown in the previous section to be a Cayley graph for the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$. Jao, Miller and Venkatesan [311] show, assuming a generalisation of the Riemann hypothesis, that the ordinary isogeny graph is an expander graph (indeed, it is "nearly Ramanujan", i.e., $\lambda_1(X) \leq O(k^\beta)$ for some $0 < \beta < 1$).

25.3.3 Supersingular Isogeny Graph

For the supersingular isogeny graph we work over $\overline{\mathbb{F}}_p$. The graph is finite. Indeed, Theorem 9.11.12 implies $p/12 - 1 < \#X_{E,\overline{\mathbb{F}}_p,S} < p/12 + 2$. Note that it suffices to consider elliptic curves defined over $\mathbb{F}_{p^2}$ (although the isogenies between them are over $\overline{\mathbb{F}}_p$ in general).

In contrast to the ordinary case, the supersingular graph is always connected using isogenies of any fixed degree. A proof of this result, attributed to Serre, is given in Section 2.4 of Mestre [419].

Theorem 25.3.17. *Let p be a prime and let E and $\widetilde{E}$ be supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Let ℓ be a prime different from p. Then there is an isogeny from E to $\widetilde{E}$ over $\overline{\mathbb{F}}_p$ whose degree is a power of ℓ.*

Proof: See Corollary 78 of Kohel [350] or Section 2.4 of Mestre [419]. □

Hence, one can choose any prime ℓ (e.g., $\ell = 2$) and consider the ℓ-isogeny graph $X_{E,\overline{\mathbb{F}}_p,\{\ell\}}$ on supersingular curves over $\overline{\mathbb{F}}_p$. It follows that the graph is $(\ell+1)$-regular and connected.

Exercise 25.3.18. Let $p = 103$. Determine, using Theorem 9.11.12, the number of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ and over $\mathbb{F}_{p^2}$. Determine the 2-isogeny graph whose vertices are supersingular elliptic curves over $\mathbb{F}_{p^2}$.

Exercise 25.3.19. Determine the supersingular 2-isogeny graph over $\mathbb{F}_{11}$. Interpret the results in light of Remark 25.3.2.[11]
[Hint: The isomorphism classes of elliptic curves with $j(E) = 0$ and $j(E) = 1728$ are supersingular modulo 11; this follows from the theory of complex multiplication and the facts that $(\frac{-3}{11}) = (\frac{-4}{11}) = -1$.]

[10] Note that the proof on page 16 of [446] is for $\delta_e(A)$, not $\delta_v(A)$ as stated.
[11] This example was shown to me by David Kohel.

Exercise 25.3.20. Find a prime p such that the set of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ does not form a connected subgraph of $X_{E,\overline{\mathbb{F}}_p,\{2\}}$.

There is a one-to-one correspondence between supersingular elliptic curves E over $\overline{\mathbb{F}}_p$ and projective right modules of rank 1 of a maximal order of the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞ (see Section 5.3 of Kohel [350] or Gross [268]). Pizer has exploited this structure (and connections with Brandt matrices and Hecke operators) to show that the supersingular isogeny graph is a Ramanujan graph. Essentially, the Brandt matrix gives the adjacency matrix of the graph. A good survey is [481], though be warned that the paper does not mention the connection to supersingular elliptic curves.

The supersingular isogeny graph has been used by Charles, Goren and Lauter [128] to construct a cryptographic hash function. It has also been used by Mestre and Oesterlé [419] for an algorithm to compute coefficients of modular forms.

25.4 The Structure of the Ordinary Isogeny Graph

This section presents Kohel's results on the structure of the isogeny graph of ordinary elliptic curves over finite fields. Section 25.4.2 gives Kohel's algorithm to compute $\mathrm{End}(E)$ for a given ordinary elliptic curve over a finite field.

25.4.1 Isogeny Volcanoes

Let E be an ordinary elliptic curve over $\mathbb{F}_q$ and let $\#E(\mathbb{F}_q) = q + 1 - t$. Denote by K the number field $\mathbb{Q}(\sqrt{t^2 - 4q})$ and by $\mathcal{O}_K$ the ring of integers of K. We know that $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ is an order in $\mathcal{O}_K$ that contains the order $\mathbb{Z}[\pi_q] = \mathbb{Z}[(t+\sqrt{t^2-4q})/2]$ of discriminant $t^2 - 4q$. Let Δ_K be the discriminant of K, namely $\Delta_K = (t^2 - 4q)/c^2$ where c is the largest positive integer such that Δ_K is an integer congruent to 0 or 1 modulo 4. The integer c is the **conductor** of the order $\mathbb{Z}[\pi_q]$.

Suppose E_1 and E_2 are elliptic curves over $\mathbb{F}_q$ such that $\mathrm{End}(E_i) = \mathcal{O}_i$, for $i = 1, 2$, where $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders in K containing $\mathbb{Z}[\pi_q]$. We now present some results about the isogenies between such elliptic curves.

Lemma 25.4.1. *Let $\phi : E \to \widetilde{E}$ be an isogeny of elliptic curves over $\mathbb{F}_q$. If $[\mathrm{End}(E) : \mathrm{End}(\widetilde{E})] = \ell$ (or vice versa) then the degree of ϕ is divisible by ℓ.*

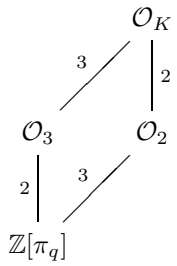
Proof: See Propositions 21 and 22 of Kohel [350]. □

Definition 25.4.2. Let ℓ be a prime and E an elliptic curve. Let $\mathrm{End}(E) = \mathcal{O}$. An ℓ-isogeny $\phi : E \to \widetilde{E}$ is called **horizontal** (respectively, **ascending**, **descending**) if $\mathrm{End}(\widetilde{E}) \cong \mathcal{O}$ (respectively, $[\mathrm{End}(\widetilde{E}) : \mathcal{O}] = \ell$, $[\mathcal{O} : \mathrm{End}(\widetilde{E})] = \ell$).

Exercise 25.4.3. Let $\phi : E \to \widetilde{E}$ be an ℓ-isogeny. Show that if ϕ is horizontal (resp., ascending, descending) then $\widehat{\phi}$ is horizontal (resp., descending, ascending).

Example 25.4.4. We now give a picture of how the orders relate to one another. Suppose the conductor of $\mathbb{Z}[\pi_q]$ is 6 (e.g., $q = 31$ and $t = \pm 4$), so that $[\mathcal{O}_K : \mathbb{Z}[\pi_q]] = 6$. Write $\mathcal{O}_K = \mathbb{Z}[\theta]$. Then the orders $\mathcal{O}_2 = \mathbb{Z}[2\theta]$ and $\mathcal{O}_3 = \mathbb{Z}[3\theta]$ are contained in $\mathcal{O}_K$ and are

such that $[\mathcal{O}_K : \mathcal{O}_i] = i$ for $i = 2, 3$.



Definition 25.4.5. Let the notation be as above. If $\mathrm{End}(E) = \mathcal{O}_K$ then E is said to be on the **surface** of the isogeny graph.[12] If $\mathrm{End}(E) = \mathbb{Z}[\pi_q]$ then E is said to be on the **floor** of the isogeny graph.

By the theory of complex multiplication, the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ on the surface is equal to the ideal class number of the ring $\mathcal{O}_K$.

Theorem 25.4.6. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ as above and let $\mathcal{O} = \mathrm{End}(E)$ be an order in $\mathcal{O}_K$ containing $\mathbb{Z}[\pi_q]$. Let $c = [\mathcal{O}_K : \mathcal{O}]$ and let ℓ be a prime. Every ℓ-isogeny $\phi : E \to \widetilde{E}$ arises from one of the following cases.*

- *If $\ell \nmid c$ then there are exactly $(1+(\frac{t^2-4q}{\ell}))$ equivalence classes of horizontal ℓ-isogenies over $\mathbb{F}_q$ from E to other elliptic curves.*[13]
- *If $\ell \mid c$ then there are no horizontal ℓ-isogenies starting at E.*
- *If $\ell \mid c$ there is exactly one ascending ℓ-isogeny starting at E.*
- *If $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi_q]]$ then the number of equivalence classes of ℓ-isogenies starting from E is $\ell + 1$, where the horizontal and ascending isogenies are as described and the remaining isogenies are descending.*
- *If $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi_q]]$ then there is no desending ℓ-isogeny.*

Proof: See Proposition 23 of Kohel [350]. A proof over $\mathbb{C}$ is also given in Appendix A.5 of [217]. □

Corollary 25.4.7. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$. Let c be the conductor of $\mathbb{Z}[\sqrt{t^2 - 4q}]$ and suppose $\ell \mid c$. Then $\ell \nmid [\mathrm{End}(E) : \mathbb{Z}[\pi_q]]$ if and only if there is a single ℓ-isogeny over $\mathbb{F}_q$ starting from E.*

Example 25.4.8. Let $q = 67$ and consider the elliptic curve $E : y^2 = x^3 + 11x + 21$ over $\mathbb{F}_q$. One has $\#E(\mathbb{F}_q) = 64 = q + 1 - t$ where $t = 4$ and $t^2 - 4q = 2^2 \cdot 3^2 \cdot (-7)$. Further, $j(E) = 42 \equiv -3375 \pmod{67}$, so E has complex multiplication by $(1 + \sqrt{-7})/2$. Since the ideal class number of $\mathbb{Q}(\sqrt{-7})$ is 1, it follows that E is the unique elliptic curve up to isomorphism on the surface of the isogeny graph.

Since 2 splits in $\mathbb{Z}[(1 + \sqrt{-7})/2]$ there are two 2-isogenies from E to elliptic curves on the surface (i.e., to E itself) and so there is only one 2-isogeny down from E. Using the modular polynomial we deduce that the 2-isogeny down maps to the isomorphism class

[12] Kohel's metaphor was intended to be aquatic: the floor represents the ocean floor and the surface represents the surface of the ocean.

[13] The symbol $(\frac{t^2-4q}{\ell})$ is the Kronecker symbol as in equation (25.4).

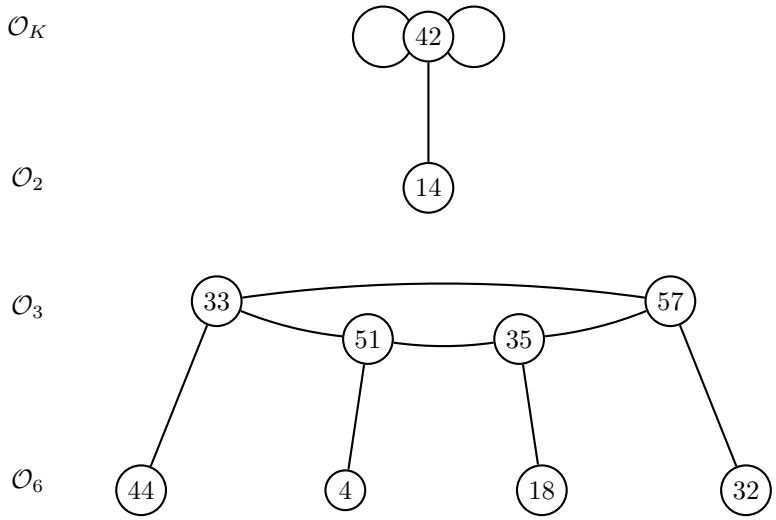


Figure 25.2: A 2-isogeny graph with two volcanoes. The symbols on the left hand side denote the endomorphism ring of curves on that level, using the same notation as Example 25.4.4.

of elliptic curves with j-invariant 14. One can verify that the only 2-isogeny over $\mathbb{F}_q$ from $j = 14$ is the ascending isogeny back to $j = 42$.

We have $(\frac{-7}{3}) = -1$ so there are no horizontal 3-isogenies from E. Hence, we expect four 3-isogenies down from E. Using the modular polynomial we compute the corresponding j-invariants to be $33, 35, 51$ and 57. One can now consider the 2-isogeny graphs containing these elliptic curves on their surfaces. It turns out that the graph is connected, and that there is a cycle of horizontal 2-isogenies from $j = 33$ to $j = 51$ to $j = 35$ to $j = 57$. For each vertex we therefore only expect one 2-isogeny down to the floor. The corresponding j-invariants are $44, 4, 18$ and 32 respectively. Figure 25.2 gives the 2-isogeny graph in this case.

Exercise 25.4.9. Draw the 3-isogeny graph for the elliptic curves in Example 25.4.8. Is $X_{E,\mathbb{F}_q,\{2,3\}}$ connected? If so, what is its diameter?

Fix a prime $\ell \mid c$ where c is the conductor of $\mathbb{Z}[\pi_q]$. Consider the sub-graph of the isogeny graph corresponding to isogenies whose degree is equal to ℓ. We call this the ℓ-isogeny graph. This graph is often not connected (for example, it is not connected when c is not a power of ℓ or when primes above ℓ do not generate $\mathrm{Cl}(\mathcal{O}_K)$). Even when ℓ splits and c is 1 or a power of ℓ, the graph is often not connected (the graph is connected only when the prime ideals above ℓ generate the ideal class group). Theorem 25.4.6 shows that each component of the ℓ-isogeny graph has a particular shape (that Fouquet and Morain [209] call a **volcano**).

We now give a precise definition for volcanoes. Let $\#E(\mathbb{F}_q) = q + 1 - t$ and let c be the conductor of $\mathbb{Z}[\pi_q]$ and suppose $\ell^m \| c$. Let $K = \mathbb{Q}(\sqrt{t^2 - 4q})$ and denote by $\mathcal{O}_K$ the maximal order in K. A **volcano** is a connected component of the graph $X_{E,\mathbb{F}_q,\{\ell\}}$. A volcano has $m + 1$ "levels" $V_0, \ldots, V_m$, being sub-graphs of the ℓ-isogeny graph; where vertices in V_i (i.e., on level i) correspond to isomorphism classes of elliptic curves $\widetilde{E}$ such that $\ell^i \| [\mathcal{O}_K : \mathrm{End}(\widetilde{E})]$. In other words, V_0 is on the surface of this component of the ℓ-isogeny graph (but not necessarily on the surface of the entire isogeny graph $X_{E,\mathbb{F}_q,S}$) and V_m is on the floor of this component of the ℓ-isogeny graph (though, again, not

necessarily on the floor of the whole isogeny graph). The surface of a volcano (i.e., V_0) is also called the **crater**. The graph V_0 is a connected regular graph with each vertex of degree at most 2. For all $0 < i \leq m$ and every vertex $v \in V_i$ there is a unique edge from v "up" to a vertex in V_{i-1}. For all $0 \leq i < m$ and every $v \in V_i$, the degree of v is $\ell + 1$. Every vertex in V_m has degree 1.

25.4.2 Kohel's Algorithm (Ordinary Case)

Kohel used the results of Section 25.4.1 to develop deterministic algorithms for computing $\mathrm{End}(E)$ (i.e., determining the level) for an elliptic curve E over $\mathbb{F}_q$. We sketch the algorithm for ordinary curves. Two facts are of crucial importance in Kohel's algorithm. The first (Corollary 25.4.7) is that one can recognise the floor when standing on it. The second fact is that if one starts a chain of ℓ-isogenies with a descending isogeny, and avoids backtracking, then all the isogenies in the chain are descending.

Before going any further, we discuss how to compute a non-backtracking chain of ℓ-isogenies. Given $j(E)$ one can compute the j-invariants of ℓ-isogenous curves over $\mathbb{F}_q$ by computing the roots of $F(y) = \Phi_\ell(j(E), y)$ in $\mathbb{F}_q$. Recall that one computes $\Phi_\ell(x, y)$ in $O(\ell^{3+\epsilon})$ bit operations and finds the roots of $F(y)$ in $\mathbb{F}_q$ in expected time bounded by $O(\ell^2 \log(\ell) \log(q))$ operations in $\mathbb{F}_q$. Let $j_0 = j(E)$ and let j_1 be one of the roots of of $F(y)$. We want to find, if possible, $j_2 \in \mathbb{F}_q$ such that there are ℓ-isogenies from E to E_1 (where $j(E_1) = j_1$) and from E_1 to E_2 (where $j(E_2) = j_2$) and such that $j_2 \neq j_0$ (so the second isogeny is not the dual of the first). The trick is to find roots of $\Phi_\ell(j_1, y)/(y - j_0)$. This process can be repeated to compute a chain $j_0, j_1, j_2, \ldots$ of j-invariants of ℓ-isogenous curves. As mentioned earlier, an alternative approach to walking in the isogeny graph is to find $\mathbb{F}_q$-rational factors of the ℓ-division polynomial and use Vélu's formulae; this is less efficient in general and the method to detect backtracking is to compute the image curve using Vélu's formulae and then compute its j-invariant.

The basic idea of Kohel's algorithm is, for each prime ℓ dividing[14] the conductor of $\mathbb{Z}[\pi_q]$, to find a chain of ℓ-isogenies from E to an elliptic curve on the floor. Suppose ℓ is a prime and $\ell^m \| c$. Kohel (on page 46 of [350]) suggests to take two non-backtracking chains of ℓ-isogenies of length at most m from E. If E is on the floor then this is immediately detected. If E is not on the surface then at least one of the initial ℓ-isogenies is descending, so in at most m steps one finds oneself on the floor. So if after m steps neither chain of isogenies has reached the floor then it follows that we must have started on the surface (and some or all of the ℓ-isogenies in the chain were along the surface). Note that, apart from the algorithm for computing roots of polynomials, the method is deterministic.

Exercise 25.4.10. Let $E : y^2 = x^3 + 3x + 6$ over $\mathbb{F}_{37}$ be an elliptic curve. Note that $\#E(\mathbb{F}_{37}) = 37 + 1 - 4$ and $4^2 - 4 \cdot 37 = -2^4 \cdot 7$. Hence the conductor is 4. We have $j(E) = 10$. Using the modular polynomial one finds the following j-invariants of elliptic curves 2-isogenous to E: $11, 29, 31$. Further, there is a single 2-isogeny from j-invariants $11, 31$ (in both cases, back to $j = 10$). But from 29 there is a 2-isogeny to $j = 10$ and two 2-isogenies to $j = 29$. What is $\mathrm{End}(E)$? Give j-invariants for a curve on the floor and a curve on the surface.

The worst case of Kohel's algorithm is when the conductor is divisible by one or more very large primes ℓ (since determining the j-invariant of an ℓ-isogenous curve is polynomial in ℓ and so exponential in the input size). Since c can be as big as $\sqrt{q}$ the above method (i.e., taking isogenies to the floor) would therefore have worst-case complexity of at least

[14] It is necessary to find the square factors of $t^2 - 4q$, which can be done in deterministic time $\tilde{O}(q^{1/6})$; see Exercise 12.5.1.

$q^{1/2}$ bit operations (indeed, it would be $O(q^{3/2+\epsilon})$ operations in $\mathbb{F}_q$ if one includes the cost of generating modular polynomials). Kohel (pages 53 to 57 of [350]) noted that when ℓ is very large one can more efficiently resolve the issue of whether or not ℓ divides the conductor by finding elements in the ideal class group that are trivial for the maximal order but non-trivial for an order whose conductor is divisible by ℓ; one can then "test" such a relation using isogenies. Using these ideas Kohel proves in Theorem 24 of [350] that, assuming a certain generalisation of the Riemann hypothesis, his algorithm requires $O(q^{1/3+\epsilon})$ bit operations. Kohel also considers the case of supersingular curves.

Bisson and Sutherland [58] consider a randomised version of Kohel's method using ideas from index calculus algorithms in ideal class groups. Their algorithm has heuristic subexponential expected complexity of $O(L_q(1/2, \sqrt{3}/2))$ bit operations. We do not present the details.

Remark 25.4.11. An important remark is that neither of the two efficient ways to generate elliptic curves over finite fields is likely to lead to elliptic curves E such that the conductor of $\mathrm{End}(E)$ is divisible by a large prime.

- When generating elliptic curves by choosing a random curve over a large prime field and counting points, then $t^2 - 4q$ behaves like a random integer and so is extremely unlikely to be divisible by the square of a very large prime
- When using the CM method then it is automatic that the curves have $q+1-t$ points where $t^2 - 4q$ has a very large square factor. It is easy to arrange that the square factor is divisible by a large prime. However, the elliptic curve itself output by the CM method has $\mathrm{End}(E)$ being the maximal order. To get $\mathrm{End}(E)$ to be a non-maximal order one can either use class polynomials corresponding to non-maximal orders or use descending isogenies. Either way, it is infeasible to compute a curve E such that a very large prime divides the conductor of $\mathrm{End}(E)$. Furthermore, Kohel's algorithm is not needed in this case, since by construction one already knows $\mathrm{End}(E)$.

Hence, in practice, the potential problems with large primes dividing the conductor of $\mathrm{End}(E)$ do not arise. It is therefore safe to assume that determining $\mathrm{End}(E)$ in practice is easy.

25.5 Constructing Isogenies Between Elliptic Curves

The **isogeny problem for elliptic curves** is: given two elliptic curves E and $\widetilde{E}$ over $\mathbb{F}_q$ with the same number of points, to compute an isogeny between them. Solving this problem is usually considered in two stages:

1. Performing a pre-computation, that computes a chain of prime-degree isogenies from E to $\widetilde{E}$. The chain is usually computed as a sequence of explicit isogenies, though one could store just the "Elkies information" for each isogeny in the chain.
2. Given a specific point $P \in E(\overline{\mathbb{F}}_q)$ to compute the image of P under the isogeny.

The precomputation is typically slow, while it is desirable that the computation of the isogeny be fast (since it might be performed for a large number of points).

An algorithm to solve the isogeny problem, requiring exponential time and space in terms of the input size, was given by Galbraith [217]. For the case of ordinary elliptic curves, an improved algorithm with low storage requirements was given by Galbraith, Hess and Smart [221]. We briefly sketch both algorithms in this section.

We now make some preliminary remarks in the ordinary case. Let c_1 be the conductor of $\mathrm{End}(E)$ and c_2 the conductor of $\mathrm{End}(\widetilde{E})$. If there is a large prime ℓ that divides c_1 but not c_2 (or vice versa), then any isogeny between E and $\widetilde{E}$ will have degree divisible by ℓ and hence the isogeny will be slow to compute. Since the conductor is a square factor of $t^2 - 4q$ it can be, in theory, as big as $q^{1/2}$. It follows that one does not expect an efficient algorithm for this problem in general. However, as mentioned in Remark 25.4.11, in practice one can ignore this bad case and assume the primes dividing the conductor are moderate.

For the rest of this section, in the ordinary case, we assume that $\mathrm{End}(E) = \mathrm{End}(\widetilde{E}) = \mathcal{O}$. (If this is not the case then take vertical isogenies from E to reduce to it.) Usually $\mathcal{O}$ is the maximal order. This is desirable, because the class number of the maximal order is typically smaller (and never larger) than the class number of the sub-orders, and so the algorithm to find the isogeny works more quickly in this case. However, for the sake of generality we do not insist that $\mathcal{O}$ is the maximal order. The general case could appear if there is a very large prime dividing the conductor of $\mathcal{O}$.

25.5.1 The Galbraith Algorithm

The algorithm of Galbraith [217] finds a path between two vertices in the isogeny graph $X_{E,\Bbbk,S}$ using a breadth-first search (see Section 22.2 of [146]). This algorithm can be used in both the ordinary and supersingular cases. More precisely, one starts with sets $X_0 = \{j(E)\}$ and $Y_0 = \{j(\widetilde{E})\}$ (we are assuming the vertices of the isogeny graph are labelled by j-invariants) and, at step i, computes $X_i = X_{i-1} \cup \delta_v(X_{i-1})$ and $Y_i = Y_{i-1} \cup \delta_v(Y_{i-1})$ where $\delta_v(X)$ is the set of vertices in the graph that are connected to a vertex in X by an edge. Computing $\delta_v(X)$ involves finding the roots in $\Bbbk$ of $\Phi_\ell(j, y)$ for every $j \in X$ and every $\ell \in S$. In the supersingular case the set S of possible isogeny degrees usually consists of a single prime ℓ. In the ordinary case S could have as many as $\log(q)$ elements, and one might not compute the whole of $\delta_v(X)$ but just the boundary in a subgraph corresponding to a (random) subset of S. In either case, the cost of computing $\delta_v(X)$ is clearly proportional to $\#X$.[15] The algorithm stops when $X_i \cap Y_i \neq \varnothing$, in which case it is easy to compute the isogeny from E to $\widetilde{E}$.

Exercise 25.5.1. Write pseudocode for the above algorithm.

Under the (probably unreasonable) assumption that new values in $\delta_v(X_i)$ behave like uniformly chosen elements in the isogeny graph, one expects from the birthday paradox that the two sets have non-empty intersection when $\#X_i + \#Y_i \geq \sqrt{\pi \#X_{E,\Bbbk,S}}$. Since the graph is an expander, we know that $\#X_i = \#X_{i-1} + \#\delta_v(X_{i-1}) \geq (1 + c)\#X_{i-1}$ when X_{i-1} is small, and so $\#X_i \geq (1 + c)^i$.

In the supersingular case we have $\#X_{E,\Bbbk,S} = O(q)$ and in the ordinary case we have $\#X_{E,\Bbbk,S} = h(\mathcal{O}) = O(q^{1/2} \log(q))$. In both cases, one expects the algorithm to terminate after $O(\log(q))$ steps. Step i involves, for every vertex $j \in X_i$ (or $j \in \delta_v(X_{i-1})$) and every $\ell \in S$, computing roots of $\Phi_\ell(j, y)$ in $\mathbb{F}_q$. One can check that if all ℓ are polynomially bounded in $\log(q)$ then the expected number of bit operations is bounded by $\sqrt{\#X_{E,\Bbbk,S}}$ times a polynomial in $\log(q)$.

In the supersingular case the algorithm performs an expected $\tilde{O}(q^{1/2})$ bit operations. In the ordinary case, by Bach's result (and therefore, assuming various generalisations of the Riemann hypothesis) we can restrict to isogenies of degree at most $6 \log(q)^2$ and so each step is polynomial-time (the dominant cost of each step is finding roots of the

[15] When all $\ell \in S$ are used at every step, to compute $\delta_v(X_i)$ it suffices to consider only vertices $j \in \delta_v(X_{i-1})$.

modular polynomial; see Exercise 25.2.2). The total complexity is therefore an expected $\tilde{O}(q^{1/4})$ bit operations. The storage required is expected to be $O(q^{1/4}\log(q)^2)$ bits.

Exercise 25.5.2. Let $m \in \mathbb{N}$. Suppose all $\ell \in S$ are such that $\ell = O(\log(q)^m)$. Let $\phi : E \to \widetilde{E}$ be the isogeny output by the Galbraith algorithm. Show, under the same heuristic assumptions as above, that one can evaluate $\phi(P)$ for $P \in E(\mathbb{F}_q)$ polynomial-time.

Exercise 25.5.3. Isogenies of small degree are faster to compute than isogenies of large degree. Hence, the average cost to compute an ℓ-isogeny can be used as a weight for the edges in the isogeny graph corresponding to ℓ-isogenies. It follows that there is a well-defined notion of shortest path in the isogeny graph between two vertices. Show how Dijkstra's algorithm (see Section 24.3 of [146]) can be used to find a chain of isogenies between two elliptic curves that can be computed in minimal time. What is the complexity of this algorithm?

25.5.2 The Galbraith-Hess-Smart Algorithm

We now restrict to the ordinary isogeny graph and sketch the algorithm of Galbraith, Hess and Smart [221]. The basic idea is to replace the breadth-first search by a random walk, similar to that used in the kangaroo algorithm.

Let H be a hash function from $\mathbb{F}_q$ to a set S of prime ideals of small norm. One starts random walks at $x_0 = j(E)$ and $y_0 = j(\widetilde{E})$ and stores ideals $\mathfrak{a}_0 = (1)$, $\mathfrak{b}_0 = (1)$. One can think of $(x_0, \mathfrak{a}_0)$ as a "tame walk" and $(y_0, \mathfrak{b}_0)$ as a "wild walk". Each step of the algorithm computes new values x_i and y_i from x_{i-1} and y_{i-1}: To compute x_i set $\mathfrak{l} = H(x_{i-1})$ and $\ell = N(\mathfrak{l})$; find the roots of $\Phi_\ell(x_{i-1}, z)$; choose the root corresponding to the ideal $\mathfrak{l}$ (using the trick mentioned in Remark 25.3.9) and call it x_i. The same process is used (with the same function H) for the sequence y_i. The ideals are also updated as $\mathfrak{a}_i = \mathfrak{a}_{i-1}\mathfrak{l}$ (reduced in the ideal class group to some short canonical representation of ideals). If $x_i = y_j$ then the walks follow the same path. We designate certain elements of $\mathbb{F}_q$ as being distinguished points, and if x_i or y_i is distinguished then it is stored together with the corresponding ideal $\mathfrak{a}$ or $\mathfrak{b}$. After a walk hits a distinguished point there are two choices: it could be allowed to continue or it could be restarted at a j-invariant obtained by taking a short random isogeny chain (perhaps corresponding to primes not in S) from E or $\widetilde{E}$.

Once a collision is detected one has an isogeny corresponding to ideal $\mathfrak{a}$ from $j(E)$ to some j, and an isogeny corresponding to ideal $\mathfrak{b}$ from $j(\widetilde{E})$ to j. Hence, the ideal $\mathfrak{a}\mathfrak{b}^{-1}$ gives the isogeny from $j(E)$ to $j(\widetilde{E})$.

Stolbunov has noted that, since the ideal class group is Abelian, it is not advisable to choose S such that $\mathfrak{l}, \mathfrak{l}^{-1} \in S$ (since such a choice means that walks remain "close" to the original j-invariant, and cycles in the random walk might arise). It is also faster to use isogenies of small degree more often than those with large degree. We refer to Galbraith and Stolbunov [230] for further details.

The remaining problem is that the ideal $\mathfrak{a}\mathfrak{b}^{-1}$ is typically of large norm. By construction, it is a product of exponentially many small primes. Since the ideal class group is commutative, such a product has a short representation (storing the exponents for each prime), but this leads to an isogeny that requires exponential computation. The proposal from [221] is to represent ideals using the standard representation for ideals in quadratic fields, and to "smooth" the ideal using standard techniques from index calculus algorithms in ideal class groups. It is beyond the scope of this book to discuss these ideas in detail. However, we note that the isogeny then has subexponential length and uses

primes ℓ of subexponential degree. Hence, the second stage of the isogeny computation is subexponential-time; this is not as fast as it would be with the basic Galbraith algorithm. The idea of smoothing an isogeny has also been used by Bröker, Charles and Lauter [108] and Jao and Soukharev [312].

Since the ordinary isogeny graph is conjecturally an expander graph, we know that a random walk on it behaves close to the uniform distribution after sufficiently many steps. We make the heuristic assumption that the pseudorandom walk proposed above has this property when the number of different primes used is sufficiently large and the hash function H is good. Then, by the birthday paradox, one expects a collision after $\sqrt{\pi h(\mathcal{O})}$ vertices have been visited. As a result, the heuristic expected running time of the algorithm is $O(q^{1/4})$ isogeny chain steps, and the storage can be made low by making distinguished elements rare. The algorithm can be distributed: using L processors of equal power one solves the isogeny problem in $\tilde{O}(q^{1/4}/L)$ bit operations.

25.6 Relating the Discrete Logarithm Problem on Isogenous Curves

The main application of the algorithms in Section 25.5 is to relate the discrete logarithm problem on curves with the same number of points. More precisely, let E and $\widetilde{E}$ be elliptic curves over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = \#\widetilde{E}(\mathbb{F}_q)$. Let r be a large prime dividing $\#E(\mathbb{F}_q)$. A natural question is whether the discrete logarithm problem (in the subgroup of order r) has the same difficulty in both groups $E(\mathbb{F}_q)$ and $\widetilde{E}(\mathbb{F}_q)$. To study this question one wants to reduce the discrete logarithm problem from $E(\mathbb{F}_q)$ to $\widetilde{E}(\mathbb{F}_q)$. If we have an isogeny $\phi : E \to \widetilde{E}$ of degree not divisible by r, and if ϕ can be efficiently computed, then we have such a reduction.

As we have seen, if there is a very large prime dividing the conductor of $\mathrm{End}(E)$ but not the conductor of $\mathrm{End}(\widetilde{E})$ (or vice versa) then it is not efficient to compute an isogeny from E to $\widetilde{E}$. In this case one cannot make any inference about the relative difficulty of the DLP in the two groups. No example is known of elliptic curves E and $\widetilde{E}$ of this form (i.e., with a large conductor gap) but for which the DLP on one is known to be significantly easier than the DLP on another. The nearest we have to an example of this phenomenon is with elliptic curves E with $\#\mathrm{Aut}(E) > 2$ (and so one can accelerate the Pollard rho method using equivalence classes as in Section 14.4) but with an isogeny from E to $\widetilde{E}$ with $\#\mathrm{Aut}(\widetilde{E}) = 2$.

On the other hand, if the conductors of $\mathrm{End}(E)$ and $\mathrm{End}(\widetilde{E})$ have the same very large prime factors (or no large prime factors) then we can (conditional on a generalised Riemann hypothesis) compute an isogeny between them in $\tilde{O}(q^{1/4})$ bit operations. This is not a polynomial-time reduction. But, since the current best algorithms for the DLP on elliptic curves run in $\tilde{O}(q^{1/2})$ bit operations, it shows that from a practical point of view the two DLPs are equivalent.

Jao, Miller and Venkatesan [310] have a different, and perhaps more useful, interpretation of the isogeny algorithms in terms of random self-reducibility of the DLP in an isogeny class of elliptic curves. The idea is that if E is an elliptic curve over $\mathbb{F}_q$ then by taking a relatively short random walk in the isogeny graph one arrives at a "random" (again ignoring the issue of large primes dividing the conductor) elliptic curve $\widetilde{E}$ over $\mathbb{F}_q$ such that $\#\widetilde{E}(\mathbb{F}_q) = \#E(\mathbb{F}_q)$. Hence, one easily turns a specific instance of the DLP (i.e., for a specific elliptic curve) into a random instance. It follows that if there were a "large" set of "weak" instances of the DLP in the isogeny class of E then, after enough trials,

one should be able to reduce the DLP from E to one of the elliptic curves in the weak class. One concludes that either the DLP is easy for "most" curves in an isogeny class, or is hard for "most" curves in an isogeny class.

Chapter 26

Pairings on Elliptic Curves

This chapter is a very brief summary of the mathematics behind pairings on elliptic curves. Pairing-based cryptography was created by Sakai, Ohgishi and Kasahara [509] and Joux [316]. Some applications of pairings in elliptic curve cryptography have already been presented in the book (for example, the identity-based encryption scheme of Boneh and Franklin in Section 23.3.2 and the Boneh-Boyen signature scheme in Section 22.2.3). We present several other important applications of pairings, such as the Menezes-Okamoto-Vanstone/Frey-Rück reduction of the discrete logarithm problem from elliptic curves to finite fields.

Due to lack of space we do not give full details of the subject. Good general references for pairings and pairing-based cryptography are Chapters IX and X of [65], Chapters 6, 16 and 24 of [16] and [320].

26.1 Weil Reciprocity

The following theorem is an important tool for studying pairings. Recall that a divisor on a curve C over a field $\Bbbk$ is a finite sum $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ (i.e., $n_P = 0$ for all but finitely many $P \in C(\overline{\Bbbk})$). The support of a divisor D is the set of points $\mathrm{Supp}(D) = \{P \in C(\overline{\Bbbk}) : n_P \neq 0\}$. To a function f on a curve one associates the divisor $\mathrm{div}(f)$ as in Definition 7.7.2. If f is a function on a curve and D is a divisor such that the support of D is distinct from the support of $\mathrm{div}(f)$ then $f(D)$ is defined to be $\prod_{P \in C(\overline{\Bbbk}), n_P \neq 0} f(P)^{n_P}$.

Exercise 26.1.1. Let D_1 and D_2 be divisors with disjoint support on a curve C. Suppose D_1 is principal. Show that $f(D_2)$ is well-defined, subject to $\mathrm{div}(f) = D_1$, if and only if D_2 has degree zero.

Theorem 26.1.2. *(**Weil reciprocity**) Let C be a curve over a field $\Bbbk$. Let $f, g \in \Bbbk(C)$*

be functions such that $\mathrm{Supp}(\mathrm{div}(f)) \cap \mathrm{Supp}(\mathrm{div}(g)) = \varnothing$. *Then*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

Proof: (Sketch) One first shows that the result holds for functions on $C = \mathbb{P}^1$. Then take any covering $\phi : C \to \mathbb{P}^1$ and apply the pullback. We refer to the appendix of Chapter IX of [65] for details. A proof over $\mathbb{C}$ is given in the appendix to Section 18.1 of Lang [366]. □

Pages 24-26 of Charlap and Coley [126] present a generalised Weil reciprocity that does not require the divisors to have disjoint support.

26.2 The Weil Pairing

The Weil pairing plays an important role in the study of elliptic curves over number fields, but tends to be less important in cryptography. For completeness, we briefly sketch its definition.

Let E be an elliptic curve over $\Bbbk$ and let $n \in \mathbb{N}$ be coprime to $\mathrm{char}(\Bbbk)$. Let $P, Q \in E[n]$. Then there is a function $f \in \overline{\Bbbk}(E)$ such that $\mathrm{div}(f) = n(Q) - n(\mathcal{O}_E)$. Let $Q' \in E(\overline{\Bbbk})$ be any point such that $[n]Q' = Q$, and so $[n^2]Q' = \mathcal{O}_E$. Note that $[n]$ is unramified and the divisor $D = [n]^*((Q) - (\mathcal{O}_E))$ is equal to

$$\sum_{R \in E[n]} (Q' + R) - (R).$$

Since $\sum_{R \in E[n]} R = \mathcal{O}_E$ and $[n^2]Q' = \mathcal{O}_E$ it follows from Theorem 7.9.9 that D is a principal divisor. So there is a function $g \in \overline{\Bbbk}(E)$ such that $\mathrm{div}(g) = D = [n]^*((Q) - (\mathcal{O}_E))$. Now, consider the function $[n]^*f = f \circ [n]$. One has $\mathrm{div}([n]^*f) = [n]^*(\mathrm{div}(f)) = [n]^*(n(Q) - n(\mathcal{O}_E)) = nD$. Hence the functions $f \circ [n]$ and g^n have the same divisor. Multiplying f by a suitable constant gives $f \circ [n] = g^n$. Now, for any point $U \in E(\overline{\Bbbk})$ such that $[n]U \notin E[n^2]$ we have

$$g(U + P)^n = f([n]U + [n]P) = f([n]U) = g(U)^n.$$

In other words, $g(U + P)/g(U)$ is an n-th root of unity in $\overline{\Bbbk}$.

Lemma 26.2.1. *Let the notation be as above. Then* $g(U + P)/g(U)$ *is independent of the choice of the point* $U \in E(\overline{\Bbbk})$.

Proof: See Section 11.2 of Washington [626]. The proof is described as "slightly technical" and uses the Zariski topology. □

Definition 26.2.2. Let E be an elliptic curve over a field $\Bbbk$ and let $n \in \mathbb{N}$ be such that $\gcd(n, \mathrm{char}(\Bbbk)) = 1$. Define

$$\mu_n = \{z \in \overline{\Bbbk}^* : z^n = 1\}.$$

The **Weil pairing** is the function

$$e_n : E[n] \times E[n] \to \mu_n$$

defined (using the notation above) as $e_n(P, Q) = g(U + P)/g(U)$ for any point $U \in E(\overline{\Bbbk})$, $U \notin E[n^2]$ and where $\mathrm{div}(g) = [n]^*((Q) - (\mathcal{O}_E))$.

Theorem 26.2.3. *The Weil pairing satisfies the following properties.*

1. *(Bilinear) For* $P_1, P_2, Q \in E[n]$, $e_n(P_1+P_2, Q) = e_n(P_1, Q)e_n(P_2, Q)$ *and* $e_n(Q, P_1+P_2) = e_n(Q, P_1)e_n(Q, P_2)$.
2. *(Alternating) For* $P \in E[n]$, $e_n(P, P) = 1$.
3. *(Non-degenerate) If* $e_n(P, Q) = 1$ *for all* $Q \in E[n]$ *then* $P = \mathcal{O}_E$.
4. *(Galois invariant) If* E *is defined over* $\Bbbk$ *and* $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ *then* $e_n(\sigma(P), \sigma(Q)) = \sigma(e_n(P, Q))$.
5. *(Compatible) If* $P \in E[nm]$ *and* $Q \in E[n]$ *then*

$$e_{nm}(P, Q) = e_n([m]P, Q).$$

Proof: See Theorem III.8.1 of Silverman [564] or Theorem 11.7 of Washington [626]. The non-degeneracy proof in [564] is very sketchy, but the treatment in [626] fills in the missing details. The non-degeneracy also needs the fact that the genus of E is not zero, so there is no function with divisor $(P) - (\mathcal{O}_E)$ (see Corollary 8.6.5). □

Exercise 26.2.4. Show that any function $e : E[n] \times E[n] \to \mu_n$ that has the properties of the Weil pairing as in Theorem 26.2.3 also has the following properties.

1. $e(\mathcal{O}_E, P) = e(P, \mathcal{O}_E) = 1$ for all $P \in E[n]$.
2. $e(-P, Q) = e(P, Q)^{-1}$ for all $P, Q \in E[n]$.
3. $e(P, Q) = e(Q, P)^{-1}$ for all $P, Q \in E[n]$.
4. If $\{P, Q\}$ generate $E[n]$ then the values of e on $E[n] \times E[n]$ are uniquely determined by the single value $e(P, Q)$.

Exercise 26.2.5. Let E be an elliptic curve over $\mathbb{F}_q$ and let $n \in \mathbb{N}$. Prove that $E[n] \subseteq E(\mathbb{F}_q)$ implies $n \mid (q-1)$.

For elliptic curves over $\mathbb{C}$ the Weil pairing has a very simple interpretation. Recall that an elliptic curve over $\mathbb{C}$ is isomorphic (as a manifold) to $\mathbb{C}/L$, where L is a lattice of rank 2, and that this isomorphism also preserves the group structure. Fix a pair $\{z_1, z_2\}$ of generators for L as a $\mathbb{Z}$-module. The points of order n are $\frac{1}{n}L/L$, so are identified with $\{(az_1 + bz_2)/n : 0 \leq a, b < n\}$. The function

$$e_n((az_1 + bz_2)/n, (cz_1 + dz_2)/n) = \exp(2\pi i(ad - bc)/n)$$

is easily checked to be bilinear, non-degenerate and alternating. Hence, it is (a power of) the Weil pairing. We refer to the appendix of Section 18.1 of Lang [366] for further details. Connections with the intersection pairing are discussed in Section 12.2 of Husemoller [302] and Edixhoven [189].

There is an alternative definition[1] of the Weil pairing that is more useful for implementation, but for which it is harder to prove non-degeneracy. For $P, Q \in E[n]$ let D_P and D_Q be degree zero divisors such that $D_P \equiv (P) - (\mathcal{O}_E)$, $D_Q \equiv (Q) - (\mathcal{O}_E)$ and $\mathrm{Supp}(D_P) \cap \mathrm{Supp}(D_Q) = \varnothing$. Let $f_P, f_Q \in \overline{\Bbbk}(E)$ be functions such that $\mathrm{div}(f_P) = nD_P$ and $\mathrm{div}(f_Q) = nD_Q$. Then

$$e_n(P, Q) = f_Q(D_P)/f_P(D_Q). \tag{26.1}$$

[1]The literature is inconsistent and some of the definitions (for example, Section 18.1 of Lang [366], Exercise 3.16 of Silverman [564] and Section 3 of Miller [427]) are actually for $e_n(Q, P) = e_n(P, Q)^{-1}$. For further discussion of this issue see Remark 11.3 and Section 11.6 of Washington [626]. Also see the "Warning" at the end of Section 4 of Miller [429].

The equivalence is shown in Theorem 4 of the extended and unpublished version of Hess [282], and in Section 11.6.1 of Washington [626].

The Weil pairing can be generalised from $E[n] \times E[n]$ to $\ker(\phi) \times \ker(\hat{\phi}) \subseteq E[n] \times \widetilde{E}[n]$ where $\phi : E \to \widetilde{E}$ is an isogeny. For details see Exercise 3.15 of Silverman [564] or Garefalakis [237]. For the Weil pairing on Jacobian varieties of curves of genus $g > 1$ we refer to Section 20 of Mumford [444].

26.3 The Tate-Lichtenbaum Pairing

Tate defined a pairing for Abelian varieties over local fields and Lichtenbaum showed how to compute it efficiently in the case of Jacobian varieties of curves. Frey and Rück [213] showed how to compute it for elliptic curves over finite fields, and emphasised its cryptographic relevance. This pairing is the basic building block of most pairing-based cryptography.

Exercise 26.3.1. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let $n \in \mathbb{N}$ be such that $\gcd(n, q) = 1$ and $n \mid \#E(\mathbb{F}_q)$. Define

$$nE(\mathbb{F}_q) = \{[n]Q : Q \in E(\mathbb{F}_q)\}.$$

Show that $nE(\mathbb{F}_q)$ is a group. Show that $E(\mathbb{F}_q)[n] = \{P \in E(\mathbb{F}_q) : [n]P = \mathcal{O}_E\}$, $E(\mathbb{F}_q)/nE(\mathbb{F}_q) = \{P + nE(\mathbb{F}_q) : P \in E(\mathbb{F}_q)\}$ and $\mathbb{F}_q^*/(\mathbb{F}_q^*)^n$ are finite groups of exponent n.

Let notation be as in Exercise 26.3.1. Let $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$. Then $n(P) - n(\mathcal{O}_E)$ is principal, so there is a function $f \in \mathbb{F}_q(E)$ such that $\mathrm{div}(f) = n(P) - n(\mathcal{O}_E)$. Let D be a divisor on E with support disjoint from $\mathrm{Supp}(\mathrm{div}(f)) = \{\mathcal{O}_E, P\}$ but such that D is equivalent to $(Q) - (\mathcal{O}_E)$ (for example, $D = (Q + R) - (R)$ for some point[2] $R \in E(\overline{\mathbb{F}}_q)$, $R \notin \{\mathcal{O}_E, P, -Q, P - Q\}$). We define the **Tate-Lichtenbaum pairing** to be

$$t_n(P, Q) = f(D). \tag{26.2}$$

We will explain below that

$$t_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^n.$$

First we show that the pairing is well-defined. We sketch the proof, as it is a nice and simple application of Weil reciprocity.

Lemma 26.3.2. *Let the notation be as above. Let $P \in E(\mathbb{F}_q)[n]$ and let $f \in \mathbb{F}_q(E)$ be such that $\mathrm{div}(f) = n(P) - n(\mathcal{O}_E)$. Let D_1, D_2 be divisors on E defined over $\mathbb{F}_q$ with support disjoint from $\{\mathcal{O}_E, P\}$.*

1. *Suppose $D_1 \equiv D_2 \equiv (Q) - (\mathcal{O}_E)$ for some point $Q \in E(\mathbb{F}_q)$. Then $f(D_1)/f(D_2) \in (\mathbb{F}_q^*)^n$.*
2. *Suppose $D_1 \equiv (Q_1) - (\mathcal{O}_E)$ and $D_2 \equiv (Q_2) - (\mathcal{O}_E)$ where $Q_1, Q_2 \in E(\mathbb{F}_q)$ are such that $Q_1 \neq Q_2$ and and $Q_1 - Q_2 \in nE(\mathbb{F}_q)$. Then $f(D_1)/f(D_2) \in (\mathbb{F}_q^*)^n$.*

[2] One can usually take $R \in E(\mathbb{F}_q)$, but see page 187 of [65] for an example that shows that this is not always possible.

Proof: The first statement is a special case of the second, but it is a convenient stepping-stone for the proof. For the first statement, write $D_2 = D_1 + \mathrm{div}(h)$ where h is a function on E defined over $\mathbb{F}_q$. Note that $\mathrm{Supp}(\mathrm{div}(h)) \cap \{\mathcal{O}_E, P\} = \varnothing$. We have

$$f(D_2) = f(D_1 + \mathrm{div}(h)) = f(D_1)f(\mathrm{div}(h)).$$

Now, applying Weil reciprocity gives $f(\mathrm{div}(h)) = h(\mathrm{div}(f)) = h(n(P) - n(\mathcal{O}_E)) = (h(P)/h(\mathcal{O}_E))^n \in (\mathbb{F}_q^*)^n$.

For the second statement write $Q_1 - Q_2 = [n]R$ for some $R \in E(\mathbb{F}_q)$. We may assume that $R \neq \mathcal{O}_E$, since the first statement has already been proved. Then $(Q_1) - (Q_2) = n((R+S) - (S)) + \mathrm{div}(h_0)$ for some $h_0 \in \mathbb{F}_q(E)$ and some $S \in E(\mathbb{F}_q)$ with $S \notin \{\mathcal{O}_E, -R, P, P-R\}$.[3] We also have $D_1 = (Q_1) - (\mathcal{O}_E) + \mathrm{div}(h_1)$ and $D_2 = (Q_2) - (\mathcal{O}_E) + \mathrm{div}(h_2)$ for some $h_1, h_2 \in \mathbb{F}_q(E)$. Putting everything together

$$\begin{aligned} f(D_2) &= f(D_1 - n((R+S) - (S)) + \mathrm{div}(h_2) - \mathrm{div}(h_1) - \mathrm{div}(h_0)) \\ &= f(D_1)f((R+S) - (S))^n f(\mathrm{div}(h_2/(h_0h_1))). \end{aligned}$$

Since $\mathrm{Supp}(\mathrm{div}(h_2/(h_0h_1))) \subseteq \mathrm{Supp}(D_1) \cup \mathrm{Supp}(D_2) \cup \{R+S, S\}$ is disjoint from $\{\mathcal{O}_E, P\} = \varnothing$ the result follows from Weil reciprocity. □

Theorem 26.3.3. *The Tate-Lichtenbaum pairing satisfies the following properties.*

1. *(Bilinear) For $P_1, P_2 \in E(\mathbb{F}_q)[n]$, and $Q \in E(\mathbb{F}_q)$, $t_n(P_1+P_2, Q) = t_n(P_1, Q)t_n(P_2, Q)$. For $Q \in E(\mathbb{F}_q)[n]$ and $P_1, P_2 \in E(\mathbb{F}_q)$, $t_n(Q, P_1 + P_2) = t_n(Q, P_1)t_n(Q, P_2)$.*
2. *(Non-degenerate) Assume $\mathbb{F}_q^*$ contains a non-trivial n-th root of unity. Let $P \in E(\mathbb{F}_q)[n]$. If $t_n(P, Q) = 1$ for all $Q \in E(\mathbb{F}_q)$ then $P = \mathcal{O}_E$. Let $Q \in E(\mathbb{F}_q)$. If $t_n(P, Q) = 1$ for all $P \in E(\mathbb{F}_q)[n]$ then $Q \in nE(\mathbb{F}_q)$.*
3. *(Galois invariant) If E is defined over $\mathbb{F}_q$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ then $t_n(\sigma(P), \sigma(Q)) = \sigma(t_n(P, Q))$.*

Proof: Bilinearity can be proved using ideas similar to those used to prove Lemma 26.3.2 (for all the details see Theorem IX.7 of [65]). Non-degeneracy in the case of finite fields was shown by Frey and Rück [213], but simpler proofs can be found in Hess [282] and Section 11.7 of Washington [626]. Galois invariance is straightforward (see Theorem IX.7 of [65]). □

26.3.1 Miller's Algorithm

We now briefly explain how to compute the Tate-Lichtenbaum pairing (and hence the Weil pairing via equation (26.1)). The algorithm first appears in Miller [427].

Definition 26.3.4. Let $P \in E(\Bbbk)$ and $i \in \mathbb{N}$. A **Miller function** $f_{i,P} \in \Bbbk(E)$ is a function on E such that $\mathrm{div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O}_E)$. Furthermore, we assume that Miller functions are "normalised at infinity" in the sense that the power series expansion at infinity with respect to the canonical uniformizer $t_\infty = x/y$ is 1.

Exercise 26.3.5. Show that $f_{1,P} = 1$. Show that if $f_{i,P}$ and $f_{j,P}$ are Miller functions then one can take

$$f_{i+j,P} = f_{i,P}f_{j,P}l(x,y)/v(x,y)$$

where $l(x,y)$ and $v(x,y)$ are the lines arising in the elliptic curve addition of $[i]P$ to $[j]P$ (and so $\mathrm{div}(l(x,y)) = ([i]P) + ([j]P) + (-[i+j]P) - 3(\mathcal{O}_E)$ and $\mathrm{div}(v(x,y)) = ([i+j]P) + (-[i+j]P) - 2(\mathcal{O}_E)$).

[3] Some tedious calculations are required to show that one can choose $S \in E(\mathbb{F}_q)$ rather than $E(\overline{\mathbb{F}}_q)$ in all cases, but the claim is easy when n is large.

We can now give Miller's algorithm to compute $f_{n,P}(D)$ for any divisor D (see Algorithm 29). The basic idea is to compute the Miller function out of smaller Miller functions using a "square-and-multiply" strategy. As usual, we write an integer n in binary as $(1n_{m-1}\dots n_1n_0)_2$ where $m = \lfloor \log_2(n) \rfloor$. Note that the lines l and v in lines 6 and/or 10 may be simplified if the operation is $[2]T = \mathcal{O}_E$ or $T + P = \mathcal{O}_E$.

Algorithm 29 Miller's Algorithm

INPUT: $n = (1n_{m-1}\dots n_1n_0)_2 \in \mathbb{N}$, $P \in E(\Bbbk)$, such that $[n]P = \mathcal{O}_E$, $D \in \mathrm{Div}_{\overline{\Bbbk}}(E)$
OUTPUT: $f_{n,P}(D)$
1: $f = 1$
2: $T = P$
3: $i = m - 1 = \lfloor \log_2(n) \rfloor - 1$
4: **while** $i \geq 0$ **do**
5: Calculate lines l and v for doubling T
6: $f = f^2 \cdot l(D)/v(D)$
7: $T = [2]T$
8: **if** $n_i = 1$ **then**
9: Calculate lines l and v for addition of T and P
10: $f = f \cdot l(D)/v(D)$
11: $T = T + P$
12: **end if**
13: $i = i - 1$
14: **end while**
15: **return** f

The main observation is that Miller's algorithm takes $O(\log_2(n))$ iterations, each of which comprises field operations in $\Bbbk$ if P and all points in the support of D lie in $E(\Bbbk)$. There are a number of important techniques to speed up Miller's algorithm in practice; we mention some of them in the following sections and refer to Chapter IX of [65], Chapter XII of [320] or Section 16.4 of [16] for further details.

Exercise 26.3.6. Give simplified versions of lines 6 and 10 of Algorithm 29 that apply when $[2]T = \mathcal{O}_E$ or $T + P = \mathcal{O}_E$.

26.3.2 The Reduced Tate-Lichtenbaum Pairing

Definition 26.3.7. Let $n, q \in \mathbb{N}$ be such that $\gcd(n, q) = 1$. Define the **embedding degree** $k(q, n) \in \mathbb{N}$ to be the smallest positive (non-zero) integer such that $n \mid (q^{k(q,n)} - 1)$.

Let E be an elliptic curve over $\mathbb{F}_q$ and suppose $n \mid \#E(\mathbb{F}_q)$ is such that $\gcd(n, q) = 1$. Let $k = k(q, n)$ be the embedding degree. Then $\mu_n \subseteq \mathbb{F}_{q^k}^*$ (in some cases μ_n can lie in a proper subfield of $\mathbb{F}_{q^k}$) and so the Tate-Lichtenbaum pairing maps into $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$. In practice it is inconvenient to have a pairing taking values in this quotient group, as cryptographic protocols require well-defined values. To have a canonical representative for each coset in $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$ it would be much more convenient to use μ_n. This is easily achieved using the facts that if $z \in \mathbb{F}_{q^k}^*$ then $z^{(q^k-1)/n} \in \mu_n$, and that the cosets $z_1(\mathbb{F}_{q^k}^*)^n$ and $z_2(\mathbb{F}_{q^k}^*)^n$ are equal if and only if $z_1^{(q^k-1)/n} = z_2^{(q^k-1)/n}$. Also, exponentiation is a group homomorphism from $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$ to μ_n.

For this reason, one usually considers the **reduced Tate-Lichtenbaum pairing**

$$\hat{t}_n(P, Q) = t_n(P, Q)^{(q^k-1)/n},$$

which maps $E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ to μ_n. The exponentiation to the power $(q^k-1)/n$ is called the **final exponentiation**.

Exercise 26.3.8. Let $n \mid N \mid (q^k-1)$. Show that

$$t_n(P,Q)^{(q^k-1)/n} = t_N(P,Q)^{(q^k-1)/N}.$$

Exercise 26.3.9. Explain why working in a group whose order has low Hamming weight leads to relatively fast pairings. Suppose $n = E(\mathbb{F}_q)$ has low Hamming weight but $r \mid n$ does not. Explain how to compute the reduced Tate-Lichtenbaum pairing $\hat{t}_r(P,Q)$ efficiently if n/r is small.

In the applications one usually chooses the elliptic curve E to satisfy the mild conditions in Exercise 26.3.10. In these cases it follows from the Exercise that we can identify $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ with $E(\mathbb{F}_{q^k})[r]$. Hence, if the conditions hold, we may interpret the reduced Tate-Lichtenbaum pairing as a map

$$\hat{t}_r : E[r] \times E[r] \to \mu_r,$$

just as the Weil pairing is.

Exercise 26.3.10. Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a prime such that $r \| \#E(\mathbb{F}_q)$, $\gcd(r,q) = 1$, $E[r] \subseteq E(\mathbb{F}_{q^k})$ and $r^2 \| \#E(\mathbb{F}_{q^k})$, where $k = k(q,r)$ is the embedding degree. Show that $E[r]$ is set of representatives for $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$.

In most cryptographic situations one restricts to the case of points of prime order r. Further, one can often insist that $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. An important observation is that if $k > 1$ and $z \in \mathbb{F}_q^*$ then $z^{(q^k-1)/r} = 1$. This allows us to omit some computations in Miller's algorithm. A further trick, due[4] to Barreto, Kim, Lynn and Scott [29], is given in Lemma 26.3.11 (a similar fact for the Weil pairing is given in Proposition 8 of Miller [429]).

Lemma 26.3.11. *Let E be an elliptic curve over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ a point of prime order r (where $r > 4$ and $\gcd(q,r) = 1$), and $Q \in E(\mathbb{F}_{q^k}) - E(\mathbb{F}_q)$ where $k > 1$ is the embedding degree. Then*

$$\hat{t}_r(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}.$$

Proof: A proof for general curves (and without any restriction on r) is given in Lemma 1 of Granger, Hess, Oyono, Thériault and Vercauteren [265]. We give a similar argument.

We have $\hat{t}_r(P,Q) = f_{r,P}((Q+R)-(R))^{(q^k-1)/r}$ for any point $R \in E(\mathbb{F}_{q^k}) - \{\mathcal{O}_E, P, -Q, P-Q\}$. Choose $R \in E(\mathbb{F}_q) - \{\mathcal{O}_E, P\}$. Since $f_{r,P}(R) \in \mathbb{F}_q^*$ and $k > 1$ it follows that

$$\hat{t}_r(P,Q) = f_{r,P}(Q+R)^{(q^k-1)/r}.$$

Now, it is not possible to take $R = \mathcal{O}_E$ in the above argument. Instead we need to prove that $f_{r,P}(Q+R)^{(q^k-1)/r} = f_{r,P}(Q)^{(q^k-1)/r}$ directly. It suffices to prove that

$$f_{r,P}((Q+R)-(Q))^{(q^k-1)/r} = 1.$$

To do this, note that $(Q+R)-(Q) \equiv (R)-(\mathcal{O}_E) \equiv ([2]R)-(R)$. Set, for example, $R = [2]P$ so that $([2]R)-(R)$ has support disjoint from $\{\mathcal{O}_E, P\}$ (this is where the

[4]Though be warned that the "proof" in [29] is not rigorous.

condition $r > 4$ is used). Then there is a function $h \in \mathbb{F}_{q^k}(E)$ such that $(Q+R)-(Q) = ([2]R)-(R)+\mathrm{div}(h)$. We have

$$f_{r,P}((Q+R)-(Q)) = f_{r,p}(([2]R)-(R)+\mathrm{div}(h)) = f_{r,P}(([2]R)-(R))h(\mathrm{div}(f_{r,P})).$$

Finally, note that $f_{r,P}(([2]R)-(R)) \in \mathbb{F}_q^*$ and that $h(\mathrm{div}(f_{r,P})) = (h(P)/h(\mathcal{O}_E))^r \in (\mathbb{F}_{q^k}^*)^r$. The result follows. □

Exercise 26.3.12. Let the embedding degree k be even, $r \nmid (q^{k/2}-1)$, $P \in E(\mathbb{F}_q)$ and $Q = (x_Q, y_Q) \in E(\mathbb{F}_{q^k})$ points of order r. Suppose $x_Q \in \mathbb{F}_{q^{k/2}}$ (this is usually the case for points of cryptographic interest). Show that all vertical line functions can be omitted when computing the reduced Tate-Lichtenbam pairing.

26.3.3 Ate Pairing

Computing pairings on elliptic curves usually requires significantly more effort than exponentiation on an elliptic curve. There has been a concerted research effort to make pairing computation more efficient, and a large number of techniques are known. Due to lack of space we focus on one particular method known as "loop shortening". This idea originates in the work of Duursma and Lee [187] (for hyperelliptic curves) and was further developed by Barreto, Galbraith, Ó hÉigeartaigh and Scott [28]. We present the idea in the ate pairing formulation of Hess, Smart and Vercauteren [284]. Note that the ate pairing is not a "new" pairing. Rather, it is a way to efficiently compute a power, of a restriction to certain subgroups, of the Tate-Lichtenbaum pairing.

Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a large prime such that $r \mid \#E(\mathbb{F}_q) = q+1-t$ and $r \mid (q^k-1)$ for some relatively small integer k, but $r \nmid (q-1)$. It follows that $\#(E[r] \cap E(\mathbb{F}_q)) = r$. Since the Frobenius map is linear on the $\mathbb{F}_r$-vector space $E[r]$, and its characteristic polynomial satisfies

$$x^2 - tx + q \equiv (x-1)(x-q) \pmod{r},$$

it follows that π_q has distinct eigenvalues 1 and $q \pmod r$ and corresponding eigenspaces (i.e., subgroups)

$$G_1 = E[r] \cap \ker(\pi_q - [1]), \quad G_2 = E[r] \cap \ker(\pi_q - [q]). \tag{26.3}$$

Since, $r \mid (q^k-1)$ and $q \equiv (t-1) \pmod r$ it follows that $r \mid ((t-1)^k - 1)$. Let $T = t-1$ and $N = \gcd(T^k-1, q^k-1)$. Note that $r \mid N$. Define the **ate pairing** $a_T : G_2 \times G_1 \to \mu_r$ by

$$a_T(Q,P) = f_{T,Q}(P)^{(q^k-1)/N}.$$

The point is that $|t| \leq 2\sqrt{q}$ and, typically, $r \approx q$. Hence, computing the Miller function $f_{T,Q}$ typically requires at most half the number of steps as required to compute $f_{r,P}$. On the downside, the coefficients of the function $f_{T,Q}$ lie in $\mathbb{F}_{q^k}$, rather than $\mathbb{F}_q$ as before. Nevertheless, the ate pairing often leads to faster pairings if carefully implemented (especially when twists are exploited).

Theorem 26.3.13. *Let the notation be as above (in particular, $T = t-1$ and $N = \gcd(T^k-1, q^k-1)$). Let $L = (T^k-1)/N$ and $c = \sum_{i=0}^{k-1} q^i T^{k-1-i} \pmod r$. Then*

$$a_T(Q,P)^c = t_r(Q,P)^{L(q^k-1)/r}.$$

Hence, a_T is bilinear, and a_T is non-degenerate if and only if $r \nmid L$.

Proof: (Sketch) Consider $t_r(Q,P)^{(q^k-1)/r} = f_{r,Q}(P)^{(q^k-1)/r}$. Since $r \mid N$, Exercise 26.3.8 implies that this is equal to

$$f_{N,Q}(P)^{(q^k-1)/N}.$$

Indeed,

$$t_r(Q,P)^{L(q^k-1)/r} = f_{LN,Q}(P)^{(q^k-1)/N} = f_{T^k-1,Q}(P)^{(q^k-1)/N}.$$

Now, $[T^k-1]Q = \mathcal{O}_E$ so one can take $f_{T^k,Q} = f_{T^k-1,Q}$. (To prove this note that $\mathrm{div}(f_{T^k,Q}) = T^k(Q) - ([T^k]Q) - (T^k-1)(\mathcal{O}_E) = T^k(Q) - (Q) - (T^k-1)(\mathcal{O}_E) = (T^k-1)(Q) - (T^k-1)(\mathcal{O}_E)$.) Hence, the L-th power of the reduced Tate-Lichtenbaum pairing is $f_{T^k,Q}(P)^{(q^k-1)/N}$. Now,

$$f_{T^k,Q}(P) = f_{T,Q}(P)^{T^{k-1}} f_{T,[T]Q}(P)^{T^{k-2}} \cdots f_{T,[T^{k-1}]Q}(P), \tag{26.4}$$

which follows by considering the divisors of the left- and right-hand sides. The final step, and the only place we use $\pi_q(Q) = [q]Q = [T]Q$, is to note that

$$f_{T,[T]Q}(P) = f_{T,\pi_q(Q)}(P) = f_{T,Q}^q(P). \tag{26.5}$$

where f^q denotes raising all coefficients of the rational function f to the power q. This follows because E and P are defined over $\mathbb{F}_q$, so $\sigma(f_{T,Q}(P)) = f_{T,\sigma(Q)}(P)$ for all $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$. One therefore computes $f_{T^k,Q}(P) = f_{T,Q}(P)^c$, which completes the proof. □

Exercise 26.3.14. Generalise Theorem 26.3.13 to the case where $T \equiv q^m \pmod r$ for some $m \in \mathbb{N}$. What is the corresponding value of c?

26.3.4 Optimal Pairings

Lee, Lee and Park [369], Hess [283] and Vercauteren [618] have used combinations of pairings that have the potential for further loop shortening over that provided by the ate pairing.

Ideally, one wants to compute a pairing as $f_{M,Q}(P)$, with some final exponentation, where M is as small as possible. Hess and Vercauteren conjecture that the smallest possible value for $\log_2(M)$, for points of prime order r in an elliptic curve E over $\mathbb{F}_q$ with embedding degree $k(q,r)$, is $\log_2(r)/\varphi(k(q,r))$. For such a pairing, Miller's algorithm would be sped up by a factor of approximately $\varphi(k(q,r))$ compared with the time required when not using loop shortening. The method of Vercauteren actually gives a pairing as a product of $\prod_{i=0}^{l} f_{M_i,Q}(P)^{q^i}$ (together with some other terms) where all the integers M_i are of the desired size; such a pairing is not automatically computed faster than the naive method, but if the integers M_i all have a large common prefix in their binary expansions then such a saving can be obtained. If a pairing can be computed with approximately $\log_2(r)/\varphi(k(q,r))$ iterations in Miller's algorithm then it is called an **optimal pairing**.

The basic principle of Vercauteren's construction is to find a multiple ur, for some $u \in \mathbb{N}$, of the group order that can be written in the form

$$ur = \sum_{i=0}^{l} M_i q^i \tag{26.6}$$

where the $M_i \in \mathbb{Z}$ are "small". One can then show, just like with the ate pairing, that a certain power of the Tate-Lichtenbaum pairing is

$$\left(\prod_{i=0}^{l} f_{M_i,Q}(P)^{q^i} \prod_{i=1}^{l} g_i(P) \right)^{(q^k-1)/r}, \tag{26.7}$$

where the functions g_i take into account additions of certain elliptic curve points. Vercauteren proves that if

$$ukq^{k-1} \not\equiv \tfrac{(q^k-1)}{r} \left(\sum_{i=0}^{l} iM_i q^{i-1} \right) \pmod{r}$$

then the pairing is non-degenerate. The value of equation (26.7) can be computed efficiently only if all $f_{M_i,Q}(P)$ can, in some sense, be computed simultaneously. This is easiest when all but one of the M_i are small (i.e., in $\{-1, 0, 1\}$) or when the M_i have a large common prefix of most significant bits (possibly in signed binary expansion).

Vercauteren [618] suggests finding solutions to equation (26.6) using lattices. More precisely, given r and q one considers the lattice spanned by the rows of the following matrix

$$B = \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -q & 1 & 0 & \cdots & 0 \\ -q^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -q^l & 0 & 0 & \cdots & 1 \end{pmatrix}. \tag{26.8}$$

One sees that $(u, M_1, M_2, \ldots, M_l)B = (M_0, M_1, \ldots, M_l)$ and so candidate values for $u, M_0, \ldots, M_l$ can be found by finding short vectors in the lattice. A demonstration of this method is given in Example 26.6.3.

Note that loop shortening methods should not be confused with the methods, starting with Scott [534], that use an endomorphism on the curve to "recycle" some computations in Miller's algorithm. Such methods do not reduce the number of squarings in Miller's algorithm and, while valuable, do not give the same potential performance improvements as methods that use loop shortening.

26.3.5 Pairing Lattices

Hess [283] developed a framework for analysing pairings that is closely related to the framework in the previous section. We briefly sketch the ideas.

Definition 26.3.15. Let notation be as in Section 26.3.3, in particular q is a prime power, r is a prime, q is a primitive k-th root of unity modulo r, and the groups G_1 and G_2 are as in equation (26.3). Let $s \equiv q^m \pmod{r}$ for some $m \in \mathbb{N}$. For any $h(x) \in \mathbb{Z}[x]$ write $h(x) = \sum_{i=0}^{d} h_i x^i$. Let $P \in G_1$, $Q \in G_2$ and define $f_{s,h(x),Q}$ to be a function normalised at infinity (in the sense of Definition 26.3.4) such that

$$\operatorname{div}(f_{s,h(x),Q}) = \sum_{i=0}^{d} h_i(([s^i]Q) - (\mathcal{O}_E)).$$

Define

$$a_{s,h(x)}(Q, P) = f_{s,h(x),Q}(P)^{(q^k-1)/r}.$$

We stress here that h is a polynomial, not a rational function (as it was in previous sections).

Since $[s]Q = [q^m]Q = \pi_q^m(Q)$, a generalisation of equation (26.5) shows that $f_{h_i,[s^i]Q}(P) = f_{h_i,Q}(P)^{q^{mi}}$. It follows that one can compute $f_{s,h(x),Q}(P)$ efficiently using Miller's algorithm in a similar way to computing the pairings in the previous section. The running

time of Miller's algorithm is proportional to $\sum_{i=0}^{d} \log_2(\max\{1, |h_i|\})$ in the worse case (it performs better when the h_i have a large common prefix in their binary expansion).

Hess [283] shows that, for certain choices of $h(x)$, $a_{s,h(x)}$ is a non-degenerate and bilinear pairing. The goal is also to obtain good choices for $h(x)$ so that the pairing can be computed using a short loop. One of the major contributions of Hess [283] is to prove lower bounds on the size of the coefficients of any polynomial $h(x)$ that leads to a non-degenerate, bilinear pairing. This supports the optimality conjecture mentioned in the previous section.

Lemma 26.3.16. *Let notation be as in Definition 26.3.15.*

1. $a_{s,r}(Q,P)$ *is the Tate pairing.*
2. $a_{s,x-s}(Q,P)$ *is a power of the ate pairing.*
3. $a_{s,h(x)x}(Q,P) = a_{s,h(x)}(Q,P)^s$.
4. *Let* $h(x), g(x) \in \mathbb{Z}[x]$. *Then*

$$a_{s,h(x)+g(x)}(Q,P) = a_{s,h(x)}(Q,P)a_{s,g(x)}(Q,P) \quad \text{and} \quad a_{s,h(x)g(x)}(Q,P) = a_{s,h(x)}(Q,P)^{g(s)}.$$

Exercise 26.3.17.★ Prove Lemma 26.3.16.

Theorem 26.3.18. *Let notation be as above. Let* $s \in \mathbb{N}$ *be such that* s *is a primitive* k*-th root of unity modulo* r^2. *Let* $h(x) \in \mathbb{Z}[x]$ *be such that* $h(s) \equiv 0 \pmod{r}$ *but* $r^2 \nmid h(s)$. *Then* $a_{s,h(x)}$ *is a non-degenerate, bilinear pairing on* $G_2 \times G_1$.

Proof: Since $s^k \equiv 1 \pmod{r}$ it follows that $s \equiv q^m \pmod{r}$ for some $m \in \mathbb{N}$. Since $h(s) \equiv 0 \pmod{r}$ we can write

$$h(x) = g_1(x)(x-s) + g_2(x)r$$

for some $g_1(x), g_2(x) \in \mathbb{Z}[x]$. It follows from Lemma 26.3.16 that, for some $c \in \mathbb{N}$,

$$a_{s,h(x)}(Q,P) = a_T(Q,P)^{cg_1(s)}\hat{t}_r(Q,P)^{g_2(s)}$$

and so $a_{s,h(x)}$ is a bilinear pairing on $G_2 \times G_1$.

Finally, we need to prove non-degeneracy. By assumption, $r^2 \mid (s^k - 1)$ and so, in the version of Theorem 26.3.13 of Exercise 26.3.14, $r \mid L$. It follows that $a_T(Q,P) = 1$. Hence, $a_{s,h(x)}(Q,P) = \hat{t}_r(Q,P)^{g_2(s)}$. To complete the proof, note that $g_2(s) = h(s)/r$, and so $a_{s,h(x)}$ is non-degenerate if and only if $r^2 \nmid h(s)$. □

Hess [283] explains that this construction is "complete" in the sense that every bilinear map coming from functions in a natural class must correspond to some polynomial $h(x)$. Hess also proves that any polynomial $h(x) = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ satisfying the required conditions is such that $\sum_{i=0}^{d} |h_i| \geq r^{1/\varphi(k)}$. Polynomials $h(x)$ that have one coefficient of size $r^{1/\varphi(k)}$ and all other coefficients small satisfy the optimality conjecture. Good choices for the polynomial $h(x)$ are found by considering exactly the same lattice as in equation (26.8) (though in [283] it is written with q replaced by s).

26.4 Reduction of ECDLP to Finite Fields

An early application of pairings in elliptic curve cryptography was to reduce the discrete logarithm problem in $E(\mathbb{F}_q)[n]$, when $\gcd(n,q) = 1$, to the discrete logarithm problem in

the multiplicative group of a finite extension of $\mathbb{F}_q$. Menezes, Okamoto and Vanstone [417] used the Weil pairing to achieve this, while Frey and Rück [213] used the reduced Tate-Lichtenbaum pairing. The case $\gcd(n,q) \neq 1$ will be handled in Section 26.4.1.

The basic idea is as follows: Given an instance P, $Q = [a]P$ of the discrete logarithm problem in $E(\mathbb{F}_q)[n]$ and a non-degenerate bilinear pairing e, one finds a point $R \in E(\overline{\mathbb{F}}_q)$ such that $z = e(P,R) \neq 1$. It follows that $e(Q,R) = z^a$ in $\mu_n \subseteq \mathbb{F}_{q^k}^*$ where $k = k(q,n)$ is the embedding degree. When q is a prime power that is not prime then there is the possibility that μ_r lies in a proper subfield of $\mathbb{F}_{q^k}$, in which case re-define k to be the smallest positive rational number such that $\mathbb{F}_{q^k}$ is the smallest field of characteristic $\mathrm{char}(\mathbb{F}_q)$ containing μ_n.

The point is that if k is sufficiently small then index calculus algorithms in $\mathbb{F}_{q^k}^*$ could be faster than the baby-step-giant-step or Pollard rho algorithms in $E(\mathbb{F}_q)[n]$. Hence, one has reduced the discrete logarithm problem to a potentially easier problem. The reduction of the DLP from $E(\mathbb{F}_q)$ to a subgroup of $\mathbb{F}_{q^k}^*$ is called the **MOV/FR attack**.

Menezes, Okamoto and Vanstone [417] suggested to use the Weil pairing for the above idea. In this case, the point R can, in principle, be defined over a large extension of $\mathbb{F}_q$. Frey and Rück explained that the Tate-Lichtenbaum pairing is a more natural choice, since it is sufficient to take a suitable point $R \in E(\mathbb{F}_{q^k})$ where $k = k(q,n)$ is the embedding degree. Balasubramanian and Koblitz [26] showed that, in most cases, it is also sufficient to work in $E(\mathbb{F}_{q^k})$ when using the Weil pairing.

Theorem 26.4.1. *Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that $r \nmid (q-1)$ and that $\gcd(r,q) = 1$. Then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if r divides $(q^k - 1)$.*

Proof: See [26]. □

Balasubramanian and Koblitz also show that a "random" curve is expected to have very large embedding degree. Hence, the MOV/FR attack is not a serious threat to the ECDLP on randomly chosen elliptic curves. However, as noted by Menezes, Okamoto and Vanstone, supersingular elliptic curves are always potentially vulnerable to the attack.

Theorem 26.4.2. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$ and suppose $r \mid \#E(\mathbb{F}_q)$. Then the embedding degree $k(q,r)$ is such that $k(q,r) \leq 6$.*

Proof: See Corollary 9.11.9. □

26.4.1 Anomalous Curves

The discrete logarithm problem on elliptic curves over $\mathbb{F}_p$ with p points (such curves are called **anomalous elliptic curves**) can be efficiently solved. This was first noticed by Semaev [537] and generalised to higher genus curves by Rück [506]. We present their method in this section. An alternative way to view the attack (using p-adic lifting rather than differentials) was given by Satoh and Araki [512] and Smart [570].

The theoretical tool is an observation of Serre [541].

Lemma 26.4.3. *Let $P \in E(\mathbb{F}_p)$ have order p. Let f_P be a function in $\mathbb{F}_p(E)$ with $\mathrm{div}(f_P) = p(P) - p(\mathcal{O}_E)$. Then the map*

$$P \mapsto \frac{df_P}{f_P}$$

is a well-defined group homomorphism from $E(\mathbb{F}_p)[p]$ to $\Omega_{\mathbb{F}_p}(E)$.

Proof: First note that f_P is defined up to a constant, and that $d(cf_P)/(cf_P) = df_P/f_P$. Hence, the map is well-defined.

Now let $Q = [a]P$ and let f_P be as in the statement of the lemma. Then there is a function g such that

$$\mathrm{div}(g) = (Q) - a(P) + (a-1)(\mathcal{O}_E).$$

One has

$$\begin{aligned} \mathrm{div}(g^p f_P^a) &= p\mathrm{div}(g) + a\mathrm{div}(f_P) \\ &= p(Q) - ap(P) + p(a-1)(\mathcal{O}_E) + ap(P) - ap(\mathcal{O}_E) \\ &= p(Q) - p(\mathcal{O}_E). \end{aligned}$$

Hence, one can let $f_Q = g^p f_P^a$. Now, using part 4 of Lemma 8.5.17,

$$\frac{df_Q}{f_Q} = \frac{d(g^p f_P^a)}{g^p f_P^a} = \frac{g^p df_P^a + f_P^a dg^p}{g^p f_P^a}.$$

Part 6 of Lemma 8.5.17 gives $dg^p = pg^{p-1}dg = 0$ (since we are working in $\mathbb{F}_p$) and $df_P^a = af_P^{a-1}df_P$. Hence,

$$\frac{df_Q}{f_Q} = a\,\frac{df_P}{f_P},$$

which proves the result. □

Exercise 26.4.4. Generalise Lemma 26.4.3 to arbitrary curves.

Lemma 26.4.3 therefore maps the DLP in $E(\mathbb{F}_p)[p]$ to a DLP in $\Omega_{\mathbb{F}_p}(E)$. It remains to solve the DLP there.

Lemma 26.4.5. *Let the notation be as in Lemma 26.4.3. Let t be a uniformizer at $\mathcal{O}_E$. Write $f_P = t^{-p} + f_1 t^{-(p-1)} + f_2 t^{-(p-2)} + \cdots$. Then*

$$\frac{df_P}{f_P} = (f_1 + \cdots)dt.$$

Proof: Clearly, $f_P^{-1} = t^p - f_1 t^{p+1} + \cdots$. From part 8 of Lemma 8.5.17 we have

$$df_P = \left(\frac{\partial f_P}{\partial t}\right) dt = (-pt^{-p-1} - (p-1)f_1 t^{-p} + \cdots)dt.$$

Since we are working in $\mathbb{F}_p$, we have $df_P = (f_1 t^{-p} + \cdots)dt$. The result follows. □

Putting together Lemma 26.4.3 and Lemma 26.4.5: if $Q = [a]P$ then $df_P/f_P = (f_1 + \cdots)dt$ and $df_Q/f_Q = (af_1 + \cdots)dt$. Hence, as long as one can compute the expansion of df_P/f_P with respect to t, then one can solve the DLP. Indeed, this is easy: use Miller's algorithm with power series expansions to compute the power series expansion of f_P and follow the above calculations. Rück [506] gives an elegant formulation (for general curves) that computes only the desired coefficient f_1; he calls it the "additive version of the Tate-Lichtenbaum pairing".

26.5 Computational Problems

26.5.1 Pairing Inversion

We briefly discuss a computational problem that is required to be hard for many cryptographic applications of pairings.

Definition 26.5.1. Let G_1, G_2, G_T be groups of prime order r and let $e : G_1 \times G_2 \to G_T$ be a non-degenerate bilinear pairing. The **pairing inversion problem** is: Given $Q \in G_2, z \in G_T$ to compute $P \in G_1$ such that $e(P, Q) = z$.

The bilinear Diffie-Hellman problem was introduced in Definition 23.3.9. In additive notation it is: Given $P, Q, [a]Q, [b]Q$ to compute $e(P, Q)^{ab}$.

Lemma 26.5.2. *If one has an oracle for pairing inversion then one can solve BDH.*

Proof: Given the BDH instance $P, Q, [a]Q, [b]Q$ compute $z_1 = e(P, [a]Q)$ and call the pairing inversion oracle on (Q, z_1) to get P' such that $e(P', Q) = z_1$. It follows that $P' = [a]P$. One then computes $e(P', [b]Q) = e(P, Q)^{ab}$ as required. □

Further discussion of pairing inversion is given by Galbraith, Hess and Vercauteren [222].

Exercise 26.5.3. Show that if one can solve pairing inversion then one can solve the Diffie-Hellman problem in G_1.

Exercise 26.5.4. Show that if one has an oracle for pairing inversion then one can perform passive selective forgery of signatures in the Boneh-Boyen scheme presented in Figure 23.3.9.

Exercise 26.5.5. Show that if one has an oracle for pairing inversion then one can solve the q-SDH problem of Definition 22.2.17.

26.5.2 Solving DDH using Pairings

Pairings can be used to solve the decision Diffie-Hellman (DDH) problem in some cases. First, we consider a variant of DDH that can sometimes be solved using pairings.

Definition 26.5.6. Let $E(\mathbb{F}_q)$ be an elliptic curve and let $P, Q \in E(\mathbb{F}_q)$ have prime order r. The **co-DDH problem** is: Given $(P, [a]P, Q, [b]Q)$ to determine whether or not $a \equiv b \pmod{r}$.

Exercise 26.5.7. Show that co-DDH is equivalent to DDH if $Q \in \langle P \rangle$.

Suppose now that $E[r] \subseteq E(\mathbb{F}_q)$, $P \neq \mathcal{O}_E$, and that $Q \notin \langle P \rangle$. Then $\{P, Q\}$ generates $E[r]$ as a group. By non-degeneracy of the Weil pairing, we have $e_r(P, Q) \neq 1$. It follows that

$$e_r([a]P, Q) = e_r(P, Q)^a \quad \text{and} \quad e_r(P, [b]Q) = e_r(P, Q)^b.$$

Hence, the co-DDH problem can be efficiently solved using the Weil pairing.

The above approach cannot be used to solve DDH, since $e_r(P, P) = 1$ by the alternating property of the Weil pairing. In some special cases, the reduced Tate-Lichtenbaum pairing satisfies $\hat{t}_r(P, P) \neq 1$ and so can be used to solve DDH in $\langle P \rangle$. In general, however, DDH cannot be solved by such simple methods.

When E is a supersingular elliptic curve and $P \neq \mathcal{O}_E$ then, even if $\hat{t}_r(P, P) = 1$, there always exists an endomorphism $\psi : E \to E$ such that $\hat{t}_r(P, \psi(P)) \neq 1$. Such an endomorphism is called a **distortion map**; see Section 26.6.1. It follows that DDH is easy on supersingular elliptic curves.

26.6 Pairing-Friendly Elliptic Curves

The cryptographic protocols given in Sections 22.2.3 and 23.3.2 relied on "pairing groups". We now mention the properties needed to have a practical system, and give some popular examples.

For pairing-based cryptography it is desired to have elliptic curves E over $\mathbb{F}_q$ such that:

1. there is a large prime r dividing $\#E(\mathbb{F}_q)$, with $\gcd(r, q) = 1$;
2. the DLP in $E(\mathbb{F}_q)[r]$ is hard;
3. the DLP in $\mathbb{F}_{q^k}^*$ is hard, where $k = k(q, r)$ is the embedding degree;
4. computation in $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^*$ is efficient;
5. elements of $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^*$ can be represented compactly.

Elliptic curves with these properties are called **pairing-friendly curves**. Note that the conditions are incompatible: for the DLP in $\mathbb{F}_{q^k}^*$ to be hard it is necessary that q^k be large (say, at least 3000 bits) to resist index calculus attacks like those in Chapter 15, whereas to represent elements of $\mathbb{F}_{q^k}^*$ compactly we would like q^k to be small. Luckily, we can use techniques such as those in Chapter 6 to represent field elements relatively compactly.

There is a large literature on pairing-friendly elliptic curves, culminating in the "taxonomy" by Freeman, Scott and Teske [210]. We give two examples below.

Example 26.6.1. For $a = 0, 1$ define

$$E_a : y^2 + y = x^3 + x + a$$

over $\mathbb{F}_2$. Then E_a is supersingular and $\#E_a(\mathbb{F}_{2^l}) = 2^l \pm 2^{(l+1)/2} + 1$ when l is odd. Some of these integers have large prime divisors, for example $2^{241} - 2^{121} + 1$ is prime. The embedding degree can be shown to be 4 in general; this follows since

$$(2^l + 2^{(l+1)/2} + 1)(2^l - 2^{(l+1)/2} + 1) = 2^{2l} + 1 \mid (2^{4l} - 1).$$

Example 26.6.2. (Barreto-Naehrig curves [30]) Consider the polynomials

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \quad \text{and} \quad t(x) = 6x^2 + 1 \tag{26.9}$$

in $\mathbb{Z}[x]$. Note that $t(x)^2 - 4p(x) = -3(6x^2 + 4x + 1)^2$, that $r(x) = p(x) + 1 - t(x)$ is irreducible over $\mathbb{Q}$, and that $r(x) \mid (p(x)^{12} - 1)$. Suppose $x_0 \in \mathbb{Z}$ is such that $p = p(x_0)$ is prime and $r = r(x_0)$ is prime (or is the product of a small integer with a large prime). Then the embedding degree $k(p, r)$ is a divisor of 12 (and is typically equal to 12). Furthermore, one can easily construct an elliptic curve $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = r$; one of the 6 twists of $y^2 = x^3 + 1$ will suffice. Note that $p \equiv 1 \pmod 3$ and E is an ordinary elliptic curve.

Example 26.6.3. The family of curve parameters in Example 26.6.2 has $t \approx \sqrt{p}$ and so the ate pairing is computed in about half the time of the reduced Tate-Lichtenbaum pairing, as usual. We now demonstrate an optimal pairing with these parameters.

Substituting the polynomials $r(x)$ and $p(x)$ for the values r and q in the matrix of equation (26.8) gives a lattice. Lattice reduction over $\mathbb{Z}[x]$ yields the short vector $(M_0, M_1, M_2, M_3) = (6x+2, 1, -1, 1)$. It is easy to verify that $6x+2+p(x)-p(x)^2+p(x)^3 \equiv 0 \pmod{r(x)}$.

Now $f_{1,Q} = 1$ and $f_{-1,Q} = v_Q$ (and so both can be omitted in pairing computation, by Exercise 26.3.12). The ate pairing can be computed as $f_{6x+2,Q}(P)$ multiplied with three straight line functions, and followed by the final exponentiation; see Section IV of [618]. The point is that Miller's algorithm now runs for approximately one quarter of the iterations as when computing the Tate-Lichtenbaum pairing.

26.6.1 Distortion Maps

As noted, when $\hat{t}_r(P,P) = 1$ one can try to find an endomorphism $\psi : E \to E$ such that $\hat{t}_r(P, \psi(P)) \neq 1$.

Definition 26.6.4. Let E be an elliptic curve over $\mathbb{F}_q$, let $r \mid \#E(\mathbb{F}_q)$ be prime, let $e : E[r] \times E[r] \to \mu_r$ be a non-degenerate and bilinear pairing, and let $P \in E(\mathbb{F}_q)[r]$. A **distortion map** with respect to E, r, e and P is an endomorphism ψ such that $e(P, \psi(P)) \neq 1$.

Verheul (Theorem 5 of [620]) shows that if E is a supersingular elliptic curve then, for any point $P \in E(\mathbb{F}_{q^k}) - \{\mathcal{O}_E\}$, a distortion map exists. In particular, when $P \in E(\mathbb{F}_q)[r] - \{\mathcal{O}_E\}$ and $k > 1$ then there is an endomorphism ψ (necessarily not defined over $\mathbb{F}_q$) such that $\hat{t}(P, \psi(P)) \neq 1$. Since P is defined over the small field, we have a compact representation for all elliptic curve points in the cryptosystem, as well as efficiency gains in Miller's algorithm. For this reason, pairings on supersingular curves are often the fastest choice for certain applications.

Example 26.6.5. Consider again the elliptic curves from Example 26.6.1. An automorphism on E_a is $\psi(x,y) = (x + s^2, y + sx + t)$ where $s \in \mathbb{F}_{2^2}$ and $t \in \mathbb{F}_{2^4}$ satisfy $s^2 = s + 1$ and $t^2 = t + s$. One can represent $\mathbb{F}_{2^{4m}}$ using the basis $\{1, s, t, st\}$. It is clear that if $P \in E_a(\mathbb{F}_{2^l})$ where l is odd then $\psi(P) \in E_a(\mathbb{F}_{2^{4l}})$ and $\psi(P) \notin E_a(\mathbb{F}_{2^{2l}})$, and so ψ is a distortion map for P.

Exercise 26.6.6. Let E be an elliptic curve over $\mathbb{F}_q$ and let $r \mid \#E(\mathbb{F}_q)$ be prime. Let $k = k(q,r) > 1$ be the embedding degree. For any point $P \in E(\mathbb{F}_{q^k})$ define the trace map

$$\mathrm{Tr}(P) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)} \sigma(P).$$

Show that $\mathrm{Tr}(P) \in E(\mathbb{F}_q)$. Now, suppose $P \in E[r]$, $P \notin E(\mathbb{F}_q)$ and $\mathrm{Tr}(P) \neq \mathcal{O}_E$. Show that $\{P, \mathrm{Tr}(P)\}$ generates $E[r]$. Deduce that the trace map is a distortion map with respect to E, r, e_r and P.

Exercise 26.6.7. Let notation be as in Exercise 26.6.6. Show that if $Q \in E[r] \cap \ker(\pi_q - [1])$ then $\mathrm{Tr}(Q) = [k]Q$. Show that if $Q \in E[r] \cap \ker(\pi_q - [q])$ then $\mathrm{Tr}(Q) = \mathcal{O}_E$. Hence, deduce that the trace map is not a distortion map for the groups G_1 or G_2 of equation (26.3).

26.6.2 Using Twists to Improve Pairing-Based Cryptography

There are significant advantages from using twists in pairing-based cryptography when using ordinary elliptic curves. Suppose we are using the ate pairing or some other optimal pairing and are working with the subgroups $G_1, G_2 \subset E(\mathbb{F}_{q^k})$, which are Frobenius eigenspaces. Then $G_1 \subset E(\mathbb{F}_q)$ and it can be shown that $G_2 \subset E'(\mathbb{F}_q^{k/d})$ where E' is a twist of E and $d = \#\mathrm{Aut}(E)$. For the elliptic curve in Example 26.6.2 one can represent the p-eigenspace of Frobenius in $E(\mathbb{F}_{p^{12}})$ as a subgroup of $E'(\mathbb{F}_{p^2})$ for a suitable twist of E (this is because $\#\mathrm{Aut}(E) = 6$). For details we refer to [30, 284].

There are at least two advantages to this method. First, elements in the group G_2 of the pairing have a compressed representation. Second, the ate pairing computation is made much more efficient by working with Miller functions on the twisted curve E'. We do not present any further details.

Appendix A

Background Mathematics

For convenience, we summarise some notation, conventions, definitions and results that will be used in the book. This chapter is for reference only.

A.1 Basic Notation

We write $\mathbb{R}$ for the real numbers and define $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$ and similarly for $\mathbb{R}_{>0}$. We write $\mathbb{Z}$ for the integers and $\mathbb{N} = \mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, \ldots\}$ for the natural numbers.

We write $\#S$ for the number of elements of a finite set S. If S, T are sets we write $S - T$ for the set difference $\{s \in S : s \notin T\}$. We denote the empty set by $\varnothing$.

We write $\mathbb{Z}/n\mathbb{Z}$ for the ring of integers modulo n (many authors write $\mathbb{Z}_n$). When n is a prime and we are using the field structure of $\mathbb{Z}/n\mathbb{Z}$ we prefer to write $\mathbb{F}_n$. The statement $a \equiv b \pmod{n}$ means that $n \mid (a - b)$. We follow a common mis-use of this notation by writing $b \pmod{n}$ for the integer $a \in \{0, 1, \ldots, n-1\}$ such that $a \equiv b \pmod{n}$. Hence, the statement $a = b \pmod{n}$ is an assignment of a to the value of the operator $b \pmod{n}$ and should not be confused with the predicate $a \equiv b \pmod{n}$.

The word **map** $f : X \to Y$ means a function on some subset of X. In other words a map is not necessarily defined everywhere. Usually the word **function** implicitly means "defined everywhere on X", though this usage does not apply in algebraic geometry where a rational function is actually a rational map. If $f : X \to Y$ is a map and $U \subset X$ then we write $f|_U$ for the restriction of f to U, which is a map $f|_U : U \to Y$.

If $P = (x_P, y_P)$ is a point and f is a function on points then we write $f(x_P, y_P)$ rather than $f((x_P, y_P))$ for $f(P)$. We write $f \circ g$ for composition of functions (i.e., $(f \circ g)(x) = f(g(x))$); the notation fg will always mean product (i.e., $fg(P) = f(P)g(P)$). The notation f^n usually means exponentiating the value of the function f to the power n, except when f is an endomorphism of an elliptic curve (or Abelian variety), in which

context it is standard to write f^n for n-fold composition. Hence, we prefer to write $f(P)^n$ than $f^n(P)$ when denoting powering (and so we write $\log(x)^n$ rather than $\log^n(x)$).

A.2 Groups

Let G be a group and $g \in G$. The **subgroup generated by** g is $\langle g \rangle = \{g^a : a \in \mathbb{Z}\}$. The **order** of the element g is the number of elements in the group $\langle g \rangle$. The **exponent** of a finite group is the smallest positive integer n such that $g^n = 1$ for all $g \in G$.

Let G be a finite Abelian group. The classification of finite Abelian groups (see Theorem II.2.1 of [301] or Section I.8 of [367]) states that G is isomorphic to a direct sum of cyclic groups of orders $m_1, m_2, \ldots, m_t$ such that $m_1 \mid m_2 \mid \cdots \mid m_t$.

A.3 Rings

All rings in this book have a multiplicative identity 1. For any ring R, the smallest positive integer n such that $n1 = 0$ is called the **characteristic** of the ring and is denoted $\mathrm{char}(R)$. If there is no such n then we define $\mathrm{char}(R) = 0$.

If R is a ring and $n \in \mathbb{N}$ then we write $M_n(R)$ for the ring of $n \times n$ matrices with entries in R.

If R is a ring then R^* is the multiplicative group of invertible elements of R. The **Euler phi function** $\varphi(n)$ is the order of $(\mathbb{Z}/n\mathbb{Z})^*$. One has

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Theorem A.3.1. *There exists $N \in \mathbb{N}$ such that $\varphi(n) > n/(3\log(\log(n)))$ for all $n \in \mathbb{N}_{>N}$.*

Proof: Theorem 328 of [276] states that

$$\liminf_{n \to \infty} \frac{\varphi(n)\log(\log(n))}{n} = e^{-\gamma}$$

where $\gamma \approx 0.57721566$ is the Euler-Mascheroni constant. Since $e^{-\gamma} \approx 0.56 > 1/3$ the result follows from the definition of $\liminf$. □

An element $a \in R$ is **irreducible** if $a \notin R^*$ and $a = bc$ for $b, c \in R$ implies $b \in R^*$ or $c \in R^*$. We write $a \mid b$ for $a, b \in R$ if there exists $c \in R$ such that $b = ac$. An element $a \in R$ is **prime** if $a \mid bc$ implies $a \mid b$ or $a \mid c$.

An integral domain R is a **unique factorisation domain** (UFD) if each $a \in R$ can be written uniquely (up to ordering and multiplication by units) as a product of irreducibles. In a UFD an element is prime if and only if it is irreducible.

A.4 Modules

Let R be a ring. An R-module M is an Abelian group, written additively, with an operation rm for $r \in R$ and $m \in M$, such that $(r_1 + r_2)m = r_1 m + r_2 m$ and $r(m_1 + m_2) = rm_1 + rm_2$. An R-module M is **finitely generated** if there is a set $\{m_1, \ldots, m_k\} \subset M$ such that $M = \{\sum_{i=1}^k r_i m_i : r_i \in R\}$.

A finitely generated R-module M is a **free module** if there is a set $\{m_1, \ldots, m_k\}$ that generates M and is such that $0 = \sum_{i=1}^{k} r_i m_i$ if and only if $r_i = 0$ for all $1 \leq i \leq k$. Such an R-module is said to have **rank** k.

Let R be a commutative ring, M an R-module and $\Bbbk$ a field containing R. Consider the set of all symbols of the form $m \otimes a$ where $m \in M$, $a \in \Bbbk$ under the equivalence relation $rm \otimes a \equiv m \otimes ra$ for $r \in R$, $(m_1 + m_2) \otimes a = (m_1 \otimes a) + (m_1 \otimes a)$ and $m \otimes (a_1 + a_2) = (m \otimes a_1) + (m \otimes a_2)$. The **tensor product** $M \otimes_R \Bbbk$ is the set of all equivalence classes of such symbols. If M is a finitely generated free R-module with generating set $\{m_1, \ldots, m_k\}$ then $M \otimes_R \Bbbk$ is a $\Bbbk$-vector space of dimension k with basis $\{m_1 \otimes 1, \ldots, m_k \otimes 1\}$.

A.5 Polynomials

Let R be a commutative ring. Denote by $R[\underline{x}] = R[x_1, \ldots, x_n]$ the set of polynomials over R in n variables. We write $\deg_{x_i}(F(x_1, \ldots, x_n))$ to be the degree as a polynomial in x_i with coefficients in $R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. For polynomials $F(x) \in R[x]$ we write $\deg(F(x))$ for $\deg_x(F(x))$. The **total degree** of a polynomial $F(\underline{x}) = \sum_{i=1}^{l} F_i x_1^{m_{i,1}} \cdots x_n^{m_{i,n}}$ (with $F_i \neq 0$) is $\deg(F) = \max_{1 \leq i \leq l} \sum_{j=1}^{n} m_{i,j}$.

Let R be a commutative ring with a unit 1. A degree d polynomial in $R[x]$ is **monic** if the coefficient of x^d is 1.

A polynomial $F(\underline{x}) \in R[\underline{x}]$ is divisible by $G(\underline{x}) \in R[\underline{x}]$ if there exists a polynomial $H(\underline{x}) \in R[\underline{x}]$ such that $F(\underline{x}) = G(\underline{x})H(\underline{x})$. A polynomial $F(\underline{x}) \in R[\underline{x}]$ is **irreducible** over R (also called R-irreducible) if whenever $F(\underline{x}) = G(\underline{x})H(\underline{x})$ with $G(\underline{x}), H(\underline{x}) \in R[\underline{x}]$ then either G or H is a constant polynomial.

There are various ways to show that a polynomial is irreducible. **Eisenstein's criteria** states that $F(x) = \sum_{i=0}^{n} F_i x^i \in R[x]$, where R is a UFD, is irreducible if there is a prime p in R such that $p \nmid F_n$, $p \mid F_i$ for $0 \leq i < n$, and $p^2 \nmid F_0$. We refer to Proposition III.1.14 of [589], Theorem IV.3.1 of [367] or Theorem III.6.15 of [301] for proofs.

If $\Bbbk$ is a field then the polynomial ring $\Bbbk[x_1, \ldots, x_n]$ is a UFD (Theorem III.6.14 of [301]). Let $F(x) \in \Bbbk[x]$ be a polynomial in one variable of degree d. Then either $F = 0$ or else $F(x)$ has at most d roots in $\Bbbk$.

Lemma A.5.1. *Let $N_{d,q}$ be the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[x]$. Then $q^d/2d \leq N_{d,q} \leq q^d/d$.*

Proof: See Theorem 20.11 of [556] or Exercise 3.27 of [388]. A more precise result is given in Theorem 15.5.12. □

Let $F(x) \in \Bbbk[x]$. One can define the **derivative** $F'(x)$ by using the rule $(F_n x^n)' = nF_n x^{n-1}$ for $n \geq 0$ for each monomial. This is a formal algebraic operation and does not require an interpretation in terms of calculus.

Lemma A.5.2. *Let $F_1(x), F_2(x) \in \Bbbk[x]$. Then*

1. $(F_1(x) + F_2(x))' = F_1'(x) + F_2'(x)$.
2. $(F_1(x)F_2(x))' = F_1(x)F_2'(x) + F_2(x)F_1'(x)$.
3. $(F_1(F_2(x))' = F_1'(F_2(x))F_2'(x)$
4. *If* $\mathrm{char}(\Bbbk) = p$ *then* $F'(x) = 0$ *if and only* $F(x) = G(x)^p$ *for some* $G(x) \in \Bbbk[x]$.

Similarly, the notation $\partial F/\partial x_i$ is used for polynomials $F(\underline{x}) \in \Bbbk[\underline{x}]$ and an analogue of Lemma A.5.2 holds.

A.5.1 Homogeneous Polynomials

Definition A.5.3. A non-zero polynomial $F(\underline{x}) \in \Bbbk[\underline{x}]$ is **homogeneous** of degree d if all its monomials have degree d, i.e.,

$$F(x_0, \ldots, x_n) = \sum_{\substack{i_0, i_1, \ldots, i_n \in \mathbb{Z}_{\geq 0} \\ i_0 + i_1 + \cdots i_n = d}} F_{i_0, i_1, \ldots, i_n} x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n}.$$

Any polynomial $F(\underline{x}) \in \Bbbk[x_0, \ldots, x_n]$ can be written as a **homogeneous decomposition** $\sum_{i=0}^{m} F_i(\underline{x})$ for some $m \in \mathbb{N}$ where $F_i(\underline{x})$ is a homogeneous polynomial of degree i; see Section II.3 of [367].

Lemma A.5.4. *Let R be an integral domain.*

1. *If $F(x) \in R[x_0, \ldots, x_n]$ is homogeneous and $\lambda \in R$ then $F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n)$.*
2. *If $F_1, F_2 \in R[x_0, \ldots, x_n]$ are non-zero and homogeneous of degrees r and s respectively then $F_1(\underline{x})F_2(\underline{x})$ is homogeneous of degree $r + s$.*
3. *Let $F_1, F_2 \in R[x_0, \ldots, x_n]$ be non-zero. If $F_1(\underline{x})F_2(\underline{x})$ is homogeneous then $F_1(\underline{x})$ and $F_2(\underline{x})$ are both homogeneous.*

Proof: See Exercise 1-1 (page 6) of Fulton [216]. □

A.5.2 Resultants

Let R be a commutative integral domain. Let $F(x) = F_n x^n + F_{n-1} x^{n-1} + \cdots + F_0$ and $G(x) = G_m x^m + G_{n-1} x^{n-1} + \cdots + G_0$ be two polynomials over R with $F_0, F_n, G_0, G_m \neq 0$. The polynomials $F, xF, \ldots, x^{m-1}F, G, xG, \ldots, x^{n-1}G$ can be written as $n+m$ linear combinations of the $n+m$ variables $1, x, \ldots, x^{n+m-1}$ and so the variable x may be eliminated to compute the **resultant** (there should be no confusion between the use of the symbol R for both the ring and the resultant)

$$R(F, G) = R_x(F, G) = \det \begin{pmatrix} F_0 & F_1 & \cdots & F_n & 0 & 0 & \cdots & 0 \\ 0 & F_0 & \cdots & F_{n-1} & F_n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & F_0 & F_1 & \cdots & F_n \\ G_0 & \cdots & G_m & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & G_0 & \cdots & G_m & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & G_0 & \cdots & G_m \end{pmatrix}.$$

Theorem A.5.5. *Let $\Bbbk$ be a field and $F(x), G(x) \in \Bbbk[x]$. Write $F(x) = \sum_{i=0}^{n} F_i x^i$ and $G(x) = \sum_{i=0}^{m} G_i x^i$. Suppose $F_0 G_0 \neq 0$. Then $R(F(x), G(x)) = 0$ if and only if $F(x)$ and $G(x)$ have a common root in $\overline{\Bbbk}$.*

Proof: See Proposition IV.8.1 and Corollary IV.8.4 of Lang [367] or Proposition 3.5.8 of Cox, Little and O'Shea [158]. □

Theorem A.5.5 is generalised to polynomials in $R[x]$ where R is a UFD in Lemma 2.6 on page 41 of Lorenzini [394]. Section IV.2.7 of [394] also describes the relation between $R(F, G)$ and the norm of $G(\alpha)$ in the number ring generated by a root α of $F(x)$.

If $F(x, y), G(x, y) \in \mathbb{Z}[x, y]$ then write $R_x(F, G) \in \mathbb{Z}[y]$ for the resultant, which is a polynomial in y, obtained by treating F and G as polynomials in x over the ring $R = \mathbb{Z}[y]$. If F and G have total degree d in x and y then the degree in y of $R_x(F, G)$ is $O(d^2)$.

A.6 Field Extensions

General references for fields and their extensions are Chapter II of Artin [14], Chapter V of Hungerford [301] or Chapter V of Lang [367].

Let $\Bbbk$ be a field. An **extension** of $\Bbbk$ is any field $\Bbbk'$ such that $\Bbbk \subseteq \Bbbk'$, in which case we write $\Bbbk'/\Bbbk$. Then $\Bbbk'$ is a vector space over $\Bbbk$. If this vector space has finite dimension then the **degree** of $\Bbbk'/\Bbbk$, denoted $[\Bbbk' : \Bbbk]$, is the vector space dimension of $\Bbbk'$ over $\Bbbk$.

An element $\theta \in \Bbbk'$ is **algebraic** over $\Bbbk$ if there is some polynomial $F(x) \in \Bbbk[x]$ such that $F(\theta) = 0$. An extension $\Bbbk'$ of $\Bbbk$ is **algebraic** if every $\theta \in \Bbbk'$ is algebraic over $\Bbbk$. If $\Bbbk'/\Bbbk$ is algebraic and $\Bbbk \subseteq \Bbbk'' \subseteq \Bbbk'$ then $\Bbbk''/\Bbbk$ and $\Bbbk'/\Bbbk''$ are algebraic. Similarly, if $\Bbbk'/\Bbbk$ is finite then $[\Bbbk' : \Bbbk] = [\Bbbk' : \Bbbk''][\Bbbk'' : \Bbbk]$.

Lemma A.6.1. *Let $\Bbbk$ be a field. Every finite extension of $\Bbbk$ is algebraic.*

Proof: See Theorem 4 of Section II.3 of [640], Proposition V.1.1 of [367], or Theorem V.1.11 of [301]. □

The **compositum** of two fields $\Bbbk$ and $\Bbbk'$ is the smallest field that contains both of them. We define $\Bbbk(\theta) = \{a(\theta)/b(\theta) : a(x), b(x) \in \Bbbk[x], b(\theta) \neq 0\}$ for any element θ. This is the smallest field that contains $\Bbbk$ and θ. For example, θ may be algebraic over $\Bbbk$ (e.g., $\Bbbk(\sqrt{-1})$) or transcendental (e.g., $\Bbbk(x)$). More generally, $\Bbbk(\theta_1, \ldots, \theta_n) = \Bbbk(\theta_1)(\theta_2)\cdots(\theta_n)$ is the field generated over $\Bbbk$ by $\theta_1, \ldots, \theta_n$. A field extension $\Bbbk'/\Bbbk$ is **finitely generated** if $\Bbbk' = \Bbbk(\theta_1, \ldots, \theta_n)$ for some $\theta_1, \ldots, \theta_n \in \Bbbk'$.

Theorem A.6.2. *Let $\Bbbk$ be a field. Suppose K is field that is finitely generated as a ring over $\Bbbk$. Then K is an algebraic extension of $\Bbbk$.*

Proof: See pages 31-33 of Fulton [216]. □

An **algebraic closure** of a field $\Bbbk$ is a field $\overline{\Bbbk}$ such that every non-constant polynomial in $\overline{\Bbbk}[x]$ has a root in $\overline{\Bbbk}$. For details see Section V.2 of [367]. We always assume that there is a fixed algebraic closure of $\Bbbk$ and we assume that every algebraic extension $\Bbbk'/\Bbbk$ is chosen such that $\Bbbk' \subset \overline{\Bbbk}$ and that $\overline{\Bbbk'} = \overline{\Bbbk}$. Since the main case of interest is $\Bbbk = \mathbb{F}_q$ this assumption is quite natural.

We recall the notions of separable and purely inseparable extensions (see Sections V.4 and V.6 of Lang [367], Section V.6 of Hungerford [301] or Sections A.7 and A.8 of Stichtenoth [589]). An element α, algebraic over a field $\Bbbk$, is **separable** (respectively, **purely inseparable**) if the minimal polynomial of α over $\Bbbk$ has distinct roots (respectively, one root) in $\overline{\Bbbk}$. Hence, α is separable over $\Bbbk$ if its minimal polynomial has non-zero derivative. If $\mathrm{char}(\Bbbk) = p$ then α is purely inseparable if the minimal polynomial of α is of the form $x^{p^m} - a$ for some $a \in \Bbbk$.

Let $\Bbbk'/\Bbbk$ be a finite extension of fields and let $\alpha \in \Bbbk'$. One can define the **norm** and **trace** of α in terms of the matrix representation of multiplication by α as a linear map on the vector space $\Bbbk'/\Bbbk$ (see Section A.14 of [589] or Section IV.2 of [394]). When $\Bbbk'/\Bbbk$ is separable then an equivalent definition is to let $\sigma_i : \Bbbk' \to \overline{\Bbbk}$ be the $n = [\Bbbk' : \Bbbk]$ distinct embeddings (i.e., injective field homomorphisms), then the norm of $\alpha \in \Bbbk'$ is $N_{\Bbbk'/\Bbbk}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ and the **trace** is $\mathrm{Tr}_{\Bbbk'/\Bbbk}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.

An element $x \in K$ is **transcendental** over $\Bbbk$ if x is not algebraic over $\Bbbk$. Unless there is an implicit algebraic relation between $x_1, \ldots, x_n$ we write $\Bbbk(x_1, \ldots, x_n)$ to mean the field $\Bbbk(x_1)(x_2)\cdots(x_n)$ where each x_i is transcendental over $\Bbbk(x_1, \ldots, x_{i-1})$.

Definition A.6.3. Let K be a finitely generated field extension of $\Bbbk$. The **transcendence degree** of $K/\Bbbk$, denoted $\mathrm{trdeg}(K/\Bbbk)$, is the smallest integer n such that there are $x_1, \ldots, x_n \in K$ with K algebraic over $\Bbbk(x_1, \ldots, x_n)$ (by definition x_i is transcendental over $\Bbbk(x_1, \ldots, x_{i-1})$). Such a set $\{x_1, \ldots, x_n\}$ is called a **transcendence basis** for $K/\Bbbk$.

Theorem A.6.4. *Let $K/\Bbbk$ be a finitely generated field extension. Then the transcendence degree is well-defined (i.e., all transcendence bases have the same number of elements).*

Proof: See Theorem 25 of Section II.12 of [640], Theorem VI.1.8 of [301] or Theorem 1.6.13 of [635]. □

Theorem A.6.5. *Let $K/\Bbbk$ and F/K be finitely generated field extensions. Then* $\mathrm{trdeg}(F/\Bbbk) = \mathrm{trdeg}(F/K) + \mathrm{trdeg}(K/\Bbbk)$.

Proof: See Theorem 26 of Section II.12 of [640]. □

Corollary A.6.6. *Let $K/\Bbbk$ be finitely generated with transcendence degree 1 and let $x \in K$ be transcendental over $\Bbbk$. Then K is a finite algebraic extension of $\Bbbk(x)$.*

A **perfect field** is one for which every algebraic extension is separable. A convenient equivalent definition is that a field $\Bbbk$ of characteristic p is perfect if $\{x^p : x \in \Bbbk\} = \Bbbk$ (see Section V.6 of Lang [367]). We restrict to perfect fields for a number of reasons, one of which is that the primitive element theorem does not hold for non-perfect fields, and another is due to issues with fields of definition (see Remark 5.3.7). Finite fields, fields of characteristic 0, and algebraic closures of finite fields are perfect (see Exercise V.7.13 of [301] or Section V.6 of [367]).

Theorem A.6.7. ***(Primitive element theorem)*** *Let $\Bbbk$ be a perfect field. If $\Bbbk'/\Bbbk$ is a finite, separable extension then there is some $\alpha \in \Bbbk'$ such that $\Bbbk' = \Bbbk(\alpha)$.*

Proof: Theorem V.6.15 of [301], Theorem 27 of [14], Theorem V.4.6 of [367]. □

A.7 Galois Theory

For an introduction to Galois theory see Chapter V of Hungerford [301], Chapter 6 of Lang [367] or Stewart [585]. An algebraic extension $\Bbbk'/\Bbbk$ is Galois if it is normal (i.e., every irreducible polynomial $F(x) \in \Bbbk[x]$ with a root in $\Bbbk'$ splits completely over $\Bbbk'$) and separable. The Galois group of $\Bbbk'/\Bbbk$ is

$$\mathrm{Gal}(\Bbbk'/\Bbbk) = \{\sigma : \Bbbk' \to \Bbbk' : \sigma \text{ is a field automorphism, and } \sigma(x) = x \text{ for all } x \in \Bbbk\}.$$

Theorem A.7.1. *Let $\Bbbk'/\Bbbk$ be a finite Galois extension. Then there is a one-to-one correspondence between the set of subfields $\{\Bbbk'' : \Bbbk \subseteq \Bbbk'' \subseteq \Bbbk'\}$ and the set of normal subgroups H of* $\mathrm{Gal}(\Bbbk'/\Bbbk)$*, via*

$$\Bbbk'' = \{x \in \Bbbk' : \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Proof: See Theorem V.2.5 of [301]. □

If $\Bbbk$ is a perfect field then $\overline{\Bbbk}$ is a separable extension and hence a Galois extension of $\Bbbk$. If $\Bbbk'$ is any algebraic extension of $\Bbbk$ (not necessarily Galois) then $\overline{\Bbbk}/\Bbbk'$ is Galois. The Galois group $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ can be defined using the notion of an inverse limit (see Chapter 5 of [124]). Topological aspects of $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ are important, but we do not discuss them.

A.7.1 Galois Cohomology

One finds brief summaries of **Galois cohomology** in Appendix B of Silverman [564] and Chapter 19 of Cassels [122]. More detailed references are Serre [542] and Cassels and Frölich [124].

Let $K/\Bbbk$ be Galois (we include $K = \overline{\Bbbk}$). Let $G = \mathrm{Gal}(K/\Bbbk)$. Unlike most references we write our Galois groups acting on the left (i.e., as $\sigma(f)$ rather than f^σ). A 1-cocyle in the additive group K is a function[1] $\xi : G \to K$ such that $\xi(\sigma\tau) = \sigma(\xi(\tau)) + \xi(\sigma)$. A 1-coboundary in K is the function $\xi(\sigma) = \sigma(\gamma) - \gamma$ for some $\gamma \in K$. The group of 1-cocycles modulo 1-coboundaries (the group operation is addition $(\xi_1 + \xi_2)(\tau) = \xi_1(\tau) + \xi_2(\tau)$) is denoted $H^1(G, K)$. Similarly, for the multiplicative group K^*, a 1-cocyle satisfies $\xi(\sigma\tau) = \sigma(\xi(\tau))\xi(\sigma)$, a 1-coboundary is $\sigma(\gamma)/\gamma$ and the quotient group is denoted $H^1(G, K^*)$.

Theorem A.7.2. *Let $K/\Bbbk$ be Galois. Then $H^1(\mathrm{Gal}(K/\Bbbk), K) = \{0\}$ and (**Hilbert 90**) $H^1(\mathrm{Gal}(K/\Bbbk), K^*) = \{1\}$ (i.e., both groups are trivial).*

Proof: The case of finite extensions $K/\Bbbk$ is given in Exercise 20.5 of Cassels [122] or Propositions 1 and 2 of Chapter 10 of [542]. For a proof in the infinite case see Propositions 2 and 3 (Sections 2.6 and 2.7) of Chapter 5 of [124]. □

A.8 Finite Fields

Let p be a prime. Denote by $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the finite field of p elements. The multiplicative group of non-zero elements is $\mathbb{F}_p^*$. Recall that $\mathbb{F}_p^*$ is a cyclic group. A generator for $\mathbb{F}_q^*$ is called a **primitive root**. The number of primitive roots in $\mathbb{F}_q^*$ is $\varphi(q-1)$.

Theorem A.8.1. *Let p be a prime and $m \in \mathbb{N}$. Then there exists a field $\mathbb{F}_{p^m}$ having p^m elements. All such fields are isomorphic. Every finite field can be represented as $\mathbb{F}_p[x]/(F(x))$ where $F(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree m; the corresponding vector space basis $\{1, x, \ldots, x^{m-1}\}$ for $\mathbb{F}_{p^m}/\mathbb{F}_p$ is called a **polynomial basis**.*

Proof: See Corollary V.5.7 of [301] or Section 20.2 of [556]. □

If p is a prime and $q = p^m$ then $\mathbb{F}_{p^{nm}}$ may be viewed as a degree n algebraic extension of $\mathbb{F}_q$.

Theorem A.8.2. *Every finite field $\mathbb{F}_{p^m}$ has a vector space basis over $\mathbb{F}_p$ of the form $\{\theta, \theta^p, \ldots, \theta^{p^{m-1}}\}$; this is called a **normal basis**.*

Proof: See Theorem 2.35 or Theorem 3.73 of [388, 389] or Exercise 20.14 of [556] (the latter proof works for extensions of $\mathbb{F}_p$, but not for all fields). □

We discuss methods to construct a normal basis in Section 2.14.1.

Theorem A.8.3. *Let q be a prime power and $m \in \mathbb{N}$. Then $\mathbb{F}_{q^m}$ is an algebraic extension of $\mathbb{F}_q$ that is Galois. The Galois group is cyclic of order m and generated by the q-power Frobenius automorphism $\pi : x \mapsto x^q$.*

Let $\alpha \in \mathbb{F}_{q^m}$. The **trace** and **norm** with respect to $\mathbb{F}_{q^m}/\mathbb{F}_q$ are

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i} \quad \text{and} \quad \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \prod_{i=0}^{m-1} \alpha^{q^i}.$$

The **characteristic polynomial** over $\mathbb{F}_q$ of $\alpha \in \mathbb{F}_{q^m}$ is $F(x) = \prod_{i=0}^{m-1}(x - \alpha^{q^i}) \in \mathbb{F}_q[x]$. The trace and norm of $\alpha \in \mathbb{F}_{q^m}$ are (up to sign) the coefficients of x^{m-1} and x^0 in the characteristic polynomial.

An element $\alpha \in \mathbb{F}_q$ is a **square** or **quadratic residue** if the equation $x^2 = \alpha$ has a solution $x \in \mathbb{F}_q$. If g is a primitive root for $\mathbb{F}_q$ then g^a is a square if and only if a is even. Hence α is a square in $\mathbb{F}_q^*$ if and only if $\alpha^{(q-1)/2} = 1$.

[1] It is also necessary that ξ satisfy some topological requirements, but we do not explain these here.

Lemma A.8.4. *Let $g \in \mathbb{F}_{q^m}$, where $m > 1$, be chosen uniformly at random. The probability that g lies in a proper subfield $K \subset \mathbb{F}_{q^m}$ such that $\mathbb{F}_q \subseteq K$ is at most $1/q$.*

Proof: If $m = 2$ then the probability is $q/q^2 = 1/q$ so the result is tight in this case. When $m = l^i$ is a power of a prime $l \geq 2$ then all proper subfields of $\mathbb{F}_{q^m}$ that contain $\mathbb{F}_q$ are contained in $\mathbb{F}_{q^{l^{i-1}}}$ so the probability is $q^{l^{i-1}}/q^{l^i} = 1/q^{l^{i-1}(l-1)} \leq 1/q$. Finally, write $m = nl^i$ where $l \geq 2$ is prime, $i \geq 1$, $n \geq 2$ and $\gcd(n, l) = 1$. Then every proper subfield containing $\mathbb{F}_q$ lies in $\mathbb{F}_{q^{l^i}}$ or $\mathbb{F}_{q^{nl^{i-1}}}$. The probability that a random element lies in either of these fields is

$$\leq q^{l^i}/q^{nl^i} + q^{nl^{i-1}}/q^{nl^i} = 1/q^{l^i(n-1)} + 1/q^{nl^{i-1}(l-1)} \leq 1/q^2 + 1/q^2 \leq 1/q.$$

□

A.9 Ideals

If R is a commutative ring then an R-**ideal** is a subset $I \subset R$ that is an additive group and is such that for all $a \in I$ and $r \in R$ then $ar \in I$. An R-ideal I is proper if $I \neq R$ and is non-trivial if $I \neq \{0\}$. A **principal ideal** is $(a) = \{ar : r \in R\}$ for some $a \in R$. If $S \subset R$ then (S) is the R-ideal $\{\sum_{i=1}^n s_i r_i : n \in \mathbb{N}, s_i \in S, r_i \in R\}$. An ideal I is **finitely generated** if $I = (S)$ for a finite subset $S \subset R$. The **radical** of an ideal I in a ring R is $\mathrm{rad}_R(I) = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$ (see Definition VIII.2.5 and Theorem VIII.2.6 of Hungerford [301]). If I_1 and I_2 are ideals of R then

$$I_1 I_2 = \left\{ \sum_{i=1}^n a_i b_i : n \in \mathbb{N}, a_i \in I_1, b_i \in I_2 \right\}.$$

Note that $I_1 I_2 \subseteq I_1 \cap I_2$. For $a, b \in R$ one has $(ab) = (a)(b)$.

Let $I_1, \ldots, I_n$ be ideals in a ring R such that the ideal $(I_i \cup I_j) = R$ for all $1 \leq i < j \leq n$ (we call such ideals pairwise-coprime). If $a_1, \ldots, a_n \in R$ then there exists an element $a \in R$ such that $a \equiv a_i \pmod{I_i}$ (in other words, $a - a_i \in I_i$) for all $1 \leq i \leq n$. This is the **Chinese remainder theorem** for rings; see Theorem III.2.25 of [301] or Theorem II.2.1 of [367].

The following result gives three equivalent conditions for an ideal to be prime.

Lemma A.9.1. *Let I be an ideal of R. The following conditions are equivalent and, if they hold, I is called a* ***prime ideal****.*

1. *If $a, b \in R$ are such that $ab \in I$ then $a \in I$ or $b \in I$.*
2. *R/I is an integral domain (i.e., has no zero divisors).*
3. *If I_1 and I_2 are ideals of R such that $I_1 I_2 \subseteq I$ then $I_1 \subseteq I$ or $I_2 \subseteq I$.*

If $F(\underline{x}) \in \Bbbk[\underline{x}]$ is irreducible then the $\Bbbk[\underline{x}]$-ideal $(F(\underline{x})) = \{F(\underline{x})G(\underline{x}) : G(\underline{x}) \in \Bbbk[\underline{x}]\}$ is a prime ideal.

An R-ideal I is **maximal** if every R-ideal J such that $I \subseteq J \subseteq R$ is such that either $J = I$ or $J = R$.

Lemma A.9.2. *An R-ideal I is maximal if and only if R/I is a field (hence, a maximal R-ideal is prime). If I is a maximal R-ideal and $S \subset R$ is a subring then $I \cap S$ is a prime S-ideal.*

Proof: For the first statement see Theorem III.2.20 of [301] or Section II.2 of [367]. The second statement is proved as follows: Let I be maximal and consider the injection $S \to R$ inducing $S \to R/I$ with kernel $J = S \cap I$. Then $S/J \to R/I$ is is an injective ring homomorphism into a field, so J is a prime S-ideal. □

Let R be a commutative ring. A sequence $I_1 \subset I_2 \subset \cdots$ of R-ideals is called an **ascending chain**. A commutative ring R is **Noetherian** if every ascending chain of R-ideals is finite. Equivalently, a ring is Noetherian if every ideal is finitely generated. For more details see Section VIII.1 of [301] or Section X.1 of [367].

Theorem A.9.3. *(Hilbert basis theorem) If R is a Noetherian ring then $R[x]$ is a Noetherian ring.*

Proof: See Theorem 1 page 13 of [216], Theorem VIII.4.9 of [301] Section IV.4 of [367], or Theorem 7.5 of [15]. □

Corollary A.9.4. *$\Bbbk[x_1, \ldots, x_n]$ is Noetherian.*

A **multiplicative subset** of a ring R is a set S such that $1 \in S$, $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$. The **localisation** of a ring R with respect to a multiplicative subset S is the set

$$S^{-1}R = \{r/s : r \in R, s \in S\}$$

with the equivalence relation $r_1/s_1 \equiv r_2/s_2$ if $r_1 s_2 - r_2 s_1 = 0$. For more details see Chapter 3 of [15], Section 1.3 of [542], Section I.1 of [365], Section II.4 of [367] or Section III.4 of [301]. In the case $S = R^*$ we call $S^{-1}R$ the **field of fractions** of R. If $\mathfrak{p}$ is a prime ideal of R then $S = R - \mathfrak{p}$ is a multiplicative subset and the localisation $S^{-1}R$ is denote $R_{\mathfrak{p}}$.

Lemma A.9.5. *If R is Noetherian and S is a multiplicative subset of R then the localisation $S^{-1}R$ is Noetherian.*

Proof: See Proposition 7.3 of [15] or Proposition 1.6 of Section X.1 of [367]. □

A ring R is **local** if it has a unique maximal ideal. If $\mathfrak{m}$ is a maximal idea of a ring R then the localisation $R_{\mathfrak{m}}$ is a local ring. It follows that $R_{\mathfrak{m}}$ is Noetherian.

A.10 Vector Spaces and Linear Algebra

The results of this section are mainly used when we discuss lattices in Chapter 16. A good basic reference is Curtis [163].

Let $\Bbbk$ be a field. We write vectors in $\Bbbk^n$ as row vectors. We interchangeably use the words **points** and **vectors** for elements of $\Bbbk^n$. The zero vector is $\underline{0} = (0, \ldots, 0)$. For $1 \leq i \leq n$ the i-th unit vector is $\underline{e}_i = (e_{i,1}, \ldots, e_{i,n})$ such that $e_{i,i} = 1$ and $e_{i,j} = 0$ for $1 \leq j \leq n$ and $j \neq i$.

A **linear map** is a function $A : \Bbbk^n \to \Bbbk^m$ such that $A(\lambda \underline{x} + \mu \underline{y}) = \lambda A(\underline{x}) + \mu A(\underline{y})$ for all $\lambda, \mu \in \Bbbk$ and $\underline{x}, \underline{y} \in \Bbbk^n$. Given a basis for $\Bbbk^n$ any linear map can be represented as an $n \times m$ matrix A, such that $A(\underline{x}) = \underline{x}A$. We denote the entries of A by $A_{i,j}$ for $1 \leq i \leq n, 1 \leq j \leq m$. Denote by I_n the $n \times n$ **identity matrix**. We denote by A^T the **transpose**, which is an $m \times n$ matrix such that $(A^T)_{i,j} = A_{j,i}$. We have $(AB)^T = B^T A^T$.

A fundamental computational problem is to solve the linear system of equations $\underline{x}A = \underline{y}$ and it is well known that this can be done using Gaussian elimination (see Section 6 of Curtis [163] or Chapter 3 of Schrijver [531]).

The **rank** of an $m \times n$ matrix A (denoted $\mathrm{rank}(A)$) is the maximum number of linearly independent rows of A (equivalently, the maximum number of linearly independent

columns). If A is an $n \times n$ matrix then the **inverse** of A, if it exists, is the matrix such that $AA^{-1} = A^{-1}A = I_n$. If A and B are invertible then $(AB)^{-1} = B^{-1}A^{-1}$. One can compute A^{-1} using Gaussian elimination.

A.10.1 Inner Products and Norms

Definition A.10.1. The **inner product** of two vectors $\underline{v} = (v_1, \ldots, v_n)$ and $\underline{w} = (w_1, \ldots, w_n) \in \Bbbk^n$ is

$$\langle \underline{v}, \underline{w} \rangle = \sum_{i=1}^{n} v_i w_i.$$

The **Euclidean norm** or ℓ_2**-norm** of a vector $\underline{v} \in \mathbb{R}^n$ is

$$\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle}.$$

More generally for $\mathbb{R}^n$ one can define the ℓ_a**-norm** of a vector $\underline{v}$ for any $a \in \mathbb{N}$ as $\|\underline{v}\|_a = (\sum_{i=1}^n |v_i|^a)^{1/a}$. Important special cases are the ℓ_1-norm $\|\underline{v}_i\| = \sum_{i=1}^n |\underline{v}_i|$ and the ℓ_∞-norm $\|\underline{v}\|_\infty = \max\{|v_1|, \ldots, |v_n|\}$. (The reader should not confuse the notion of norm in Galois theory with the notion of norm on vector spaces.)

Lemma A.10.2. *Let $\underline{v} \in \mathbb{R}^n$. Then*

$$\|\underline{v}\|_\infty \leq \|\underline{v}\|_2 \leq \sqrt{n}\|\underline{v}\|_\infty \quad \text{and} \quad \|\underline{v}\|_\infty \leq \|\underline{v}\|_1 \leq n\|\underline{v}\|_\infty.$$

Lemma A.10.3. *Let $\underline{v}, \underline{w} \in \mathbb{R}^n$ and let $\|\underline{v}\|$ be the Euclidean norm.*

1. $\|\underline{v} + \underline{w}\| \leq \|\underline{v}\| + \|\underline{w}\|$.
2. $\langle \underline{v}, \underline{w} \rangle = \langle \underline{w}, \underline{v} \rangle$.
3. $\|\underline{v}\| = 0$ *implies* $\underline{v} = \underline{0}$.
4. $|\langle \underline{v}, \underline{w} \rangle| \leq \|\underline{v}\|\|\underline{w}\|$.
5. *Let A be an $n \times n$ matrix over $\mathbb{R}$. The following are equivalent:*
   (a) $\|\underline{x}A\| = \|\underline{x}\|$ *for all* $\underline{x} \in \mathbb{R}^n$;
   (b) $\langle \underline{x}A, \underline{y}A \rangle = \langle \underline{x}, \underline{y} \rangle$ *for all* $\underline{x}, \underline{y} \in \mathbb{R}^n$;
   (c) $AA^T = I_n$ *(which implies* $\det(A)^2 = 1$*).*

   Such a matrix is called an ***orthogonal matrix****.*

Definition A.10.4. A basis $\{v_1, \ldots, v_n\}$ for a vector space is **orthogonal** if

$$\langle v_i, v_j \rangle = 0$$

for all $1 \leq i < j \leq n$. If we also have the condition $\langle v_i, v_i \rangle = 1$ then the basis is called **orthonormal**.

Lemma A.10.5. *Let $\{\underline{v}_1, \ldots, \underline{v}_n\}$ be an orthogonal basis for $\mathbb{R}^n$. If $\underline{v} = \sum_{j=1}^n \lambda_j \underline{v}_j$ then $\|\underline{v}\|^2 = \sum_{j=1}^n \lambda_j^2 \|\underline{v}_j\|^2$.*

If one has an orthogonal basis $\{\underline{v}_1, \ldots, \underline{v}_n\}$ then it is extremely easy to decompose an arbitrary vector $\underline{w}$ over the basis. The representation is

$$\underline{w} = \sum_{i=1}^{n} \frac{\langle \underline{w}, \underline{v}_i \rangle}{\langle \underline{v}_i, \underline{v}_i \rangle} \underline{v}_i.$$

This is simpler and faster than solving the linear system using Gaussian elimination.

If $V \subseteq \mathbb{R}^n$ is a subspace then the **orthogonal complement** is $V^\perp = \{\underline{w} \in \mathbb{R}^n : \langle \underline{w}, \underline{v} \rangle = 0 \text{ for all } \underline{v} \in V\}$. The dimension of $V^\perp$ is $n - \dim(V)$. Given a basis $\{\underline{v}_1, \ldots, \underline{v}_m\}$ for V (where $m = \dim(V) < n$) one can compute a basis $\{\underline{v}_{m+1}, \ldots, \underline{v}_n\}$ for $V^\perp$. The **orthogonal projection** of $\mathbb{R}^n$ to a subspace V is a linear map $P : \mathbb{R}^n \to V$ that is the identity on V and is such that $P(V^\perp) = \{0\}$. In other words, if $\underline{v} \in \mathbb{R}^n$ then $\underline{v} - P(\underline{v}) \in V^\perp$.

A.10.2 Gram-Schmidt Orthogonalisation

Given a basis $\underline{v}_1, \ldots, \underline{v}_n$ for a vector space, the Gram-Schmidt algorithm iteratively computes an orthogonal basis $\underline{v}_1^*, \ldots, \underline{v}_n^*$ (called the **Gram-Schmidt orthogonalisation** or **GSO**). The idea is to set $\underline{v}_1^* = \underline{v}_1$ and then, for $2 \leq i \leq n$, to compute

$$\underline{v}_i^* = \underline{v}_i - \sum_{j=1}^{i-1} \mu_{i,j} \underline{v}_j^* \quad \text{where} \quad \mu_{i,j} = \frac{\langle \underline{v}_i, \underline{v}_j^* \rangle}{\langle \underline{v}_j^*, \underline{v}_j^* \rangle}.$$

We discuss this algorithm further in Section 17.3.

A.10.3 Determinants

Let $\underline{b}_1, \ldots, \underline{b}_n$ be n vectors in $\Bbbk^n$. One can define the **determinant** of the sequence $\underline{b}_1, \ldots, \underline{b}_n$ (or of the matrix B whose rows are $\underline{b}_1, \ldots, \underline{b}_n$) in the usual way (see Chapter 5 of Curtis [163] or Section VII.3 of Hungerford [301]).

Lemma A.10.6. *Let $\underline{b}_1, \ldots, \underline{b}_n \in \Bbbk^n$.*

1. *Let B be the matrix whose rows are $\underline{b}_1, \ldots, \underline{b}_n$. Then B is invertible if and only if $\det(\underline{b}_1, \ldots, \underline{b}_n) \neq 0$.*
2. *For $\lambda \in \Bbbk$, $\det(\underline{b}_1, \ldots, \underline{b}_{i-1}, \lambda \underline{b}_i, \underline{b}_{i+1}, \ldots, \underline{b}_n) = \lambda \det(\underline{b}_1, \ldots, \underline{b}_n)$.*
3. *$\det(\underline{b}_1, \ldots, \underline{b}_{i-1}, \underline{b}_i + \underline{b}_j, \underline{b}_{i+1}, \ldots, \underline{b}_n) = \det(\underline{b}_1, \ldots, \underline{b}_n)$ for $i \neq j$.*
4. *If $\{\underline{e}_1, \ldots, \underline{e}_n\}$ are the standard unit vectors in $\Bbbk^n$ then $\det(\underline{e}_1, \ldots, \underline{e}_n) = 1$.*
5. *If B_1, B_2 are square matrices then $\det(B_1 B_2) = \det(B_1) \det(B_2)$.*
6. *$\det(B) = \det(B^T)$.*
7. *(Hadamard inequality) $|\det(\underline{b}_1, \ldots, \underline{b}_n)| \leq \prod_{i=1}^{n} \|\underline{b}_i\|$ (where $\|\underline{b}\|$ is the Euclidean norm).*

Proof: See Theorems 16.6, 17.6, 17.15, 18.3 and 19.13 of Curtis [163]. □

Definition A.10.7. Let $\underline{b}_1, \ldots, \underline{b}_n$ be a set of vectors in $\mathbb{R}^n$. The **fundamental parallelepiped** of the set is

$$\left\{ \sum_{i=0}^{n} \lambda_i \underline{b}_i : 0 \leq \lambda_i < 1 \right\}.$$

Lemma A.10.8. *Let the notation be as above.*

1. *The volume of the fundamental parallelepiped of* $\{\underline{b}_1, \ldots, \underline{b}_n\}$ *is* $|\det(\underline{b}_1, \ldots, \underline{b}_n)|$.
2. $|\det(\underline{b}_1, \ldots, \underline{b}_n)| = \prod_{i=1}^{n} \|\underline{b}_i^*\|$ *where* $\underline{b}_i^*$ *are the Gram-Schmidt vectors.*

Proof: The first claim is Theorem 19.12 of Curtis [163]. The second claim is Exercise 19.11 (also see Theorem 19.13) of [163]. □

There are two methods to compute the determinant for vectors in $\mathbb{R}^n$. The first is to perform Gaussian elimination to diagonalise and then take the product of the diagonal elements. The second is to apply Gram-Schmidt (using floating point arithmetic) and then the determinant is just the product of the norms. Over $\mathbb{R}$ both methods only give an approximation to the determinant. To compute the determinant for vectors with entries in $\mathbb{Z}$ or $\mathbb{Q}$ one can use Gaussian elimination or Gram-Schmidt with exact arithmetic in $\mathbb{Q}$ (this gives an exact solution but suffers from coefficient explosion). Alternatively, one can compute the determinant modulo p_i for many small or medium sized primes p_i and use the Chinese remainder theorem.

A.11 Hermite Normal Form

Definition A.11.1. An $n \times m$ integer matrix $A = (A_{i,j})$ is in (row) **Hermite normal form** (**HNF**) if there is some integer $1 \leq r \leq n$ and a strictly increasing map $f : \{1, \ldots, n-r\} \to \{1, \ldots, m\}$ (i.e., $f(i+1) > f(i)$) such that

1. the last r rows of A are zero
2. $0 \leq A_{j,f(i)} < A_{i,f(i)}$ for $1 \leq j < i$ and $A_{j,f(i)} = 0$ for $i < j \leq n$.

In particular, an $n \times n$ matrix that is upper triangular and that satisfies the condition $0 \leq A_{j,i} < A_{i,i}$ for $1 \leq j < i \leq n$ is in Hermite normal form. The reader is warned that there are many variations on the definition of the Hermite normal form.

The HNF A' of an integer matrix A is unique and there is an $n \times n$ **unimodular matrix** U (i.e., U is a matrix with integer entries and determinant ± 1) such that $A' = UA$. For more details of the Hermite normal form see Section 2.4.2 of Cohen [136] or Section 4.1 of Schrijver [531] (though note that both books use columns rather than rows).

A.12 Orders in Quadratic Fields

A quadratic field is $\mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. If $d < 0$ then the field is called an **imaginary quadratic field**. The **discriminant** of $K = \mathbb{Q}(\sqrt{d})$ is $D = d$ if $d \equiv 1 \pmod 4$ or $D = 4d$ otherwise. The **ring of integers** of a quadratic field of discriminant D is is $\mathcal{O}_K = \mathbb{Z}[(D + \sqrt{D})/2]$.

An **order** in a field $\Bbbk$ containing $\mathbb{Q}$ is a subring R of $\Bbbk$ that is finitely generated as a $\mathbb{Z}$-module and is such that $R \otimes_{\mathbb{Z}} \mathbb{Q} = \Bbbk$. Every order in a quadratic field is of the form $\mathbb{Z}[c(D + \sqrt{D})/2]$ for some $c \in \mathbb{N}$. The integer c is called the **conductor** and the discriminant of the order is $c^2 D$.

A.13 Binary Strings

The binary representation of an integer $a = \sum_{i=0}^{l-1} a_i 2^i$ is written as

$$(a_{l-1} \ldots a_1 a_0)_2 \quad \text{or} \quad a_{l-1} \ldots a_1 a_0 \tag{A.1}$$

where $a_i \in \{0,1\}$ and $a_{l-1} = 1$. We say that the **bit-length** of a is l. An integer $a \in \mathbb{N}$ is represented by a binary string of bit-length $\lfloor \log_2(a) \rfloor + 1$. The **least significant bit** of a is $\mathrm{LSB}(a) = a_0 = a \pmod 2$. We call a_i the **i-th bit** or **bit** i of a. The "most significant bit" is trivially always one, but in certain contexts one uses different notions of MSB; for example see Definition 21.7.1.

Binary strings of length l are sequences $a_1 a_2 \ldots a_l$ with $a_i \in \{0,1\}$. Such a sequence is also called an **l-bit string**. The i-th bit is a_i. There is an ambiguity when one wants to interpret a binary string as an integer; our convention is that a_l is the least significant bit.[2]

We denote by $\{0,1\}^l$ the set of all length l binary strings and $\{0,1\}^*$ the set of all binary strings of arbitrary finite length. If a and b are binary strings then the exclusive-or (i.e., **XOR**) $a \oplus b$ is the binary string whose i-th bit is $a_i + b_i \pmod 2$ for $1 \leq i \leq l$.

A.14 Probability and Combinatorics

We briefly recall some ideas from probability. Good references are Ross [502], Woodroofe [636] and Chapter 6 of Shoup [556].

The number of ways to choose t items from n without replacement, and where the ordering matters, is $n(n-1)(n-2)\cdots(n-t+1) = n!/(n-t)!$. The number of ways to choose t items from n without replacement, and where the ordering does not matter, is $\binom{n}{t} = n!/(t!(n-t)!)$. The number of ways to choose t items from n with replacement and where the ordering doesn't matter is $\binom{n+t-1}{t-1}$. We have

$$\left(\frac{n}{m}\right)^m \leq \binom{n}{m} \leq \left(\frac{ne}{m}\right)^m$$

Stirling's approximation to the factorial is $n! \approx \sqrt{2\pi n} e^{-n} n^n$ or $\log(n!) \approx n(\log(n) - 1)$ (where log denotes the natural logarithm). For proof see Section 5.4.1 of [636].

Let $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. A **distribution** on a set S is a function Pr mapping "nice"[3] subsets of S to $[0,1]$, with the properties that $\Pr(\varnothing) = 0$, $\Pr(S) = 1$ and if $A, B \subseteq S$ are disjoint and "nice" then $\Pr(A \cup B) = \Pr(A) + \Pr(B)$. For $s \in S$ we define $\Pr(s) = \Pr(\{s\})$ if $\{s\}$ is "nice". The **uniform distribution** on a finite set S is given by $\Pr(s) = 1/\#S$.

An **event** is a "nice" subset $E \subseteq S$, and $\Pr(E)$ is called the probability of the event. We define $\neg E$ to be $S - E$, so that $\Pr(\neg E) = 1 - \Pr(E)$. We have $\Pr(E_1) \leq \Pr(E_1 \cup E_2) \leq \Pr(E_1) + \Pr(E_2)$. We define $\Pr(E_1 \text{ and } E_2) = \Pr(E_1 \cap E_2)$.

Let S be a finite set with an implicit distribution on it (usually the uniform distribution). In an algorithm we write $s \leftarrow S$ to mean that $s \in S$ is randomly selected from S according to the distribution, i.e., s is chosen with probability $\Pr(s)$.

If $A, E \subseteq S$ and $\Pr(E) > 0$ then the **conditional probability** is

$$\Pr(A \mid E) = \frac{\Pr(A \cap E)}{\Pr(E)}.$$

If $\Pr(A \cap E) = \Pr(A)\Pr(E)$ then A and E are **independent events** (equivalently, if $\Pr(E) > 0$ then $\Pr(A \mid E) = \Pr(A)$). If S is the disjoint union $E_1 \cup E_2 \cup \cdots \cup E_n$ then $\Pr(A) = \sum_{i=1}^n \Pr(A \mid E_i)\Pr(E_i)$.

[2] This means that the i-th bit of a binary string is not the i-th bit of the corresponding integer. This inconsistency will not cause confusion in the book.

[3] Technically, S must be a set with a measure and the "nice" subsets are the measurable ones. When S is finite or countable then every subset is "nice".

Let S be a set. A **random variable** is a function[4] $X : S \to \mathbb{R}$. Write $\mathcal{X} \subseteq \mathbb{R}$ for the image of X (our applications will always have $\mathcal{X}$ either finite or $\mathbb{N}$). Then X induces a distribution on $\mathcal{X}$, defined for $x \in \mathcal{X}$ by $\Pr(X = x)$ is the measure of $X^{-1}(\{x\})$ (in the case where S is finite or countable, $\Pr(X = x) = \sum_{s \in X^{-1}(x)} \Pr(s)$). Random variables X_1 and X_2 are **independent random variables** if $\Pr(X_1 = x_1 \text{ and } X_2 = x_2) = \Pr(X_1 = x_1) \Pr(X_2 = x_2)$ for all $x_1 \in \mathcal{X}_1$ and $x_2 \in \mathcal{X}_2$.

The **expectation** of a random variable X taking values in a finite or countable set $\mathcal{X} \subseteq \mathbb{R}$ is

$$E(X) = \sum_{x \in \mathcal{X}} x \Pr(X = x).$$

If $\mathcal{X} = \mathbb{N}$ then $E(X) = \sum_{n=0}^{\infty} \Pr(X > n)$ (this is shown in the proof of Theorem 14.1.1). Note that if $\mathcal{X}$ is finite then $E(X)$ exists, but for $\mathcal{X}$ countable then the expectation only exists if the sum is convergent. If X_1 and X_2 are random variables on S then $E(X_1 + X_2) = E(X_1) + E(X_2)$. If X_1 and X_2 are independent then $E(X_1 X_2) = E(X_1)E(X_2)$.

Example A.14.1. Consider flipping a coin, with probability p of "heads" and probability $1 - p$ of "tails" (where $0 < p < 1$). Assume the coin flips are independent events. What is the expected number of trials until the coin lands "heads"?

Let X be the random variable with values in $\mathbb{N}$ where $\Pr(X = n)$ is the probability that the first head is on the n-th throw. Then $\Pr(X > n) = (1 - p)^n$ and $\Pr(X = n) = (1 - p)^{n-1}p$. This gives the **geometric distribution** on $\mathbb{N}$. One can check that $\sum_{n=1}^{\infty} \Pr(X = n) = 1$.

The expectation of X is $E(X) = \sum_{n=1}^{\infty} n \Pr(X = n)$ (the ratio test shows that this sum is absolutely convergent). Write $T = \sum_{n=1}^{\infty} n(1 - p)^{n-1}$. Then

$$E(X) = pT = T - (1-p)T = \sum_{n=1}^{\infty} n(1-p)^{n-1} - \sum_{n=1}^{\infty} (n-1)(1-p)^{n-1} = 1 + \sum_{n=2}^{\infty} (1-p)^{n-1} = \frac{1}{p}.$$

To define this problem formally, one should define the geometric random variable $X : S \to \mathbb{N}$, where S is the (uncountable) set of countable length sequences of bits, such that $X(s_1 s_2 \dots) > n$ if and only if $s_1 = \cdots s_n =$ "tails". This leads to measure-theoretic technicalities that are beyond the scope of this book, but which are well understood in probability theory.

Example A.14.2. Suppose one has a set S of N items and one chooses elements of S (with replacement) uniformly and independently at random. Let X be a random variable taking values in $\mathbb{N}$ such that $\Pr(X = n)$ is the probability that, after sampling n elements from S, the first $n - 1$ elements are distinct and the n-th element is equal to one of the previously sampled elements. In other words, X is the number of samples from S until some element is sampled twice. A version of the **birthday paradox** states that the expected value of X is approximately $\sqrt{\pi N/2}$. We discuss this in detail in Section 14.1.

Example A.14.3. A version of the **coupon collector** problem is the following: Suppose S is a set of N items and one chooses elements of S (with replacement) uniformly at random.

Let X be a random variable taking values in $\mathbb{N}$ such that $\Pr(X \geq n)$ is the probability that after choosing $n - 1$ elements (sampled uniformly and independently at random from S) one has not yet chosen some element of S. In other words, X is the number of "coupons" to be collected until one has a full set of all N types. The expected value of X is $N(1 + 1/2 + \cdots + 1/(N - 1) + 1/N) \approx N \log(N)$ (see Example 7.2j of Ross [502]).

[4]Technically, a random variable is defined on a probability space, not an arbitrary set, and is a measurable function; we refer to Woodroofe [636] for the details.

The **statistical distance** (also called the **total variation**) of two distributions $\Pr_1$ and $\Pr_2$ on a finite or countable set S is $\Delta(\Pr_1, \Pr_2) = \frac{1}{2}\sum_{x \in S} |\Pr_1(s) - \Pr_2(s)|$. It is easy to see that $\Delta(\Pr_1, \Pr_1) = 0$ and $0 \leq \Delta(\Pr_1, \Pr_2) \leq 1$ (see Theorem 6.14 of Shoup [556]). Two distributions are **statistically close** if their statistical distance is "negligible" in some appropriate sense (typically, in cryptographic applications, this will mean "negligible in terms of the security parameter").

We end with a result that is often used in the analysis of algorithms.

Theorem A.14.4. *The probability that two uniformly and independently chosen integers* $1 \leq n_1, n_2 < N$ *satisfy* $\gcd(n_1, n_2) = 1$ *tends to* $1/\zeta(2) = 6/\pi^2 \approx 0.608$ *as* N *tends to infinity.*

Proof: See Theorem 332 of [276]. □

Appendix B

Hints and Solutions to Exercises

Chapter 1: Introduction

1.3.3: Encryption is deterministic so one can compare the challenge ciphertext c with $\mathsf{m}_0^e \pmod N$.

1.3.4: Given c, submit $\mathsf{c}' = \mathsf{c}2^e \pmod N$ to the decryption oracle to get $2\mathsf{m} \pmod N$ and hence compute m.

1.3.5: If it does not have semantic security there is some function $f : \mathsf{M}_\kappa \to \{0,1\}$ which can be computed given a ciphertext, so choose messages $\mathsf{m}_0, \mathsf{m}_1$ such that $f(\mathsf{m}_i) = i$ and then one can break IND security.

1.3.7: A UF-CMA adversary is a randomised polynomial-time algorithm which takes as input a public key pk for a signature scheme, is allowed to query a signing oracle on messages of its choice, and outputs a message m and a signature s. The adversary wins if the signature s satisfies the verification algorithm on message m and key pk and if m was not one of the queries to the signing oracle. A scheme has UF-CMA security if every adversary succeeds with only negligible probability (in the security parameter). See Definition 12.2 of Katz and Lindell [334].

1.3.8: Yes, if the RSA problem is hard.

1.3.9: Choose random s and set $\mathsf{m} = \mathsf{s}^e \pmod N$.

1.3.10: Given m call signing oracle on $2^e\mathsf{m} \pmod N$ to get s'. Output $\mathsf{s} = \mathsf{s}'2^{-1} \pmod N$.

Chapter 2: Basic Algorithms

2.2.3: See Section 9.5.1 of Crandall and Pomerance [162], Section 3.5 of Shoup [556] or Section 8.1 of von zur Gathen and Gerhard [238].

2.2.8: See Section 9.2.2 of [162], Sections 1.5.1 and 1.5.2 of Brent and Zimmermann [100] or Section 1.7.1 of Cohen [136]. The complexity is $O(M(\log(a)))$,

2.2.9: Since $e \leq \log_2(N)$ the idea is to compute $N^{1/e}$ for $e = 1, 2, \ldots, \lfloor \log_2(N) \rfloor$ to find the largest e such that $N^{1/e} \in \mathbb{N}$.

2.4.4: See Section 5.9 of Bach and Shallit [22] or Algorithm 2.3.5 of Crandall and Pomerance [162].

2.4.5: Show the algorithm is faster than computing $\gcd(m, n)$ using Euclid; the fundamental step is computing m mod n but the numbers are always at most as large as those in Euclid's algorithm.

2.4.6: Choose random $1 < a < p$ and compute $(\frac{a}{p})$ until the Legendre symbol is -1. Since the probability of success is at least 0.5 for each trial, the expected number of trials is 2. This is a Las Vegas algorithm (it may never terminate, but the answer is always correct). See the proof of Lemma 2.9.5 for further details.

2.4.9: This goes back to A. Cobham. See Shoup [557] or Bach and Sorensen [23] for the analysis.

2.4.10: Computing Legendre symbols using quadratic reciprocity requires $O(\log(p)^2)$ bit operations while computing $a^{(p-1)/2} \pmod p$ needs $O(\log(p)M(\log(p)))$ bit operations (see Corollary 2.8.4). So using quadratic reciprocity is (theoretically) always better.

2.5.5: First compute and store $b_2, \ldots, b_m$ where $b_i = \prod_{j=1}^{i} a_j$, then b_m^{-1}, then, for $i = m$ downto 2 compute $a_i^{-1} = b_{i-1}b_i^{-1}, b_{i-1}^{-1} = a_i b_i^{-1}$. See Algorithm 11.15 of [16], Section 2.4.1 of [100] or Section 2.2.5 of [274].

2.6.4:

2.8.6: For pseudocode of the algorithm see Algorithm IV.4 of [64] or Algorithm 9.10 of [16].

2.8.7: Consider a window of length w representing an odd integer. If the bits of m are uniformly distributed then the probability the next most significant bit after the window is 0 is 0.5. Hence the expected number of zeroes before the first 1 is $0.5 \cdot 0 + 0.25 \cdot 1 + 0.125 \cdot 2 + \cdots = \sum_{i=1}^{\infty} i/2^{i+1} = 1$.

2.8.10: For pseudocode see Section 2.2 of Möller [432]. The problem is that there is no fixed precomputation of powers of g.

2.8.11: The values m_i in addition chain satisfy $m_i \leq 2^i$.

2.9.8: See Adleman, Manders and Miller [3].

2.10.2: See Chapters 2 and 3 of von zur Gathen and Gerhard [238].

2.10.4: Assume that $F(0) \neq 0$ so that x is coprime to $F(x)$. Replace $R = 2^k$ in the description of Montgomery reduction in Section 2.5 by $R = x^d \pmod{F(x)}$. See Koç and Acar [349] for details and discussion.

2.10.5: See Section 9.6.3 of [162].

2.12.1: Compute $F'(x)$. If $F'(x) = 0$ then, by Lemma A.5.2, $F(x) = G(x)^p$ where $p = \mathrm{char}\mathbb{F}_q$, and $F(x)$ is not square-free. Otherwise, compute $\gcd(F(x), F'(x))$ and if this is not 1 then $F(x)$ is not square-free. The computation requires $O(\deg(F)^2)$ field operations.

2.12.2: Given $F(x) \in \mathbb{F}_q[x]$ compute $F'(x)$. If $F'(x) = 0$ then $F(x) = G(x)^p$ and repeat process on $G(x)$. Otherwise, compute $F_1(x) = F(x)/\gcd(F(x), F'(x))$ and factor $F_1(x)$. Once the factors of $F_1(x)$ are known then one can factor $F(x)/F_1(x)$ efficiently by testing divisibility by the known factors of $F_1(x)$.

2.12.3: One computes $x^q \pmod{F(x)}$ in $O(\log(q)d^2)$ field operations and a further $O(d^2)$ operations are needed for the gcd computation. The answer to the decision problem is "yes" if and only if $\deg(R_1(x)) > 0$.

2.12.5: One is essentially doing "divide and conquer" to separate the $\deg(R_1(x)) \leq d$ roots. Each trial is expected to split $R_1(x)$ into two polynomials of degree $\approx \deg(R_1(x))/2$. Hence, an expected $O(\log_2(\deg(R_1(x)))) = O(\log_2(d))$ trials are required to factor $R_1(x)$. Since each trial involves computing $u(x)^{(q-1)/2} \pmod{R_1(x)}$ (which has complexity $O(\log(q)M(d))$ operations in $\mathbb{F}_q$) and then computing the gcd of polynomials of degree $\leq d$ (which requires $O(d^2)$ operations in $\mathbb{F}_q$) the total expected cost is $O(\log(q)\log(d)d^2)$ field operations. For a detailed analysis of the probabilities see Section 21.3.2 of Shoup [556].

2.12.10: If $F(x)$ is not irreducible then it has a factor of degree $\leq \deg(F(x))/2$. Hence it is sufficient that $\gcd(F(x), x^{q^i} - x) = 1$ for $1 \leq i \leq d/2$. To compute all these polynomials efficiently one computes $s_1(x) \equiv x^q \pmod{F(x)}$ and then $\gcd(F(x), s_1(x) - x)$. For the next step compute $s_2(x) = s_1(x)^q \pmod{F(x)}$ and $\gcd(F(x), s_2(x) - x)$,

and so on. There are $d/2$ steps, each taking $O(\log(q)d^2)$ field operations, so the overall complexity is $O(d^3 \log(q))$. See Algorithm IPT of Section 21.1 of [556] or Section 3 of [370].

2.12.11: One first computes $\gcd(x^{q^b} - x, F(x))$ in time $O(b \log(q))$ operations on polynomials of degree at most d. The rest of the algorithm is the same as the root finding algorithm of Exercise 2.12.5 where we raise polynomials to at most the power q^b.

2.14.1: Construct $\{\theta, \theta^q, \ldots, \theta^{q^{m-1}}\}$ in $O(m^3)$ operations in $\mathbb{F}_q$ (using the fact that q-th powering is linear) and then $O(m^3)$ operations in $\mathbb{F}_q$ for the Gaussian elimination. Hence the complexity is an expected $O(m^3 \log_q(m))$ bit operations.

2.14.4: Suppose $\theta^2 = d$. Given $g = g_0 + g_1\theta$ we must solve for $x, y \in \mathbb{F}_q$ such that $(x + \theta y)^2 = g_0 + g_1\theta$. Expanding gives $x^2 + dy^2 = g_0$ and $2xy = g_1$ and one can eliminate y to get $4x^4 - 4g_0x^2 + dg_1^2 = 0$ which can be solved using two square roots in $\mathbb{F}_q$.

2.14.5: See Fong-Hankerson-López-Menezes [207].

2.14.10: Computing S_m requires $O(m^3)$ operations in $\mathbb{F}_q$. Computing a linear dependence among m vectors can be done using Gaussian elimination in $O(m^3)$ field operations.

2.14.11: Since $1 - 1/q \geq 1/2$ the number of trials is at most 2. The complexity is therefore an expected $O(m^3)$ operations in $\mathbb{F}_q$.

2.14.12: Expected $O(m^3)$ operations in $\mathbb{F}_{q^m}$.

2.14.13: The cost of finding a root of the polynomial $F_1(x)$ of degree m is an expected $O(\log(m)\log(q)m^2)$ operations in $\mathbb{F}_q$ and this dominates the cost of the isomorphism algorithm in the forwards direction. The cost of the linear algebra to compute the inverse to this isomorphism is $O(m^3)$. (If one repeats the algorithm with the roles of F_1 and F_2 swapped then one gets a field isomorphism from $\mathbb{F}_q[y]/(F_2(y))$ to $\mathbb{F}_q[x]/(F_1(x))$ but it is not necessarily the inverse of the function computed in the first step.

2.15.1: Writing $q - 1 = \prod_{i=1}^{m} l_i^{e_i}$ we have $m = O(\log(q))$ and then computing $g^{(q-1)/l_i}$ requires $O(\log(q)^3)$ bit operations.

2.15.8: The naive solution requires $\approx 2/3 \log_2(N)$ group operations in the precomputation, followed by $\approx 3\frac{1}{2} \log_2(N^{2/3}) = \log_2(N)$ group operations. The same trick can be used in the first stage of Algorithm 4, giving $\approx \frac{2}{3} \log_2(N)$ group operations. But the three exponentiations in the second stage are all to different bases and so the total work is $\approx \frac{3}{2} \log_2(N)$ group operations. The naive solution is therefore better. The naive method becomes even faster compared with Algorithm 4 if one uses window methods.

Chapter 5: Varieties

5.1.3: $V(y - x^2), V(y^2 - x), V((x-1)^3 - y^2)$.

5.1.4: If $f(x, y)$ has no monomials featuring y then it is a polynomial in x only; take any root $a \in \overline{\mathbb{k}}$ and then $\{(a, b) : b \in \overline{\mathbb{k}}\} \subseteq V(f)$. For the remaining case, for each $a \in \overline{\mathbb{k}}$ then $f(a, y)$ is a polynomial in y and so has at least one root $b \in \overline{\mathbb{k}}$.

5.1.7: Let $z = x + iy \in \mathbb{F}_{p^2}$. Then $z^p = x - iy$. Hence $z^{p+1} = 1$ if and only if $1 = (x + iy)(x - iy) = x^2 + y^2$. If follows that the map $x + iy \mapsto (x, y)$ is a bijection from G to $X(\mathbb{F}_p)$. Showing that this is a group isomorphism is straightforward.

5.1.10: In $X = \mathbb{A}^1(\mathbb{F}_p)$ we have $X = V(x^p - x)$.

5.2.8: $V(x^2 + y^2 - z^2)(\mathbb{R})$ is the same as the circle $V(x^2 + y^2 - 1)(\mathbb{R}) \subseteq \mathbb{A}^2(\mathbb{R})$. Over $\mathbb{C}$ it would also contain the points $(1 : \pm i : 0)$.

$V(yz - x^2)$ is the parabola $y = x^2$ in $\mathbb{A}^2$ together with the single point $(0 : 1 : 0)$ at infinity. Note that this algebraic set is exactly the same as the one in Example 5.2.7 under a change of coordinates.

5.2.21: $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$.

5.2.35: We have $\overline{X} = V(f(x_0, x_1, x_2)) = V(\overline{f})$. A point in $\overline{X} - X$ has $x_2 = 0$ and at least one of $x_0, x_1 \neq 0$. Hence, the points at infinity are in the union of $(\overline{X} \cap U_0) \cap V(x_2) = \{(1 : y : 0) : f(1, y, 0) = 0\}$ and $(\overline{X} \cap U_1) \cap V(x_2) = \{(x : 1 : 0) : f(x, 1, 0) = 0\}$. Both sets are finite.

5.3.3: It decomposes as $V(x, z) \cup V(w - x, x^2 - yz)$ and one can see that neither of these sets is equal to X.

5.3.5: $k[x, y]/(y - x^2) \cong k[x]$ is an integral domain, so $(y - x^2)$ is prime.

5.3.6: If $gh \in I_{\Bbbk}(X)$ then $g(f_1(t), \ldots, f_n(t))h(f_1(t), \ldots, f_n(t))$ is a polynomial in t which is identically zero on $\overline{\Bbbk}$. The result follows. See Proposition 5 of Section 4.5 of Cox, Little and O'Shea [158] for details and a generalisation.

5.3.14: If $U_1 \cap U_2 = \varnothing$ then $X = (X - U_1) \cup (X - U_2)$ is a union of proper closed sets.

5.4.6: We show that $(f_1/f_2)(P) - (f_3/f_4)(P) = 0$. By assumption $f_2(P), f_4(P) \neq 0$ and so it suffices to show $(f_1 f_4 - f_2 f_3)(P) = 0$. This follows since $(f_1 f_4 - f_2 f_3) \in I_{\Bbbk}(X)$.

5.5.7: Recall from Exercise 5.3.14 that $U_1 \cap U_2 \neq \varnothing$. Then apply the same arguments as in the proof of Theorem 5.4.8.

5.5.9: The solution is not unique. An example of maps $\phi : X \to Y$ and $\psi : Y \to X$ is $\phi(x, y) = (x : 1 : 1)$ and $\psi(x_0 : x_1 : x_2) = (x_0/x_1, x_1/x_0)$. One can check that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity when they are defined.

5.5.14: The line of slope t through $(-1, 0)$ has equation $y = t(x + 1)$ and hits X and $(-1, 0)$ and a point $\phi(t) = (x(t), y(t)) = ((1 - t^2)/(1 + t^2), 2t/(1 + t^2))$. Hence, define $\phi : \mathbb{P}^1 \to X$ by $f([t : u]) = ((u^2 - t^2)/(u^2 + t^2), 2ut/(u^2 + t^2))$. The inverse morphism $\psi : X \to \mathbb{P}^1$ is $\psi(x, y) = (y : x + 1) = (x - 1 : y)$; note that these two descriptions of ψ are equivalent (multiply the former through by $y/(x + 1)$) and that the former is regular away from $(-1 : 0)$ and the latter regular away from $(1 : 0)$. Since the slope of the line between (-1.0) and (x, y) is $y/(x + 1)$ it follows that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity.

5.5.19: Write Z for the Zariski closure of $\phi(X)$ in Y. If $Z = Z_1 \cup Z_2$ is a union of closed sets then $X = \phi^{-1}(Z_1) \cup \phi^{-1}(Z_2)$ is also a union of closed sets so, without loss of generality, $\phi^{-1}(Z_1) = X$ and so Z_1 contains the Zariski closure of $\phi(X)$.

5.5.26: Suppose $\theta(f) = 0$ for some $f \in K_1^*$. Then $ff^{-1} = 1$ and so $1 = \theta(1) = \theta(f)\theta(f^{-1}) = 0$ which is a contradiction.

5.6.5: A proof is given in Proposition 1.13 of Hartshorne [278]. We also give a proof here: Let $f \in \Bbbk[x_1, \ldots, x_n]$. Without loss of generality suppose f contains at least one monomial featuring x_n. Then write $f = f_r x_n^r + f_{r-1} x_n^{r-1} + \cdots + f_0$ with $f_i \in \Bbbk[x_1, \ldots, x_{n-1}]$ or $\Bbbk[x_0, \ldots, x_{n-1}]$. One can check that the field $\Bbbk(X)$ contains a subfield isomorphic to $\Bbbk(x_1, \ldots, x_{n-1})$. Finally, $\Bbbk(X)$ is an algebraic extension of $\Bbbk(x_1, \ldots, x_n)$.

5.6.6: $\overline{\Bbbk}(X) = \overline{\Bbbk}[X] = \overline{\Bbbk}$ and so $I_{\overline{\Bbbk}}(X)$ is a maximal ideal and so by the Nullstellensatz $X = \{P\}$.

5.6.10: Let X be a variety of dimension 1 and let Y be a proper closed subset. Let $Y = \cup_{i=1}^n Y_i$ be the decomposition of Y into irreducible components. By Corollary 5.6.9 we have $\dim(Y_i) = 0$. Exercise 5.6.6 implies $\#Y_i(\overline{\Bbbk}) = 1$ and so $\#Y(\overline{\Bbbk}) = n$.

5.7.5: $V(y_1^2 - y_2^2, y_1 y_2 - 1)$.

5.7.6: $V(y_{1,1}^2 - y_{1,2}^2 + y_{2,1}^2 - y_{2,2}^2 - 1, y_{1,1} y_{1,2} + y_{2,1} y_{2,2} - 1)$.

Chapter 6: Tori, LUC and XTR

6.1.4: If $p \nmid n$ then

$$\Phi_{np}(x) = \prod_{d|n} \left((x^{np/d} - 1)^{\mu(d)} (x^{n/d} - 1)^{\mu(dp)} \right)$$

and use $\mu(dp) = -\mu(d)$. If $p \mid n$ then

$$\Phi_{np}(x) = \left(\prod_{d|n}(x^{np/d}-1)^{\mu(d)}\right)\left(\prod_{d|np, d\nmid n}(x^{np/d}-1)^{\mu(d)}\right).$$

and note that if $d \mid np$ but $d \nmid n$ then $p^2 \mid d$ and so $\mu(d) = 0$. The final statement follows since, when n is odd, $z^n = 1$ if and only if $(-z)^{2n} = 1$.

6.3.2: To compute $(u+v\theta)(u'+v'\theta)$ compute uu', vv' and $(u+v)(u'+v')$. To square $(u+v\theta)$ compute u^2, v^2 and $(u+v)^2$. One inverts $(u+v\theta)$ by computing $(u+v\overline{\theta})/(u^2 - Auv + Bv^2)$.

6.3.3: The first two parts are similar to Exercise 6.3.2. For inversion, note that $(u+v\theta)^{-1} = (u-v\theta)/(u^2+v^2)$. For square roots, note that $(u+v\theta)^2 = (u^2-v^2)+2uv\theta$ so to compute the square root of $a+b\theta$ requires solving these equations. We assume here that $a+b\theta$ is a square, and so $(\frac{a^2+b^2}{q}) = 1$. One finds that $u^4 - au^2 - b^2/4 = 0$ and so $u^2 = (a \pm \sqrt{a^2+b^2})2^{-1}$. Only one of the two choices is a square, so one must compute the Legendre symbol $(\frac{a+\sqrt{a^2+b^2}}{q})$ to determine the answer (taking into account that $(\frac{2}{q})$ is known from $q \pmod 8$). One then multiplies the appropriate $(a \pm \sqrt{a^2+b^2})$ by 2^{-1}, which is easy (either shift right or add q and shift right). Taking the square root gives u. An inversion and multiplication gives v.

6.3.15: See Williams [634].

6.3.17: The characteristic polynomial of g is $(x-g)(x-g^q) = x^2 - \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)x + 1$ so $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g')$ implies g' is a root of the same polynomial as g.

6.3.22: 34.

6.3.23: Exercises 6.3.2 and 6.3.3 give costs of 3 squarings in $\mathbb{F}_q$ for computing a squaring in $\mathbb{F}_{q^2}$ and 3 squarings plus 3 multiplications in $\mathbb{F}_q$ for a square-and-multiply. Lucas sequences give just one multiplication and squaring for each operation; only one third the number of operations in the worst case.

6.4.5: Need $q \equiv 2 \pmod 3$ or else $\zeta_3 \in \mathbb{F}_q$. Also need $q^2 \not\equiv 1 \pmod 9$ or else $\zeta_9 \in \mathbb{F}_{q^2}$.

6.4.7: Consider $0 = f(a)^q = a^{3q} - t^q a^{2q} + t^{q^2} a^q - 1 = (-1 + t^q a^{-q} - t a^{-2q} + a^{-3q})(-a^{3q})$. This shows that $f(a^{-q}) = 0$. Now, suppose $f(x)$ is neither irreducible nor split completely. Then $f(x) = (x-u)g(x)$ where $u \in \mathbb{F}_{q^2}$ and $g(x)$ is an irreducible quadratic over $\mathbb{F}_{q^2}$. Let $a \in \mathbb{F}_{q^4} - \mathbb{F}_{q^2}$ be a root of $g(x)$. Then a^{-q} is the other root, but then $(a^{-q})^{-q} = a^{q^2} = a$ and we have $a \in \mathbb{F}_{q^2}$.

6.4.10: See Lenstra and Verheul [375].

6.4.11: Squaring requires computing $(t_{2n+1}, t_{2n}, t_{2n-1})$ which is one iteration of each formula in the previous exercise. Square-and-multiply requires computing $(t_{2n+2}, t_{2n+1}, t_{2n})$ which is twice formula 2 and once formula 3 above. Let M (respectively S, P) be the costs of a multiplication (respectively, squaring, q-th powering) in $\mathbb{F}_{q^2}$. Then a squaring (i.e., going from t_n to t_{2n}) requires $4M + S + 5P$ while a square-and-multiply requires $2M + 2S + 4P$. The reader is warned that in practice it is often more efficient to use other ladder algorithms than traditional square-and-multiply, see Chapter 3 of Stam [579].

6.4.12: The trick is to represent t_n using the triple (t_{n+1}, t_n, t_{n-1}) as above when n is odd, but (t_{n+2}, t_{n+1}, t_n) when n is even. One then must use formula 1 of Exercise 6.4.10. For example, if n is even and one is computing $(t_{2n+2}, t_{2n+1}, t_{2n})$ then the middle term is computed as $t_{2(n+1)-1}$. See Lenstra and Verheul [375] for details.

6.4.13: $t_6 = 7 + 48i, t_7 = 35 + 65i, t_8 = 6 + 8i$.

6.4.14: One can represent the equivalence class of g^n by (t_n, t_{-n}). For the ladder one can store the 6-tuple $(t_{n+1}, t_n, t_{n-1}, t_{-n-1}, t_{-n}, t_{-n+1})$ and compute an analogous 6-tuple

centered at (t_{2n}, t_{-2n}) or (t_{2n+1}, t_{-2n-1}). See Gong and Harn [259] and also Stam [579] for further details.

6.4.15: See Shirase et al [551].

6.6.2: Modulo each prime p_i there are usually two values h such that $\mathrm{Tr}_{\mathbb{F}_{p_i^2}/\mathbb{F}_{p_i}}(h) = \mathrm{Tr}_{\mathbb{F}_{p_i^2}/\mathbb{F}_{p_i}}(g)$. Hence, by the Chinese remainder theorem, there are 2^k values for h in general.

The second claim follows immediately, or one can prove it using the same argument as the first part: modulo each prime p_i, $2 + (p_i - 1)/2 \approx p_i/2$ values arise as the trace of an element in $G_{p_i,2}$.

Chapter 7: Curves and Divisor Class Groups

7.1.7: The first claim is immediate, since $f \in \mathcal{O}_P$ implies $f(P) \in \Bbbk$ is defined, and $(f - f(P)) \in \mathfrak{m}_P$. For the second claim, note that $\mathfrak{m}_P/\mathfrak{m}_P^2$ is an $\mathcal{O}_P/\mathfrak{m}_P$-module, i.e., a $\Bbbk$-vector space. Without loss of generality, $P = (0, \ldots, 0)$. and $\mathfrak{m}_P$ is the $\mathcal{O}_P$-ideal $(x_1, \ldots, x_n)$. Then every monomial $x_i x_j$ for $1 \leq i, j \leq n$ lies in $\mathfrak{m}_P^2$. Therefore every element of $\mathfrak{m}_P$ is of the form $a_1 x_1 + \cdots a_n x_n + g$ where $a_i \in \Bbbk$ for $1 \leq i \leq n$ and $g \in \mathfrak{m}_P^2$. Hence there is a map $d : \mathfrak{m}_P \to \Bbbk^n$ given by

$$d(a_1 x_1 + \cdots + a_n x_n + g) = (a_1, \ldots, a_n).$$

7.1.9: $x = y^2 - yx - x^4 \in \mathfrak{m}_P^2$ so $\{y\}$ is a basis. For the second example there is no linear relation between x and y and so $\{x, y\}$ is a basis.

7.1.15: Corollary 7.1.14: By Exercise 5.6.5 the dimension of X is $d = n - 1$, so $n - d = 1$. Now, the Jacobian matrix is a single row vector and so the rank is 1 unless the vector is the zero vector. Corollary 7.1.14 is just a restatement of this.

7.2.4: Putting $z = 0$ gives the equation $x^3 = 0$ and so $x = 0$. Hence, $(0 : 1 : 0)$ is the only point at infinity. Taking the affine part by setting $y = 1$ gives the equation $E(x, z) = z + a_1 xz + a_3 z^2 - (x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3)$ and one can check that $(\partial E/\partial z)(0, 0) = 1 \neq 0$.

7.3.7: Write $\phi(P) = (\phi_0(P) : \cdots : \phi_n(P))$ and let $n = \max\{v_P(\phi_i) : 0 \leq i \leq n\}$. Let t_P be a uniformizer at P. Then $(t_P^{-n}\phi_0 : \cdots : t_P^{-n}\phi_n)$ is regular at P. See Proposition II.2.1 of Silverman [564] for further details.

7.4.3: The first 3 statements are straightforward. The definitions also directly imply that $\mathfrak{m}_v$ is an R_v-ideal. The proof that $\mathfrak{m}_v$ is maximal and that R_v is a local ring is essentially the same as the proof of Lemma 7.1.2. Statement 5 follows from Statement 2.

7.4.6: The result follows since $\mathfrak{m}_{P,\Bbbk}(C)^m = \Bbbk(C) \cap \mathfrak{m}_{P,\Bbbk'}(C)^m$ for any $m \in \mathbb{Z}_{\geq 0}$.

7.4.8: $\mathfrak{m}_P^m = (t_P^m)$ so $f \in \mathfrak{m}_P^m$ and $f \notin \mathfrak{m}_P^{m+1}$ is equivalent to $f = t_P^m u$ where $u \in \mathcal{O}_P - \mathfrak{m}_P$ and hence $u \in \mathcal{O}_P^*$.

7.4.9: Write $f = t_P^a u$ and $h = t_P^b v$ where $u, v \in \mathcal{O}_P^*$ and note that $fh = t_P^{a+b} uv$.

7.4.12: Let $f = f_1/f_2$ with $f_1, f_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$. By Lemma 7.4.7 we have $f_1 = t_P^{v_P(f_1)} u_1$ and $f_2 = t_P^{v_P(f_2)} u_2$ for some $u_1, u_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)^*$. If $v_P(f) = v_P(f_1) - v_P(f_2) > 0$ then $f = t_P^{v_P(f_1) - v_P(f_2)} u_1/u_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ and so P is not a pole of f. On the other hand, if P is a pole of f then $1/f = t_P^{v_P(f_2) - v_P(f_1)} u_2/u_1 \in \mathfrak{m}_{P,\overline{\Bbbk}}(C)$.

7.7.3: If $f \in \overline{\Bbbk}^*$ then $\mathrm{div}(f) = 0$ and the result follows.

7.7.5: (5) follows immediately from part 4 of Lemma 7.4.14.

7.7.7: First, $\mathrm{Prin}_{\Bbbk}(C) \subseteq \mathrm{Div}_{\overline{\Bbbk}}(C)$ since functions only have finitely many poles and zeros. Second, if f is defined over $\Bbbk$ and $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then $f = \sigma(f)$ and so $\sigma(\mathrm{div}(f)) = \mathrm{div}(f)$ and so $\mathrm{Prin}_{\Bbbk}(C) \subseteq \mathrm{Div}_{\Bbbk}(C)$. Finally, $\mathrm{Prin}_{\Bbbk}(C)$ is closed under addition by Lemma 7.7.4.

7.7.9: Write f as a ratio of homogeneous polynomials of the same degree and then factor them as in equation (7.8).

7.7.15: $f/h \in \Bbbk(C)$ has $\operatorname{div}(f/h) = 0$ and so $f/h \in \Bbbk^*$.

7.9.6: See Cassels [122], Reid [497] or Silverman and Tate [567].

Chapter 8: Rational Maps on Curves and Divisors

8.1.2: Any non-constant morphism ϕ has a representative of the form $(\phi_1 : \phi_2)$ where ϕ_2 is not identically zero, and so define $f = \phi_1/\phi_2$. That ϕ is a morphism follows from Lemma 7.3.6.

8.1.10: $\Bbbk(x, y/x) = \Bbbk(x, y)$.

8.1.11: $\Bbbk(x, y) = \Bbbk(x^2, y)(x) = \phi^*(\Bbbk(C_2))(x)$, which is a quadratic extension.

8.2.3: See Proposition III.1.4 of Stichtenoth [589].

8.2.10: By Lemma 7.4.7, t is a uniformizer at Q if and only if $v_Q(t) = 1$. The problem is therefore equivalent to Lemma 8.2.9.

8.2.11: Since $\phi^*(\Bbbk(C_2)) = \Bbbk(C_1)$ it follows directly from the definition in terms of $\mathcal{O}_P$ and $\mathfrak{m}_P$ that if $\phi(P) = Q$ and $f \in \Bbbk(C_2)$ then $v_Q(f) = v_P(f \circ \phi)$.

8.2.16: Follows from Lemma 8.2.9.

8.3.12: The function can also be written $\phi((x : z)) = (1 : z^2/x^2)$. One has $\phi_*(D) = (1 : 1) + (1 : 0) - (0 : 1)$, $\phi^*(D) = (i : 1) + (-i : 1) + 2(1 : 0) - 2(0 : 1)$, $\phi_*\phi^*(D) = 2(-1 : 1) + 2(1 : 0) - 2(0 : 1) = 2D$ and $\phi^*\phi_*(D) = (1 : 1) + (-1 : 1) + 2(1 : 0) - 2(0 : 1)$.

8.3.15: Follows from Exercise 8.2.17.

8.4.3: See Section 8.2 of Fulton [216] or I.4.5 to I.4.9 of Stichtenoth [589].

8.4.6: By Corollary 7.7.13 all non-constant functions have a pole. Hence $\mathcal{L}_{\Bbbk}(0) = \Bbbk$. Since $\operatorname{div}(f) \equiv 0$ the second result follows from part 6 of Lemma 8.4.2.

8.4.10: The dimensions are $1, 1, 2, 3, 4, 5, 6$.

8.5.15: $\delta(x^p) = px^{p-1}\delta(x) = 0$.

8.5.27: If $\omega_1 = f_1 dt_P$ and $\omega_2 \equiv \omega_1$ then $\omega_2 = f_2 dt_P$ with $f_1 \equiv f_2$ in $\Bbbk(C)$, so there isn't anything to show here.

For the second point suppose t and u are two uniformizers at P. Write $\omega = f_1 dt = f_2 du$, so that $f_1/f_2 = \partial u/\partial t$. We must show that $v_P(f_1) = v_P(f_2)$. Since $u \in \mathfrak{m}_{P,\Bbbk}(C) = (t)$ we have $u = ht$ for some $h \in \Bbbk(C)$ such that $h(P) \neq 0$. Then $\partial u/\partial t = \partial(ht)/\partial t = h + t(\partial h/\partial t)$. It follows that $v_P(\partial u/\partial t) = 0$ and so $v_P(f_1) = v_P(f_2)$.

8.5.29: If $\omega' = f\omega$ then $\operatorname{div}(\omega') = \operatorname{div}(\omega) + \operatorname{div}(f)$.

8.6.3: An elliptic curve with only one point, e.g., $y^2 + y = x^3 + x + 1$ over $\mathbb{F}_2$.

Chapter 9: Elliptic Curves

9.1.1: It is clear that the formula gives the doubling formula when $x_1 = x_2, y_1 = y_2$. For the other case it is sufficient to compute

$$\left(\frac{y_1 - y_2}{x_1 - x_2}\right)\left(\frac{y_1 + y_2 + (a_1x_2 + a_3)}{y_1 + y_2 + (a_1x_2 + a_3)}\right)$$

and simplify to the above formula.

9.1.4: (These ideas originate in the work of Seroussi and Knudsen.) Dividing the equation by x_P^2 gives $(y_P/x_P)^2 + (y_P/x_P) = x_P + a_2 + a_6/x_P^2$ and the result follows by Exercise 2.14.7.

The formula for λ_Q is immediate from equation (9.2) and the formulae for x_P and y_P also follow immediately. If $P = [2]Q$ then $x_P = \lambda_Q^2 + \lambda_Q + a_2$ for some $\lambda_Q \in \mathbb{F}_{2^m}$ and so $\operatorname{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_P + a_2) = 0$. Since $\operatorname{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_P + a_2 + a_6/x_P^2) = 0$ it follows that $\operatorname{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_6/x_P^2) = 0$.

Conversely, if $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a_6/x_P^2) = 0$ then one can solve for $x_Q \in \mathbb{F}_{2^m}$ the equation $x_Q^2 + x_P + a_6/x_Q^2 = 0$. Further, $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_Q + a_2 + a_6/x_Q^2) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x_Q + x_Q^2 + a_2 + x_P) = 0$ so there is an element $y_Q \in \mathbb{F}_{2^m}$ such that $Q = (x_Q, y_Q) \in E(\mathbb{F}_{2^m})$. It then follows that $P = [2]Q$.

Finally, the formulae for point halving follow from substituting $y_Q = x_Q(\lambda_Q + x_Q)$ into the formula $y_P = (x_P + x_Q)\lambda_Q + x_Q + y_Q$.

9.1.5: We have $\lambda = (y_1/z_1 - y_2/z_2)/(x_1/z_1 - x_2/z_2) = (y_1 z_2 - y_2 z_1)/(x_1 z_2 - x_2 z_1)$. Similarly, putting $x_1/z_1, x_2/z_2$ and y_1/z_1 in the addition formulae in place of x_1, x_2 and y_1 gives the above formulae.

9.3.2: There is an inverse morphism which is a group homomorphism, also defined over $\Bbbk$ by definition, such that the composition is the identity.

9.3.8: From E_1 to E_2 is just $\phi(x, y) = (x + 1, y + x)$. From E_1 to E_3 is $\phi(x, y) = (x + s^2, y + sx + t)$ where $s \in \mathbb{F}_{2^4}$ satisfies $s^4 + s + 1 = 0$ and $t \in \mathbb{F}_{2^8}$ satisfies $t^2 + t = s^6 + s^2$.

9.4.5: For $t \in \mathbb{F}_{2^4}$ show that $\mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(s^6 + s^2) = 1 + u(s^4 + s + 1)^2 = 0$. Theorem 9.3.4 implies every element of $\mathrm{Aut}(E)$ is of this form. Since there are 24 choices for (u, s, t), each giving a different function on $E(\overline{\mathbb{F}}_2)$, one has $\#\mathrm{Aut}(E) = 24$. The fact that $\mathrm{Aut}(E)$ is non-Abelian follows can be shown as follows. Let $\phi_i(x, y) = (u_i^2 x + s_i^2, u_i^3 y + u_i^2 s_i x + t_i)$ for $i = 1, 2$. One can check that the x-coordinates of $\phi_1 \circ \phi_2$ and $\phi_2 \circ \phi_1$ are $u_1^2 u_2^2 x + u_1^2 s_2^2 + s_1^2$ and $u_1^2 u_2^2 x + u_2^2 s_1^2 + s_2^2$ respectively. These are not equal when, for example, $u_1 = 1$, $s_1 = \zeta_3$, $u_2 = \zeta_3$ and s_2 is arbitrary.

9.5.5: The first part of the exercise follows from Theorem 9.3.4. Points $P = (x_P, y_P)$ either satisfy $a_1 x_P + a_3 = 0$ and so $P = -P$ or $a_1 x_P + a_3 \neq 0$ and so y_P is a solution to

$$y^2 + y = F(x)/(a_1 x + a_3)^2.$$

By Exercise 2.14.7 this is soluble if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(F(x_P)/(a_1 x_P + a_3)^2) = 0$. Hence, every $x_P \in \mathbb{F}_{2^n}$ is such that either $a_1 x_P + a_3 = 0$ (in which case both E and $\widetilde{E}$ have a single point each with x-coordinate x_P) or precisely one of $y^2 + y = F(x_P)/(a_1 x_P + a_3)^2$ and $y^2 + y = F(x_P)/(a_1 x_P + a_3)^2 + \alpha$ has a solution. The result follows.

9.5.6: If $\sigma(\phi^{-1}) \circ \phi = 1 = \phi^{-1} \circ \phi$ for all σ then $\sigma(\phi^{-1}) = \phi^{-1}$ for all σ and ϕ^{-1} is defined over $\Bbbk$.

9.5.8: Follow the method of Lemma 9.5.7; also see Proposition 1 of Hess, Smart and Vercauteren [284].

9.5.9: We have $j(E) = 0$ and the only elliptic curves $\widetilde{E}/\mathbb{F}_2$ with $j(\widetilde{E}) = 0$ in short Weierstrass form are $y^2 + y = x^3 + a_4 x + a_6$ with $(a_4, a_6) \in \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. One can verify by direct calculation that for any pair E_1, E_2 of distinct curves in this form, the isomorphism between them is not defined over $\mathbb{F}_2$.

9.6.2: Let $E_2 : y^2 + H(x)y = F(x)$. If $\phi(x, y) = (\phi_1(x, y), \phi_2(x, y))$ is a morphism then so is $-\phi(x, y) = (\phi_1(x, y), -\phi_2(x, y) - H(\phi_1(x, y))$.

9.6.7: We know that $[0]$ and $[1]$ are isogenies and that the inverse of an isogeny is an isogeny, so we may assume that $n \geq 2$. Lemma 9.6.6 shows that the sum of two isogenies is an isogeny. It follows by induction that $[n] = [n - 1] + [1]$ is an isogeny.

9.6.10: Use the fact that $[2]P = \mathcal{O}_E$ if and only if $P = -P = \iota(P)$. Everything is direct calculation except for the claim that the quartic has distinct roots, which follows by observing that if x_1 is a repeated root then the corresponding point (x_1, y_1) would be singular.

9.6.16: There are many proofs: using differentials; showing that $\ker(\pi_q) = \{\mathcal{O}_E\}$; determining $\Bbbk(E)/\pi_q^*(\Bbbk(E))$. The statement of the degree follows by Lemma 9.6.13.

9.6.20: This is an immediate consequence of Theorem 9.6.18 (the fact that λ is an isomorphism comes from considering degrees). The details are also given in Proposition 12.12 of Washington [626].

9.6.22: We have $(\psi - \widehat{\phi}) \circ \phi = [0]$ and so the result follows by the same argument using degrees as in the proof of Lemma 9.6.11. One can also use Theorem 9.6.18.

9.6.25: This follows since ρ^* is essentially $\rho^{-1}(x,y) = (\zeta_3^{-1}x, y) = (\zeta_3^2 x, y)$.

9.6.29: A point of order 3 means $[2]P = -P$ and the subgroup being rational means either P is defined over $\Bbbk$ or P is defined over $\Bbbk'/\Bbbk$ and $\sigma(P) = -P$ for all non-trivial $\sigma \in \mathrm{Gal}(\Bbbk'/\Bbbk)$. It follows that $\Bbbk'/\Bbbk$ is quadratic. Translating x to 0 gives a point $(0, v)$. Since $\mathrm{char}(\Bbbk) \neq 2$ we assume $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ and clearly $v^2 = a_6$. The condition $[2](0,v) = (0,-v)$ implies $a_2 = (a_4/2v)^2 = a_4^2/(4a_6)$ and re-arranging gives the first equation. For the twist write $w = a_4/2a_6$, $X = wx$, $Y = w^{3/2}y$ and $A = a_6w^3$. Then

$$X^3+A(X+1)^2 = w^3x^3+(A/a_6^2)(a_6wx+a_6)^2 = w^3(x^3+(A/(w^3a_6^2))((a_4/2)x+a_6)^2 = w^3y^2 = Y^2.$$

It is easy to check that this final equation is singular if and only if $A = 0$ or $27/4$.

9.6.30: See Doche, Icart and Kohel [183].

9.7.6: Let $\phi(x,y) = (\phi_1(x), cy\phi_1(x)' + \phi_3(x))$ be an isogeny from E to $\widetilde{E}$ over a field $\Bbbk$ of characteristic 2. By definition, $X = \phi_1(x)$ and $Y = cy\phi_1(x)' + \phi_3(x)$ satisfy the curve equation $Y^2 + (\widetilde{a}_1X + \widetilde{a}_3)Y = X^3 + \widetilde{a}_2X^2 + \widetilde{a}_4X + \widetilde{a}_6$. Now

$$Y^2 + (\widetilde{a}_1X + \widetilde{a}_3)Y = (cy\phi_1(x)' + \phi_3(x))^2 + (\widetilde{a}_1\phi_1(x) + \widetilde{a}_3)(cy\phi_1(x)' + \phi_3(x))$$

and $\widetilde{a}_1\phi_1(x) + \widetilde{a}_3 = c(a_1x + a_3)\phi_1(x)'$. Hence

$$Y^2 + (\widetilde{a}_1X + \widetilde{a}_3)Y = (c\phi_1(x)')^2(y^2 + (a_1x + a_3)y) + \phi_3(x)^2 + (\widetilde{a}_1\phi_1(x) + \widetilde{a}_3)\phi_3(x).$$

It follows that $\phi_3(x)$ must satisfy the following quadratic equation over $\Bbbk(x)$

$$\phi_3(x)^2+c(\widetilde{a}_1\phi_1(x)+\widetilde{a}_3)\phi_1(x)'\phi_3(x)+(c\phi_1(x)')^2(x^3+a_2x^2+a_4x+a_6)+\phi_1(x)^3+\widetilde{a}_2\phi_1(x)^2+\widetilde{a}_4\phi_1(x)+\widetilde{a}_6 = 0.$$

Since $\Bbbk(x)$ is a field there are at most two possible values for $\phi_3(x)$.

9.8.3: $[3]P = \mathcal{O}_E$ if and only if $[2]P = -P$. Hence, if $P = (x,y)$ is such that $[3]P = \mathcal{O}_E$ then $\lambda^2 = 3x = 0$ where $\lambda = (3x^2 + 2a_2x + a_4)/(2y) = (2a_2x + a_4)/(2y)$. The statements all follow from this.

9.9.5: Use the fact that the dual isogeny of $\phi^2 - [t]\phi + [d]$ is $\widehat{\phi}^2 - [t]\widehat{\phi} + [d]$ since $[\widehat{t}] = [t]$ etc.

9.10.4: For each $y \in \mathbb{F}_p$ there is a unique solution to $x^3 = y^2 - a_6$ and so there are p solutions to the affine equation. Counting the point at infinity gives the result.

9.10.5: Write the curve as $y^2 = x(x^2 + a_4)$. Since -1 is not a square, for any $x \in \mathbb{F}_p$ we have either $x(x^2 + a_4) = 0$ or exactly one of $x(x^2 + a_4)$ and $-x(x^2 + a_4)$ is a square. Hence there are p solutions to the affine equation.

9.10.10: Maintain a pair of the form (t_i, t_{i+1}). So start with $(t_1 = t, t_2 = t^2 - 2q)$. Given (t_i, t_{i+1}) we can compute (t_{2i}, t_{2i+1}) by first computing t_{2i} and then t_{2i+1} using the above formulae. To go from (t_i, t_{i+1}) to (t_{2i+1}, t_{2i+2}) one computes $t_{2i+1} = t_it_{i+1} - q^it$ and $t_{2i+2} = t_{i+1}^2 - 2q^{i+1}$. One can then perform a ladder algorithm (working through the binary expansion of n) as in Lemma 6.3.19.

9.10.11: The first statement is easy to verify by counting points. The second statement follows since if $m \mid n$ then $E_a(\mathbb{F}_{2^m})$ is a subgroup of $E_a(\mathbb{F}_{2^n})$ and so $\#E_a(\mathbb{F}_{2^m}) \mid \#E_a(\mathbb{F}_{2^n})$. Also, if $m \geq 3$ then $\#E_a(\mathbb{F}_{2^m}) > 4$. Hence, it suffices to restrict attention to prime values for n in the third part. The values for E_1 are 5, 7, 11, 17, 19, 23, 101, 107, 109, 113, 163 and the values for E_0 are 5, 7, 9, 13, 19, 23, 41, 83, 97, 103, 107, 131.

9.10.21: The possibilities are $p + 1 \pm 46$ and $p + 1 \pm 60$. One can test which arises by choosing a random point $P \in E(\mathbb{F}_p)$ and computing $[p + 1 - t]P$ for each choice of t. One finds that the orders are $p + 1 + 46, p + 1 - 60, p + 1 - 46, p + 1 - 46$ respectively.

9.10.22: The equation $p = a^2 + ab + b^2$ implies $p = (a - b\zeta_3)(a - b\zeta_3^2)$ and the corresponding value for $\pi + \overline{\pi}$ as in Theorem 9.10.18 is $(2a - b(\zeta_3 + \zeta_3^2)) = 2a + b$. To get the other solutions one notes that the solutions to $x^2 + xy + y^2 = p$ are obtained from (a, b) via the symmetries $(a, b) \mapsto (-a, -b)$; $(a, b) \mapsto (b, a)$ and $(a, b) \mapsto (b, a + b)$ which corresponds to $(a - b\zeta_3) \mapsto \zeta_3(a - b\zeta_3)$. One finds 12 pairs (a, b) and these give rise to the 6 values for t claimed.

9.11.1: The first claim is proved by induction, starting with $t \equiv 0 \pmod{p}$. For the second claim, recall that points in $E[p]$ correspond to roots of the p-th division polynomial and hence must be defined over some finite extension of $\mathbb{F}_q$. But if $E(\mathbb{F}_{q^n})$ has a point of order p then $\#E(\mathbb{F}_{q^n}) \equiv 0 \pmod{p}$.

9.11.10: We have (ignoring for the moment the easy case $P(T) = (T \pm \sqrt{q})^2$) $\frac{1}{q}P(T\sqrt{q}) \mid \Phi_m(T^2) \mid T^{2m} - 1 = (T^m - 1)(T^m + 1)$ in $\mathbb{R}[x]$ for some $m \in \{1, 2, 3, 4, 6\}$. It follows (this requires some work) that $P(T) \mid (T^m - q^{m/2})(T^m + q^{m/2})$ in $\mathbb{Z}[x]$. Hence, if α is a root of $P(T)$ then $\alpha^m = \pm q^{m/2} \in \mathbb{Z}$. Similarly, $\#E(\mathbb{F}_q) = P(1) \mid (q^m - 1)$.

9.11.14: Take any supersingular elliptic curve E_1 over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1$ and let E_2 be a non-trivial quadratic twist.

9.12.6: The statements about (X_1, Z_1) and (X_2, Z_2) are immediate. For the others, substitute X_n/Z_n, X_m/Z_m and X_{m-n}/Z_{m-n} for x_1, x_2 and x_4 in Lemma 9.12.5.

9.12.7: The idea is to store $(X_n, Z_n, X_{n+1}, Z_{n+1})$ (taking $m = n+1$ we have $(X_{m-n}, Z_{m-n}) = (x_P : 1)$ and so the above formulae may be used). The exponentiation is done using a "ladder algorithm" (analogous to Lemma 6.3.19) which computes either $(X_{2n}, Z_{2n}, X_{2n+1}, Z_{2n+1})$ or $(X_{2n+1}, Z_{2n+1}, X_{2n+2}, Z_{2n+2})$. Every step is therefore a doubling and an addition. See Algorithm 13.35 of [16]. For the improved formulae see [436] or Section 13.2.3.a of [16].

9.12.8: One has

$$[2](x, y) = (B\lambda^2 - 2x - a_2, \star)$$

where $\lambda = (3x^2 + 2a_2x + a_4)/(2By)$ and where the formula for the y-coordinate is not relevant here. Solving $[2](x, y) = (0, 0)$ is solving $B\lambda^2 = 2x + a_2$ and so $0 = (3x^2 + 2a_2x + a_4)^2 - 4(x^3 + a_2x^2 + a_4x)(2x + a_2) = (x^2 - a_4)^2$. Hence, $x = \pm\sqrt{a_4}$ and the y-values are $\pm\sqrt{x(x^2 + a_2x + a_4)/B}$ as stated.

9.12.10: The point $(1, 1)$ on $(A + 2)y^2 = x(x^2 + Ax + 1)$ has order 4.

9.12.17: Homogenising gives the equation $(ax^2 + y^2)z^2 = z^4 + dx^2y^2$ and setting $z = 0$ leads to the equation $dx^2y^2 = 0$ and hence the two points $(1 : 0 : 0)$ and $(0 : 1 : 0)$. To show that $(1 : 0 : 0)$ is singular it suffices to set $x = 1$ and show that the point $(0, 0)$ on $(a + y^2)z^2 = z^4 + dy^2$ is singular, which is easy. The other case is similar.

9.12.23: Writing the curve equation as $x^2 = (1 - y^2/(a - dy^2)$ the quadratic twist is $ux^2 = (1 - y^2)/(a - dy^2)$ which gives the result.

9.12.24: Follows directly from Theorem 9.12.12.

9.12.27: Irreducibility follows since $y^2 - g(x)$ must factor as $(y + g_1(x))(y + g_2(x))$ and it follows that $g_2(x) = -g_1(x)$ (which is prohibited by $a^2 \neq d$). The point $(0 : 1 : 0)$ on $y^2z^2 = x^4 + 2ax^2z^2 + z^4$ is singular. An affine singular point on C must satisfy $y = 0$, $4x(dx^2 + a) = 0$ and $dx^4 + 2ax^2 + 1 = 0$, which again is impossible if $a^2 \neq d$.

The birational map is easy to verify: $2Y^2 = X(2X/x^2)$ and $X(X^2 - 2aX + (a^2 - d)) = X(a^2 + 2a(y + 1)/x^2 + (y + 1)^2/x^4 - 2a^2 - 2a(y + 1)/x^2 + a^2 - d)$ and the result follows by substituting for y^2. Finally, the discriminant of $X^2 - 2aX + (a^2 - d)$ is $4d$ so when d is a square in $\Bbbk$ then there are three points $(0, 0), (a \pm \sqrt{d}, 0)$ of order 2.

9.12.29: Let P be a point of order 2 and move P to $(0, 0)$ so that the curve is $Y^2 = X(X^2 + Ax + B)$. Write $a = -A/2$ and $d = a^2 - B$ so that a twist of the curve is in the form of equation (9.16). The result follows from Exercise 9.12.27.

Chapter 10: Hyperelliptic Curves

10.1.3: When we substitute $z = 0$ we get the equation $H_{D-1}x^{D-1}y = F_D x^D$ where H_{D-1} (respectively, F_D) is the coefficient of the monomial x^{D-1} (resp., x^D) in $H(x)$ (resp., $F(x)$). The possible solutions are $x = 0$, giving the point $(x : y : z) = (0 : 1 : 0)$, or $H_{D-1}y = F_D x$ giving the point $(H_{D-1} : F_D : 0)$.

For the second part, we have $H_D = 0$ and so the only point at infinity is $(0 : 1 : 0)$. Making the curve affine by setting $y = 1$ yields $z^{D-2} + z^{D-1}H(x/z) = z^D F(x/z)$ and when $D > 3$ every monomial has degree at least 2. Hence the two partial derivatives vanish.

10.1.5: Make the change of variable $y = Y + x^3 + 1$. Then

$$y^2 + (1 - 2x^3)y = Y^2 + 3Y - x^6 + x^3 + 2$$

and so the affine curve is isomorphic to $Y^2 + 3Y = x - 1$. This curve is birational to $\mathbb{P}^1$ (taking the map $(x, Y) \mapsto Y$) and hence, by Theorem 8.6.1 and Definition 8.6.2, the curve has genus 0.

10.1.13: If $H_0 = F_1 = F_0 = 0$ then $(0, 0) \in C(\Bbbk)$ is singular. (This also follows since $C^\dagger$ is birational to C and the genus is a birational invariant.)

10.1.20: 1. One way is $(x, y) \mapsto (y : x^d : x^{d-1} : \cdots : x : 1)$. The other way is $(Y : X_d : X_{d-1} : \cdots : X_1 : X_0) \mapsto (Y, X_d/X_{d-1})$.

2. The statement about ι is clear.

3. Identifying $X_i = x^i z^{d-i}$ it follows that points at infinity (i.e., with $z = 0$) have $X_i = 0$ when $0 \leq i < d$.

4. Set $X_d = 1$ to give the point $(Y, X_{d-1}, \ldots, X_0) = (\alpha, 0, \ldots, 0)$ on the affine curve

$$Y^2 + H(X_{d-1}, \ldots, X_0)y = F(X_{d-1}, \ldots, X_0)$$

together with various other equations, including $X_i = X_{\lceil (d+i)/2 \rceil} X_{\lfloor (d+i)/2 \rfloor}$ for $0 \leq i \leq d-2$. One must determine the Jacobian matrix (see Theorem 7.1.12 and Corollary 7.1.13) at the point $(\alpha, 0, \ldots, 0)$. The number of variables is $d+1$ and the dimension is 1, so we need to show that the rank is d. Note that each of the $d-1$ equations $X_i = X_{\lceil (d+i)/2 \rceil} X_{\lfloor (d+i)/2 \rfloor}$ yields a row $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ in the Jacobian matrix (with the 1 corresponding to variable X_i). Hence, the rank is at least $d - 1$. The curve equation yields the row

$$(2\alpha + H_d, H_{d-1}\alpha - F_{2d-1}, 0, \ldots, 0)$$

in the Jacobian matrix, so to complete the proof we must show that either $2\alpha + H_d \neq 0$ or $H_{d-1}\alpha + F_{2d-1} \neq 0$. Note that at least one of $\{F_{2d}, F_{2d-1}, H_d\}$ is non-zero, otherwise we would replace d by $d - 1$.

If $\mathrm{char}(\Bbbk) \neq 2$ and both terms are zero then $\alpha = -H_d/2$ which implies that $F_{2d} = -(H_d/2)^2$ and $F_{2d-1} = -H_d H_{d-1}/2$ which violates the condition of Lemma 10.1.8. If $\mathrm{char}(\Bbbk) = 2$ then we must consider the three cases in Lemma 10.1.6. The first case is $\alpha = 0$ and $F_{2d-1} \neq 0$ and so $H_{d-1}\alpha + F_{2d-1} \neq 0$. The second and third cases have $H_d \neq 0$ and so $2\alpha + H_d = H_d \neq 0$.

10.1.23: The statement $v_\infty(x) = -2$ follows from the fact that $v_{\rho(\infty)}(Z) = 2$ as in Lemma 10.1.21. The second claim follows since $\infty = (1 : 0 : 0)$ and $1/x = c(y/x^d)^2$ for some constant c, in which case $c(y/x^d) = x^{d-1}/y$. The third claim is immediate from Lemma 10.1.22.

10.1.25: Write $d = g + 1$. Note that

$$v_\infty(y) = v_\infty((y/x^d)x^d) = v_\infty(y/x^d) + d v_\infty(x).$$

Hence, if C is in ramified model then $v_\infty(y) = 1-2d = -(2d-1) = -(2g+1)$. Similarly, if C is in split model then $v_{\infty^+}(y) = 0-d = -(g+1)$.

10.1.26: $v_P(A-yB)+v_P(A-(-y-H)B) = v_P(A^2+HAB-FB^2)$ which is $2e$ when $P=\iota(P)$ and is e otherwise.

10.1.27: A uniformizer at ∞^+ is X_{d-1}/X_d if $\iota(\infty^+) \neq \iota(\infty^+)$ and $Y/X_d - \alpha^+$ otherwise.

10.1.28: The choice of the leading coefficient already implies $\deg(G^+(x)^2+H(x)G^+(x)-F(x)) \leq 2d-1$. Write $G^+(x) = \alpha^+x^d + G_{d-1}x^{d-1} + \cdots + G_0$. One can solve a linear equation in G_{d-1} so that the degree of $G^+(x)^2 + H(x)G^+(x) - F(x)$ is at most $2d-2$. Continuing this way one solves a linear equation for each variable G_i to lower the degree to at most $d+i-1$. The result for $G^-(x)$ follows by starting with α^- instead of α^+.

10.1.29: First note that $(y-G^+(x))/x^d = (y/x^d - \alpha^+) + (1/x)G(1/x)$ for some $G(x) \in \Bbbk[x]$ and so is zero at ∞^+. Since $\alpha^+ \neq \alpha^-$ it follows that $(y-G^+(x))/x^d$ is not zero at ∞^-. Also, $v_{\infty^-}(y-G^+(x)) \geq \max\{v_{\infty^-}(y), v_{\infty^-}(G^+(x))\} = -d = -(g+1)$ Now, $\deg(G^+(x)^2 + H(x)G^+(x) - F(x)) \leq d-1 = g$ so the affine effective divisor $\mathrm{div}(y-G^+(x)) \cap \mathbb{A}^2$ has degree at most g. Since $\mathrm{div}(y-G^+(x))$ must have degree 0 and $v_{\infty^-}(y-G^+(x)) = -(g+1)$ it follows that $v_{\infty^+}(y-G^+(x)) \geq 1$.

One can also complete the proof directly from the equation

$$(y-G^+(x))(-y-H(x)-G^+(x)) = G^+(x)^2 + H(x)G^+(x) - F(x),$$

the right hand side of which is a polynomial of degree at most g. It follows that the negative integer $v_{\infty^+}(y-G^+(x)) + v_{\infty^+}(-y-H(x)-G^+(x))$ is at least $-g$.

10.2.4: This is similar to Exercise 9.5.5.

10.2.5: First take a root α of $F(x)$ and move it to ∞. Then perform a change of variable on the remaining roots so that one is 0, another is 1 and change y so that the polynomial is monic.

10.2.7: Follows immediately from Theorem 10.2.1.

10.3.8: If $P = (x_P, y_P) \neq \iota(P)$ and $(x-x_P)^{e_P} \| u(x)$ then the claim is immediate from $v_P(u(x)) = e_P$ and $v_P(y-v(x)) = v_P((y-v(x))(-y-H(x)-v(x)) = v_P(v(x)^2 + H(x)v(x) - F(x)) \geq v_P(u(x))$. If $P = \iota(P) = (x_P, y_P)$ then $y-y_P$ is a uniformizer at P. We have $v_P(u(x)) = v_P(x-x_P) = 2$ and since $v(x) = y_P + (x-x_P)G(x)$ for some polynomial $G(x) \in \overline{\Bbbk}[x]$ we have $v_P(y-v(x)) = v_P((y-y_P) - (x-x_P)G(x)) = 1$.

10.3.11: The first statement follows from the following two facts: (1) if D is effective then so is $\sigma(D)$; (2) $\sigma(\iota(P)) = \iota(\sigma(P))$. The second follows since $\sigma(D) = \sum_P n_P(\sigma(P))$ and if $u(x) = \prod_P (x-x_P)^{n_P}$ then $\sigma(u(x)) = \prod_P (x-\sigma(x_P))^{n_P} = \prod_P (x-x_{\sigma(P)})^{n_P}$ etc. The third statement follows from the second and the uniqueness of the Mumford representation.

10.3.12: Since the $u_i(x)$ are co-prime the composition does not have any special cases and the equality of divisors is clear. This can also be seen by considering points over $\overline{\Bbbk}$.

10.3.15: Note that $\iota(6,4) = (6,4)$ and so $2D_1 \equiv 2(0,4)$. The answers are $(x^2+5x, 4), (x^2-x, -3x+4), (x^2, 10x+4), (x^4+4x^3+6x^2, 4+10x+6x^2+3x^3)$.

10.3.16: All polynomials are of degree $O(m)$ and multiplication, computing the extended gcd, and division can be performed in $O(m^2)$ field multiplications.

10.4.2: The inverse of $D = \sum_P n_P(P)$ is $\iota_*(D) = \sum_P n_P(\iota(P))$. Hence, since the points P in the divisor class represented by $(u(x), v(x))$ are of the form $(x_i, v(x_i))$ where $u(x_i) = 0$ the corresponding points for the inverse of D are $(x_i, -v(x_i) - H(x_i))$. The result follows.

10.4.5: Just re-arrange the equation $D_3 - d_3(\infty) \equiv D_1 - d_1(\infty) + D_2 - d_2(\infty)$.

10.4.8: One has $v_{\infty^-}(y-v^\ddagger(x)) = v_{\infty^-}(y-G^+(x)) = -d$. The affine part of the second claim is already proved in the proof of Lemma 10.4.6. Since $\deg(\mathrm{div}(y-v^\ddagger(x))) = 0$ it

follows that $v_{\infty^+}(y - v^\ddagger(x)) = -(d_u + d_{u^\dagger} - d)$. (There is also a direct proof of this fact.)

10.4.15: This is very similar to the proofs of Lemma 10.4.6 and Lemma 10.4.11.

Let $d_u = \deg(u(x))$. The leading $d - (d_u - 1)$ coefficients of $v^\ddagger(x)$ agree with $G^+(x)$ and hence $\deg(v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x)) \leq 2d - (d - (d_u - 1)) = d + d_u - 1$. It follows that $\deg(u^\dagger(x)) \leq d - 1$. Since $v_{\infty^-}(y - v^\ddagger(x)) = -d$ and since $\mathrm{div}(y - v^\ddagger(x))$ has degree 0 one has $v_{\infty^+}(y - v^\ddagger(x)) = -(\deg(u(x) + \deg(u^\dagger(x)) - d)$. The result follows from the analogue of equation (10.17).

10.4.17: Clearly,

$$\begin{aligned} &\iota_*(D + n(\infty^+) + (g - d_u - n)(\infty^-) - D_\infty) \\ &= \iota_*(D) + n(\infty^-) + (g - d_u - n)(\infty^+) - \iota_*(D_\infty)) \end{aligned}$$

When g is even then $\iota_*(D_\infty) = D_\infty$ and the result is immediate by Exercise 10.4.2. When g is odd note that $\iota_*(D_\infty) = D_\infty + (\infty^-) - (\infty^+)$ and so

$$\begin{aligned} &\iota_* \left(D + n(\infty^+) + (g - \deg(u(x)) - n)(\infty^-) - D_\infty\right) \\ &= \iota_*(D) + (n-1)(\infty^-) + (g - \deg(u(x)) - n + 1)(\infty^+) - D_\infty. \end{aligned}$$

If $n = 0$ then this divisor is not effective and so it is necessary to perform composition and reduction at infinity.

10.4.20: This is the special case $D_1 = D_2 = 0, n_1 = 0, n_2 = \lceil g/2 \rceil + 1$ of Theorem 10.4.19, since $D = (1, 0, 0)$ is principal.

10.4.21: This follows from Theorem 10.4.19.

10.4.22: Let $\rho_P(x, y) = (1/(x - x_P), y/(x - x_P)^{g+1})$ map P to ∞^+. If $\mathrm{div}(f(x, y)) = n((P) - (\iota(P))$ then $\mathrm{div}(f \circ \rho_P^{-1}) = n((\infty^+) - (\infty^-))$.

10.5.2: By Lemma 8.1.3 and Theorem 8.2.7 we know ϕ is surjective. Hence, for any $P \in E(\overline{\Bbbk})$ choose any point $P' \in C(\overline{\Bbbk})$ such that $\phi(P') = P$ and let $P'' \in C(\overline{\Bbbk})$ be such that $\phi(P'') = \mathcal{O}_E$. Then $\phi_*((P') - (P'')) = (P) - (\mathcal{O}_E)$ as required. The second statement follows since the kernel of ϕ^* is contained in the kernel of $\phi_*\phi^* = [\deg(\phi)]$.

10.6.3: See Mumford [445] pages 3.31-3.32.

10.7.7: An elegant proof using power series is given in Exercises 17.19 and 17.20 of Shoup [556].

10.7.8: One has $t_1 = 0, t_2 = -42, t_3 = 0$. Hence $a_1 = 0, a_2 = 21$ and $a_3 = 0$. It follows that $\#\mathrm{Pic}^0_{\mathbb{F}_7}(C) = 512$.

10.7.14: First, one needs to count various types of points in $C(\mathbb{F}_q)$ and $C(\mathbb{F}_{q^2})$. Note that there is a single point at infinity ∞ on $C(\mathbb{F}_{q^n})$ for all $n \in \mathbb{N}$. Write m for the number of roots of $F(x)$ in $\mathbb{F}_q$. Let $u = \frac{1}{2}(N_1 - 1 - m) = \frac{1}{2}(q - t_1 - m)$. Then there are u values for $x_P \in \mathbb{F}_q$ such that there are points $P = (x_P, y_P) \in C(\mathbb{F}_q)$ with $P \neq \iota(P)$. Hence $\#C(\mathbb{F}_q) = 1 + m + 2u$. There are q possible values for $x_P \in \mathbb{F}_q$. We have shown that $m + u$ of them arise as x-coordinates of points in $C(\mathbb{F}_q)$ (i.e., $F(x_P)$ is a quadratic residue for those values). For the remaining $q - m - u$ values x_P it follows that $F(x_P)$ is not a square in $\mathbb{F}_q$. But $F(x_P)$ is a square in $\mathbb{F}_{q^2}$ so x_P must arise as the x-coordinate of a point in $C(\mathbb{F}_{q^2})$. Hence there are $q - m - u = \frac{1}{2}(q + t_1 - m)$ such values for x_P. Hence, there are $\frac{1}{2}(q - m + t_1)$ points $P = (x_P, y_p) \in C(\mathbb{F}_{q^2})$ with $x_P \in \mathbb{F}_q$, $y_P \notin \mathbb{F}_q$ and $P \neq \iota(P)$.

Exercise 10.4.4 classifies divisor classes so it is sufficient to count the number of representatives for each case. Case 1 gives N_1 divisor classes.

For case 2, let m be the number of roots of $F(x)$ in $\mathbb{F}_q$. Therefore, there are $m + 1$ points $P \in C(\mathbb{F}_q)$ such that $P = \iota(P)$. Hence, case 2 gives $N_1 - 1 - m$ divisor classes.

For case 3, we first count the set of pairs (P, Q) such that $P, Q \neq \infty$, and $Q \notin \{P, \iota(P)\}$. There are $N_1 - 1$ choices for P, and for each there are either $N_1 - 2$ or $N_1 - 3$ choices for Q (depending on whether $P = \iota(P)$ or not). Finally, since in this case we always have

$P \neq Q$, the number of choices for $\{P, Q\}$ is half the number of pairs (P, Q). Hence the total number of divisor classes in case 3 is

$$\tfrac{1}{2}((N_1 - m - 1)(N_1 - 3) + m(N_1 - 2)).$$

We finally consider case 4 of Exercise 10.4.4. Note that $\mathbb{K} = \mathbb{F}_{q^2}$ is the unique quadratic extension of $\mathbb{F}_q$. We have $P = \sigma(P)$ if and only if $P \in C(\mathbb{F}_q)$. Hence, the number of choices for $\{P, \sigma(P)\}$ is $\frac{1}{2}(N_2 - N_1)$. From these choices we must subtract the number of pairs $\{P, \sigma(P)\}$ such that $\sigma(P) = \iota(P)$. This happens when $x_P \in \mathbb{F}_q$ but $y_P \notin \mathbb{F}_q$ and by the above argument there are $\frac{1}{2}(q - m + t_1)$ such points. Hence, the total number of divisor classes in case 4 is

$$\tfrac{1}{2}(q^2 + 1 - t_2 - (q + 1 - t_1) - (q - m + t_1)) = \tfrac{1}{2}(q^2 - 2q - t_2 + m).$$

Adding up all the cases gives

$$(q + 1 - t_1) + (q - t_1 - m) + \tfrac{1}{2}(q^2 - q(2t_1 + 2) + t_1^2 + 2t_1 + m) + \tfrac{1}{2}(q^2 - 2q - t_2 + m)$$

which simplifies to

$$q^2 - t_1 q + (t_1^2 - t_2)/2 - t_1 + 1$$

as required.

10.9.4: This proof follows the same layout as Lemma 9.11.8 and Corollary 9.11.9. The details are given in [218].

10.9.6: We have $p \mid a_1$ and $p \mid a_2$, which is equivalent to the conditions for supersingularity.

10.9.7: First, simply show that $\#C(\mathbb{F}_{2^{nk}})$ is always odd and so t_1 and t_2 (notation as in Lemma 10.7.6) are even. Hence a_1, a_2 are even (for the details of this calculation see Lemma 2 of [218]). The result then follows from part 1 of Theorem 10.9.5 and Exercise 10.9.6.

Chapter 11: Basic Algorithms for Algebraic Groups

11.1.2: If a is odd at any stage then the new value $(a - a_i) \equiv 0 \pmod 4$ so the non-zero coefficient a_i is followed by $a_{i+1} = 0$.

11.1.6: $100 = 10\overline{1}00100$ etc.

11.1.9: The largest possible NAF of length $l + 1$ is $2^l + 2^{l-2} + 2^{l-4} + \cdots$ and taking $d_l = 2^{l-2} + 2^{l-4} + \cdots + 1$ when l is even and $d_l = 2^{l-2} + 2^{l-4} + \cdots + 2$ when l is odd gives the formula for d_l. If $a_l = -1$ then $a = -2^l + d_l < 0$, which is a contradiction. The minimal value for a is therefore $2^l - d_l$. One can check that $2^l + d_l + 1 = 2^{l+1} - d_{l+1}$. Finally, $2^{l+1}/3 < 2^l - d_L \leq a$ so $l \leq \log_2(a) - \log_2(2/3) \approx \log_2(a) + 0.585$. Since the binary expansion of a requires $\lfloor \log_2(a) \rfloor + 1$ bits the result follows.

11.1.15: Write N_k for the number of NAFs of length k (so $k = l + 1$ in the above notation). We have $N_1 = 3$ and $N_2 = 5$. Also $N_{k+1} = N_k + 2N_{k-1}$ from which the formula follows.

11.1.21: Essentially the same proof as Lemma 11.1.8. See Proposition 2.1 or Muir and Stinson [442].

11.1.23: Proposition 2.4 of Muir and Stinson [442].

11.1.26: 300070007 and $100\overline{1}000\overline{1}00\overline{1}$.

11.2.2: There are 2^n values $u_{b_1,\ldots,b_n}$ to compute: $n + 1$ of them come for free (corresponding to the vectors $(b_1, \ldots, b_n)$ that are all zero or have only one non-zero entry) and, if the computation is organised appropriately, each of the others can be obtained from

an earlier value using one additional multiplication. The second claim of the exercise is clear.

11.2.3: For windows of length w one must precompute all $u_{b_1,\ldots,b_n} = \prod_{i=1}^{n} g_i^{b_i}$ for $0 \leq b_i < 2^w$ under the constraint that at least one of the b_i is odd. The number of such values is $2^{nw} - 2^{n(w-1)}$ of which n come for free. Hence the precomputation requires $2^{nw} - 2^{n(w-1)} - n$ multiplications (actually, when $w > 1$ the computation can be arranged so that some of these are squarings). See Yen, Laih and Lenstra [638] for details.

11.2.4: See Algorithm 3.51 of [274].

11.3.1: Given $P = (x_P, y_P)$ compute a solution to $\lambda_Q^2 + \lambda_Q = x_P + a_2$, determine whether the corresponding value of x_Q^2 satisfies the trace condition (and if not, replace λ_Q by $\lambda_Q + 1$), compute a square root (which is easy in finite fields of characteristic two), and solve for y_Q. See Knudsen [342] for details.

11.3.4: The cost depends on the number of non-zero values for a_i, which is the weight. The number of elliptic curve additions is one less than the weight. We ignore the cost of computing the Frobenius maps.

11.3.10: Let $n_0 = 107$ and $n_1 = 126$ so $a_0 = -1$ and the new values for (n_0, n_1) are $(180, -54)$. The Frobenius expansion is

$$-1 - \pi^5 - \pi^7 - \pi^9 + \pi^{11} + \pi^{13} + \pi^{16}.$$

11.3.13: $P \in E(\mathbb{F}_{p^m})$ if and only if $(\pi^m - 1)P = \mathcal{O}_E$.

11.3.16: It is clear that P is in the kernel of the endomorphism corresponding to this polynomial. Now, note that $(x^{19} - 1)/(x - 1) \equiv -457 + 314x \pmod{x^2 - x + 2}$ and that $-457 + 314\pi$ has norm r. Rounding $n(-457 + 314\bar{\pi})/r$ gives $-67 - 148\pi$ from which we get

$$n - (-67 - 148\pi)(-457 + 314\pi) = -107 - 126\pi$$

as was found using the GLV method.

11.3.19: One first precomputes all $\sum_{j=0}^{w-1} [a_j]\pi^j(P)$. To do this one computes all $[a_j]P$, which needs one doubling and (when q is odd) $(q-5)/2$ additions or (when q is even) $q/2 - 2$ additions. One computes $[a_j]\pi^j(P)$ as $\pi^j([a_j]P)$ and we ignore the cost of this. To compute all the terms requires at most q^{w-1} additions. Hence, the total cost of precomputation is at most $q/2 + q^{w-1}$ group operations.

The exponentiation itself then requires at most $(l+1)/w$ additions.

11.3.20: First compute integers a_0', a_1' such that $a_0' + a_1'\pi \equiv a(\pi) \pmod{\pi^2 - t\pi + q}$ (this can be done efficiently using Lucas sequences). Then find the eigenvalue λ for π by computing $\gcd(x^2 - tx + q, x^m - 1)$. Finally, compute $a \equiv a_0' + a_1'\lambda \pmod{r}$. See Brumley and Järvinen [112].

11.3.23: Analogous to the method at the end of Section 11.3.2.

11.3.24: The first claims are immediate since $\#E(\mathbb{F}_{p^2}) = (p + 1 - t)(p + 1 + t)$. The map ψ is an endomorphism since ψ, π and ϕ^{-1} are endomorphisms (alternatively, because ψ is a morphism fixing $\mathcal{O}_{E'}$). One can directly compute that $\psi^2 = [-1]$. The formula $\psi^2 - [t]\psi + [p] = 0$ follows since π satisfies this formula and ψ is just a conjugation of π. Since $r^2 \nmid \#E'(\mathbb{F}_{p^2})$ it follows that $\psi(P) \in \langle P \rangle$ and so λ exists. The formula for λ follows from solving the simultaneous equations $\lambda^2 \equiv -1 \pmod{r}$ and $\lambda^2 - t\lambda + p \equiv 0 \pmod{r}$.

11.4.7: Let S be the set of integer k-tuples $(a_1, \ldots, a_k)$ with $0 \leq a_i < m_i$ for $1 \leq i \leq k$. Let T be the set of $(a_1, \ldots, a_k) \in S$ in such that the value of equation (11.2) is 1. Then $\prod_i g_i^{a_i} = \prod_i g_i^{b_i}$ if and only if the vector with entries $a_i - b_i \pmod{m_i}$ for $1 \leq i \leq k$ lies in T. It follows that $\#G = \#S/\#T$ and that the method samples uniformly from the group G.

11.4.9: A simple solution is to choose $a, b \in \mathbb{F}_q$ uniformly at random and reject if $a^2 - ab + b^2 = 1$. This happens with probability roughly $1/q$. One can then use the

decompress map to obtain an element of $G_{6,q}$. This process misses several points in $G_{6,q}$, such as the element 1 and the element θ^2 of order 3 (which corresponds to the point $(0,0,0)$ not appearing in the image of the map g in Example 6.4.4).

11.4.10: The expected number of trials to get a soluble quadratic equation is roughly 2 (precisely, there are at least $(q-2\sqrt{q})/2$ values for x_0 such that $y^2+H(x_0)y-F(x_0)$ is a square in $\mathbb{F}_q$ and so the probability to be successful is at least $(q-2\sqrt{q})/(2q) \approx 1/2$). One solves the quadratic equation either by computing square roots using Exercise 2.14.3 (expected complexity of $O(\log(q)^2 M(\log(q)))$ bit operations) or, in the case of characteristic 2, by Lemma 2.14.8 (complexity $O(\log(q)^3)$ bit operations). The goto statement in line 14 occurs with probability at most $\frac{1}{2}\frac{3}{q} < \frac{1}{2}$ and so the expected number of repeats is less than 2. Hence, the algorithm for finding random points on elliptic curves has expected complexity $O(\log(q)^4)$ bit operations.

11.4.12: See Section 5 of Shallue and van de Woestijne [545].

11.4.13: The first claim is checked by an elementary calculation. For the second claim equate $y - ux = v = (3A - u^4)/(6u)$ and compute the roots in $\mathbb{F}_q$ of the polynomial $6u(y - ux) - (3A - u^4)$.

11.4.17: Set $l' = l/n$ and use the method of Example 11.4.2 n times with l'-bit strings.

11.5.2: When the algorithm ends, the points P and Q generate the subgroup of $E(\mathbb{F}_q)$ of order N_0. One simply adds to P a point R of order N_1 (found using an analogue of Algorithm 5).

11.5.3: If the group is cyclic then the probability that a random element is a generator is $\varphi(l^e)/l^e = 1 - 1/l$. Hence, the probability that among two elements at least one of them is a generator is $1 - (1 - (1 - 1/l))^2 = 1 - 1/l^2$.

If the group is not cyclic, suppose its structure is $(\mathbb{Z}/l^f\mathbb{Z}) \times (\mathbb{Z}/l^{e-f}\mathbb{Z})$ where $1 \leq f \leq e - f$. Consider the projection of points $\{P, Q\}$ to elements $\{(p_1, p_2), (q_1, q_2)\}$ of this group. The points generate $E(\mathbb{F}_q)[l^e]$ if and only if the vectors $\{(p_1, p_2), (q_1, q_2)\}$ are a basis for the vector space $(\mathbb{Z}/l\mathbb{Z})^2$. Hence, one needs the first vector to be non-zero (this occurs with probability $1-1/l^2$) and the second vector to not lie on the line corresponding to the first vector (this occurs with probability $1 - 1/l$).

The probability of success overall is therefore the product for all primes l_i, which gives the stated formula. Finally, $\varphi(N_0)/N_0 > 1/(3\log(\log(N_0))) = O(1/\log(\log(q)))$ and

$$\prod_{l|N_0} \left(1 - \tfrac{1}{l^2}\right) > \prod_{l} \left(1 - \tfrac{1}{l^2}\right) = \zeta(2)^{-1} = 6/\pi^2 = O(1)$$

where the second product is over all primes l. Hence one expects $O(\log(\log(q)))$ iterations overall.

For generalisations and more detail see Section 6.1 of Miller [429].

11.6.2: Use point halving to attempt $r - 1$ halvings and then check whether the point can be halved further over $\mathbb{F}_q$ (this is only possible if the original point has odd order).

11.7.2: First, we know that $\mathrm{Tr}(x_P) = \mathrm{Tr}(a_2) = 0$. We may assume that $x_P \neq 0$ and so

$$(y_P/x_P)^2 + (y_P/x_P) = x_P + a_2 + a_6/x_P^2.$$

Hence, $\mathrm{Tr}(a_6/x_P^2) = 0$ and so $\mathrm{Tr}(\sqrt{a_6}/x_P) = 0$. It is immediate that $(0, \sqrt{a_6})$ has order 2, and since $\mathrm{Tr}(0) = 0$ it follows that it can be halved in $E(\mathbb{F}_{2^n})$. The statement about $(x_P, y_P) + (0, \sqrt{a_6})$ follows from the formulae for the group law. Since (x_P, y_P) and $(0, \sqrt{a_6})$ can both be halved, their sum can also be halved; this also follows directly since $\mathrm{Tr}(\sqrt{a_6}/x_P) = 0$.

The receiver gets an $n - 1$ bit string representing either x_P or $\sqrt{a_6}/x_P$. The receiver then computes the corresponding value $z \in \{x_P, \sqrt{a_6}/x_P\}$. One can verify that, in both

cases, $\mathrm{Tr}(z + a_2 + a_6/z^2) = 0$. Hence, one can solve $u^2 + u = z + a_2 + a_6/z^2$ for $u \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}(u) = 0$. If $z = x_P$ then u is y_P/x_P. If $z = \sqrt{a_6}/x_P$ then u is

$$\frac{y_P}{x_P} + \frac{\sqrt{a_6}}{x_P} + x_P + 1,$$

which does satisfy $\mathrm{Tr}(u) = 0$. In both cases, one determines the corresponding value y as $y = uz$.

It remains to determine the two cases. Suppose $2^i \| \#E(\mathbb{F}_{2^n})$. Then P can be halved at least i times while $(0, \sqrt{a_6})$ can only be halved $i-1$ times. It follows that $P + (0, \sqrt{a_6})$ can only be halved $i-1$ times. Hence, if one can repeatedly halve (z, y) at least i times then set $x_P = z$ and $y_P = x_P u$. Otherwise, set $x_P = \sqrt{a_6}/z$ and solve for y_P subject to $\mathrm{Tr}(y_P/x_P) = 1$. For further discussion see King [339].

11.7.3: Use action of 2-power Frobenius on x_P (represented using a normal basis) so that the least significant bits are a predictable bit pattern (for example, the longest run of ones followed by a zero). Since the expected length of the longest run of ones is roughly $\log_2(n)$ one can expect to save this many bits. One can also combine this method with the Seroussi trick of Example 11.7.1. For details see Eagle, Galbraith and Ong [188].

Chapter 12: Primality Testing and Integer Factorisation using Algebraic Groups

12.1.4: See Section 3.6 of Crandall and Pomerance [162].

12.1.5: (Gordon [262]) Let $E : y^2 = x^3 + x$ which has $N + 1$ points over $\mathbb{Z}/N\mathbb{Z}$ when N is prime. So choose a random point $P \in E(\mathbb{Z}/N\mathbb{Z})$ (by choosing a random x and computing $y = \sqrt{x^3 + x}$ using the Tonelli-Shanks algorithm) and compute $[N + 1]P$ and see if it is $\mathcal{O}_E$. If anything goes wrong then N is not prime.

12.1.6: If N is prime then the elliptic curve $E : y^2 = x^3 + a_4 x$ has $N + 1 \pm 2a$ points for some integer a such that $p = a^2 + b^2$ (there are four possible group orders); see Example 9.10.20. Hence, given N one can run the Cornacchia algorithm to compute a and b, choose a random point $P \in E(\mathbb{Z}/N\mathbb{N})$, and test whether $[N + 1 \pm 2a]P = \mathcal{O}_E$; if anything goes wrong then one deduces that N is composite.

12.1.8: Since $N - 1 = 2^4 \cdot 35$ the Miller-Rabin sequence for the base 2 is

$$263, \ \ 166, \ \ 67, \ \ 1, \ \ 1.$$

The fact that $67 \not\equiv -1 \pmod{561}$ implies that 561 is composite.

Indeed, the non-trivial solution to $x^2 \equiv 1 \pmod{N}$ leads to a partial factorisation of N via $x^2 - 1 = (x + 1)(x - 1) \equiv 0 \pmod{N}$. In this case, $\gcd(67 - 1, 561) = 33$. Unfortunately the Miller-Rabin test is not a good factoring algorithm since the condition $a^{N-1} \not\equiv 1 \pmod{N}$ is usually not satisfied.

12.2.4: Choose q, then find x_0 such that $\Phi_k(x_0) \equiv 0 \pmod{q}$, then choose $p = x_0 + lq$ for suitable l. See Section 3.1 of Lenstra and Verheul [375].

12.2.5: A solution is Gordon's algorithm; see Algorithm 4.53 of [418].

12.2.7: Theorem 4.1.1 of [162].

12.2.9: Theorem 4.1.3 of [162].

12.2.10: Generate a random prime q together with certificate (using, for example, Maurer's algorithm [403]) and determine if $p = 2q + 1$ is prime. It is easy to form a certificate for p.

12.3.6: Since there are $B/\log(B)$ primes we can save a $\log(B)$ term as long as one can find the next prime in $O(\log(B)M(\log(N)))$ bit operations; in practice this is easily done (e.g., using a sieve or Miller-Rabin).

12.3.7: List the primes $B < Q_1 < Q_2 < \cdots < Q_k \leq B$ and use the fact that $b^{Q_{i+1}} \equiv b^{Q_i} b^{Q_{i+1}-Q_i} \pmod{N}$. One precomputes all the increments $b^{Q_{i+1}-Q_i} \pmod{N}$.

12.3.8: Apply Theorem 2.16.1.

12.3.9: See Williams [634] (note that he credits Guy and Conway for the suggestion).

12.5.1: Exercise 2.2.9 showed that one can determine if N is a prime power (and factor it) in polynomial time. So suppose N has at least two distinct prime factors. If $p^2 \mid N$ then either $p < N^{1/3}$ or $N/p^2 < N^{1/3}$. Use the Pollard-Strassen method with $B = \lceil N^{1/6} \rceil$ to find all prime factors of N that are less than $N^{1/3}$ in $\tilde{O}(N^{1/6})$ bit operations. Then test whether the remaining unfactored part of N is a perfect power.

Chapter 13: Basic Discrete Logarithm Algorithms

13.0.3: Split N using Miller-Rabin style idea once know order of random g modulo N.

13.2.7: First show, using calculus, that $f(x) = x/\log_2(x)$ is monotonically increasing for $x \geq 2.7183$. Hence deduce that if $B \geq 4$ and $2 \leq x \leq B$ then $x \leq B \log_2(x)/\log_2(B)$. Finally, prove the result using induction on n.

13.3.3: Set $m = \lceil \sqrt{r/2} \rceil$ and loop giant steps up to $\lceil \sqrt{2r} \rceil$.

13.3.4: Let X be the random variable $\max\{x, y\}$ over $(x, y) \in [0, r]^2$. If $0 \leq t \leq r$ then $\Pr(X \leq t)$ is the area of the box $[0, t]^2$ divided by the area of $[0, r]^2$, i.e., t^2/r^2. Hence, $\Pr(X > t) = 1 - t^2/r^2$ and the expected value of X is $\sum_{t=0}^{r} \Pr(X > t) \approx \int_0^r (1 - t^2/r^2) dt = 2r/3$. Hence, choosing both tables to have size $\sqrt{r}$ gives an algorithm with average-case running time $2\frac{2}{3}\sqrt{r}$ group operations and which requires storing the same number of group elements. See Section 3 of Pollard [488].

13.3.6: It is convenient to replace h by hg^{-b} so that $h = g^a$ with $0 \leq a < w$. Then set $m = \lceil \sqrt{w/2} \rceil$ and run Algorithm 14 with trivial modifications (the while loop now runs to $2m$).

13.3.7: Let $m = \lceil \sqrt{w}/2 \rceil$. If $h = g^a$ then write $a = a_0 + 2ma_1$ where $-m \leq a_0 \leq m$ and $0 \leq a_1 \leq 2m$. Then one needs m group operations to produce the list of baby steps g^{a_0} and, on average, $\frac{1}{2}2m = m$ group operations for the giant steps.

13.3.8: We have $a = b + ma_1$ for some integer a_1 in the range $0 \leq a_1 < w/m$. Let $h_1 = hg^{-b}$ and $g_1 = g^m$. Then $h_1 = g_1^{a_1}$. The BSGS algorithm can be used to solve this problem in $O(\sqrt{w/m})$ group operations.

13.3.9: See van Oorshot and Wiener [472].

13.3.10: One can just run BSGS twice, but a better solution is to set $m = \lceil \sqrt{2w} \rceil$, $h_1 = hg^{-b_1}$ and $h_2 = hg^{-b_2}$. One computes m baby steps as usual and then computes $m/2$ giant steps starting from h_1 and another $m/2$ giant steps starting from h_2.

13.3.11: Solve the DLP instance $1 = g^a$.

13.3.13: Blackburn and Teske [60].

13.3.14: By Exercise 11.1.15 the number of NAFS is $\approx 2^{n+2}/3$. If a is a NAF then $a = a_0 + 2^{\lceil n/2 \rceil} a_1$ where a_0 and a_1 are NAFs of length $l = \lceil n/2 \rceil$. There is an efficient procedure to list all NAFs a_0 of length l (see Exercise 11.1.16) so one can compute and store all g^{a_0} in a sorted list. This gives a BSGS algorithm requiring $O(2^{\lceil n/2 \rceil + 2}/3)$ time and space.

13.4.6: See Maurer [404].

13.5.4: Let $m = \lfloor l/2 \rfloor$. Use the equation

$$g_1^{a_1} \cdots g_m^{a_m} = h g_{m+1}^{-a_{m+1}} \cdots g_l^{-a_l}.$$

Let $N_1 = \#\mathcal{S}_1 \cdots \#\mathcal{S}_m$ and $N_2 = \#\mathcal{S}_{m+1} \cdots \#\mathcal{S}_l$. Compute and store the left hand side of the equation in time and space $O(N_1)$ then compute the right hand side and check for

a match. The running time is $O(N_1 + N_2)$ group operations and the storage is $O(N_1)$ group elements.

13.5.5: Define $\mathcal{S}_1' = \{a_1 \cdots a_{\lfloor l/2 \rfloor} : a_j \in \mathcal{S}_j \text{ for } 1 \leq j \leq l/2\}$ and $\mathcal{S}_2' = \{a_{\lfloor l/2 \rfloor + 1} \cdots a_l : a_j \in \mathcal{S}_j\}$. We assume $\#\mathcal{S}_1' \leq \#\mathcal{S}_2'$. Compute and store (g^{a_1}, a_1), sorted according to the first component, for all $a_1 \in \mathcal{S}_1'$ then compute each $h^{a_2^{-1}}$ for $a_2 \in \mathcal{S}_2'$ and check for a match with the earlier list. The running time is $O(\#\mathcal{S}_1' + \#\mathcal{S}_2')$ group operations and the storage is $O(\#\mathcal{S}_1')$ group elements.

13.6.10: Find the largest $\alpha \in \mathbb{R}$ such that $\alpha \leq 1/2$ and $M \geq \binom{\lceil \alpha n \rfloor}{\lfloor \alpha w \rfloor}$. Compute M "baby steps" and then $\binom{n - \lceil \alpha n \rfloor}{w - \lfloor \alpha w \rfloor}$ "giant steps".

13.8.2: A solution is to sort L_1 and then, for each $x_2 \in L_2$ to check whether $x_2 \in L_1$. For the "hash-join" solution see Wagner [625].

13.8.5: See Wagner [625].

13.8.7: $\mathcal{D} = \{x \in \{0,1\}^n : \mathrm{LSB}_m(x) = 0\}$.

13.8.9: See Wagner [625].

Chapter 14: Factoring and Discrete Logarithms using Pseudorandom Walks

14.1.3: By solving $e^{-l^2/2N} < p)$ for l, for probability 0.99 the number of trials needed is $\approx 3.035\sqrt{N}$ and for probability 0.999 the number of trials is $\approx 3.717\sqrt{N}$.

14.2.4: $l_t = 20, l_h = 10$, so $x_{20} \equiv x_{40} \pmod{p}$. The walk in this example is mostly squarings, which is "not very random" and which justifies why $l_t + l_h$ is so much larger than $\sqrt{\pi r/2}$.

14.2.5: $l_t = 7, l_h = 6$, so first collision is $x_{12} = x_{24}$.

14.3.3: Solving $e^{-\alpha} = 1/r$ (the probability to simply guess the correct solution to the DLP) gives $\alpha = \log(r)$.

14.2.18: On can store some bits of $H(x_n)$, where H is a hash function. A further variant is for the clients not to compute or store the values a_i and b_i. Instead, the algorithm is structured so that the values (a_0, b_0) of the initial point $x_0 = g^{a_0} h^{b_0}$ are a function of a short random "seed"; the client then sends the end-point of the walk and the seed to the server. The server then re-calculates the walk, this time including the values a_i and b_i, once a collision has been detected. We refer to Bailey et al. [25] for details.

14.2.21: Each step of the algorithm requires computing $g^{a_0} h^{b_0}$ for random $0 < a_0, b_0 < r$, which (naively) requires $3 \log_2(r)$ group operations. The cost can be reduced to around $\log_2(r)$ (and even further) with modest precomputation and storage. In any case the total cost of the algorithm would be around $1.25\sqrt{r} \log_2(r)$ group operations on average, compared with $1.41\sqrt{r}$ for baby-step-giant-step. The storage requirements are similar.

14.4.9: $x_{i+2} = (x_i g)^{-1} g = x_i^{-1}$. To have the cycle we need $S(\hat{x}_{i+1}) = S(\hat{x}_i)$ which occurs with probability $1/n_S$ and we need $\hat{x}_{i+1} = x_{i+1}^{-1}$ which occurs with probability $1/N_C$.

14.5.6: The worst case is when $h = g^a$ with $a = 0$ or $a = w - 1$. The expected cost is then $w/(2m) + m$. To minimise this take $m = \sqrt{w/2}$. The worst-case complexity is then $(2\sqrt{2} + o(1))\sqrt{w}$ group operations.

14.5.7: Mean jump size is $m \approx 5.38$. Expected length of walk is $l \approx 8.7$. Probability of success is $1 - (1 - 1/m)^l \approx 0.83 \approx 5/6$. See Pollard [488].

14.5.9: The algorithm doesn't really change. Let d be the expected distance of the wild kangaroo from the center of the interval (for the uniform distribution on $\{0, 1, \ldots, w-1\}$ we had $d = w/4$. Then the expected running time is $d/m + 4(1+\epsilon)m/N_P^2 + 1/\theta$ group operations. The optimal value for m is $N_P\sqrt{d}/2$, giving an average-case expected running time $4(1+\epsilon)\sqrt{d}/N_P + 1/\theta$ group operations.

14.5.10: If $w \geq \pi r/8 \approx 0.4r$ then one should use the rho algorithm. If w is significantly smaller than $0.4r$ then one would use the kangaroo method. Determining the exact crossover would require careful experimentation.

14.5.12: See Galbraith, Pollard and Ruprai [226].

14.6.3: The heuristic cost is $w/(2m) + 4m/N_P^2$, which is minimised by $m = N_P\sqrt{w/8}$.

14.7.6: We always have $\#(T \cap W) = r$ where $r = \#G$. The heuristic complexity is therefore $(1 + o(1))\sqrt{\pi r} \approx (1.77 + o(1))\sqrt{r}$ group operations, which is slower than Pollard rho.

14.7.7: See Galbraith and Ruprai [227].

14.8.1 See van Oorchot and Wiener [473].

14.9.5: $x^2 + 1$ is fast to compute and does not have any trivial fixed points or short cycles. The other suggestions have fixed points independent of $p \mid N$.

14.9.6: The idea is that $f(x)$ is now m-to-1, so the expected length of the rho is shorter (this is the same as the reason why taking $n_S > 3$ is a good idea; see the end of Section 14.2.5). For more discussion of this specific case see Brent and Pollard [99].

14.9.7: One cannot "see" a match modulo p without computing a gcd.

Chapter 15: Factoring and Discrete Logarithms in Subexponential Time

15.1.4: We have the error term like $\exp(-u(\log(u) + c\log(\log(u))))$ for a suitable function $c \geq 1$. This splits as $u^{-u}\log(u)^{-cu}$. If the second term is $u^{-f(u)}$ for some function then taking logs gives $f(u)\log(u) = cu\log(\log(u))$ and so $f(u) = cu\log(\log(u))/\log(u) = o(u)$.

15.1.7: The first 4 properties are straightforward to verify. Property 5 follows since $\log(\log(N)^m) = m\log(\log(N)) < c\log(N)^a\log(\log(N))^{1-a} = \log(L_N(a,c))$ for sufficiently large N. Property 6 follows from property 5 and property 2. To prove property 7 let $f(N) = m(\log(\log(N))/\log(N))^a$ and note that $L_n(a, f(N)) = \exp(m\log(\log(N))) = \log(N)^m$. It is easy to check that $\lim_{N\to\infty} f(N) = 0$ and so $f(N) = o(1)$. Properties 8 and 9 are easily checked.

15.1.9: Let $B = L_N(1/2, c)$ and

$$u = \log(N)/\log(B) = \log(N)/(c\sqrt{\log(N)\log(\log(N))}) = \tfrac{1}{c}\sqrt{\log(N)/\log(\log(N))}.$$

The probability of being B-smooth is therefore $\Psi(N,B)/N = u^{-u(1+o(1))}$ as $N \to \infty$. Now $\log(u) = \log(1/c) + \frac{1}{2}(\log(N)\log(N) - \log(\log(\log(N)))) = (1/2 + o(1))\log(\log(N))$. The result follows.

15.2.1: For each prime $p \mid N$ (necessarily odd) the equation $x^2 \equiv 1 \pmod{p}$ has exactly two distinct solutions modulo p. If $p^e \mid N$ for $e > 1$ then by Hensel lifting the equation $x^2 \equiv 1 \pmod{p^e}$ also has exactly 2 solutions. The result follows by the Chinese remainder theorem.

15.2.3: Some random relations are

$$\begin{aligned} 1717^2 &\equiv 2^2 \cdot 3^3 \cdot 5 \cdot 7 \pmod{N} \\ 2365^2 &\equiv 2^3 \cdot 3^2 \cdot 5 \cdot 7 \pmod{N} \\ 1757^2 &\equiv 2^7 \cdot 3^3 \pmod{N} \\ 519^2 &\equiv 2^5 \cdot 3 \cdot 5^2 \pmod{N} \end{aligned}$$

and so the relation matrix is

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 3 & 2 & 1 & 1 \\ 7 & 3 & 0 & 0 \\ 5 & 1 & 2 & 0 \end{pmatrix}.$$

Adding the first three rows modulo 2 gives the all zero vector (again, we are lucky that 5 relations are not required) and let $X = 1717 \cdot 2365 \cdot 1757 \pmod N$ and $Y = 2^6 \cdot 3^4 \cdot 5 \cdot 7 \pmod N$. Then $\gcd(X - Y, N) = 73$. One has $N = 53 \cdot 73$.

15.2.5: See Exercise 16.5 of Shoup [556].

15.2.8: First note that $(\#\mathcal{B})^2 = L_N(1/2, 1 + o(1))$ as required. For the second part, write $u = \log(N^{1/2+o(1)})/\log(B)$ and note that one expects $T_B \approx u^u$. Now,

$$u = (\tfrac{1}{2} + o(1)) \log(u)/(\tfrac{1}{2}\sqrt{\log(N)\log(\log(N))}) = (1 + o(1))\sqrt{\ln(N)/\ln(\ln(N))}.$$

Hence,

$$\log(u^u) = u \log(u) = (\tfrac{1}{2} + o(1))\sqrt{\log(N)\log\log(N)}.$$

Hence $\#\mathcal{B}T_B = O(L_N(1/2, 1 + o(1))) = L_N(1/2, 1 + o(1))$. See Section 6.1 of [162] or Section 16.4.2 of [556] for further details.

15.2.10: If $x = \sqrt{kN} + \epsilon$ then either $x^2 - kN$ or $kN - x^2$ is a positive integer $\leq 2\sqrt{kN}\epsilon$. The algorithm then proceeds the same way.

15.3.4: One expects to make $L_N(1/3, 1/(2c)+o(1))$ trials until the value x is $L_N(2/3, c)$-smooth. One can use ECM to factor the numbers (if they are smooth) in $L_p(1/2, \sqrt{2}+o(1))$ operations. Inserting $p = L_N(2/3, c)$ gives the result.

15.5.1: Let $u \in \langle g \rangle \cap G' = \{1\}$. The order of u divides r and $(p-1)/r$. Since $\gcd(r, (p-1)/r) = 1$ it follows that the order of u is 1.

15.5.2: If $r < (p-1)/r$ is large then one can efficiently generate a random element $\delta \in G'$ by choosing a random element $w \in \mathbb{F}_p^*$ and computing $\delta = w^r \pmod p$. If $r \geq (p-1)/r$ then it is better to precompute an element $g_1 \in \mathbb{F}_p^*$ of order $(p-1)/r$ and then compute $\delta = g_1^i \pmod p$ for a random value of i (one can speed this up further using a Pollard-style pseudo-random walk, which is also a good solution when r is small).

15.5.3: See Algorithm 16.1 and Lemma 16.2 of Shoup [556].

15.5.7: Let $B = L_p(1/2, c)$. By Corollary 15.1.8, $T_B = L_p(1/2, 1/(2c) + o(1))$. Hence the running time of the relation collection is $O(L_p(1/2, 2c + 1/(2c) + o(1)))$ bit operations and the running time of the linear algebra is $O(L_p(1/2, 2c + o(1)))$ bit operations. The optimal value of c is $1/2$ and the complexity is as stated.

15.5.8: Let $r^e \| (p-1)$ and let $\gamma \in F_p^*$ have order r^e. Let G' be the subgroup of order $(p-1)/r^e$. Generate relations of the form $\gamma^z \delta \pmod p$ with $1 < z < r^e$ and $\delta \in G'$. One needs a relation featuring g and a relation featuring h. The linear algebra is now modulo r^e (see Exercise 15.4 of [556]). One finds $\gamma^{Z_1} g^{Z_2} = 1$ from which it follows that $r^{e-1} \mid A$ and so $\gamma_1^{Z_1'} g^{Z_2} = 1$ with $\gamma_1 = \gamma^{r^{e-1}}$ and $Z_1' = Z_1/r^{e-1}$. One therefore compute the logarithm of g to the base γ_1 and similarly for h.

15.5.9: Once the first s relations are found only one relation is needed for each h_i, and this takes $O(u^u \#\mathcal{B} M(\log(p))) = O(L_p(1/2, c + 1/(2c) + o(1))) = O(L_p(1/2, 3/2 + o(1))$ bit operations (using trial division for the relations). With our current formulation the full linear algebra has to be repeated each time (actually, this can be avoided by using a different approach), but this only costs $O(L_p(1/2, 1 + o(1)))$ bit operations.

15.5.10: We are testing numbers of size $\sqrt{p}$ for B-smoothness so the number of trials before getting a B-smooth value for w_1 is $(u')^{u'}$ where $u' = \log(\sqrt{p})/\log(B) = \frac{1}{2}\log(p)/\log(B)$. However, since we need both w_1 and w_2 to be smooth the number of trials is $(u')^{2u'} = (u/2)^u$. For $B = L_p(1/2, c)$ it follows that $\log((u/2)^u) = u \log(u/2) \approx u \log(u)$ and so one gets the same complexity as before (but a smaller $o(1)$ term).

15.5.14: Suppose b is even. One can write the sum as $p^b/b + p^{b-1}/(b-1) + \cdots + p^{b/2}/(b/2)$ plus fewer than $2b$ terms which are all $O(p^{b/2})$. Since $p^{b-i}/(b-i) \leq p^{b-i}/(b/2) = 2p^{b-i}/b$ for $0 \leq i \leq b/2$ the first result follows.

For the approximation just note that $p^b/b + p^{b-1}/(b-1) + \cdots \approx p^b/b(1 + 1/p + 1/p^2 + \cdots) = p^b/b(1 - 1/p)$.

15.5.16: Following the discussion earlier in this section, let $b = c\sqrt{n\log(n)/\log(p)}$ and $u = n/b = \frac{1}{c}\sqrt{n\log(p)/\log(n)}$. Then $\#\mathcal{B} < p^b$ and so $\#\mathcal{B} = O(L_{p^n}(1/2, c))$. Now

$$\begin{aligned}\log(u^u) = u\log(u) &= \tfrac{1}{c}\sqrt{n\log(p)/\log(n)}\left(\log(1/c) + \tfrac{1}{2}(\log(n) + \log(\log(p)) - \log(\log(n))\right)\\ &= \left(\tfrac{1}{2c} + o(1)\right)\sqrt{n\log(n)\log(p)}.\end{aligned}$$

Hence $u^u = O(L_{p^n}(1/2, 1/(2c) + o(1)))$ as usual. The total running time is therefore $O(L_{p^n}(1/2, c + 1/(2c) + o(1)) + L_{p^n}(1/2, 2c + o(1)))$ bit operations. This is minimised when $2c^2 = 1$, i.e., $c = 1/\sqrt{2}$, which gives the stated complexity. We refer to Section 4 of Odlyzko [469] for more details, but note that Odlyzko writes the complexity as $O(\exp(c\sqrt{n\log(n)}) = O(L_{p^{n/\log(n)}}(1/2, c))$.

15.5.18: Note that $\mathbb{F}_{2^d} = \mathbb{F}_2[x]/(A(x))$ where $d = \deg(A(x))$. Let $\alpha \in \mathbb{F}_{2^d}$ be a root of $A(x)$. If the equation $x^2 + x = \alpha$ has no solutions then $A(x^2 + x)$ is irreducible. If the equation $x^2 + x = \alpha$ has two solutions (namely, α and $\alpha + 1$) in $\mathbb{F}_{2^d}$ then $A(x^2 + x)$ is the product of their minimal polynomials.

15.5.22: For example $F_1(t) = t^4 + t^2 + t + 1$ and $F_2(t) = t^4 + t^2$.

15.5.23: Note that $\phi_1(\psi_1(x)) = t$, $\phi_1(\psi_1(y)) = \phi_1(F_1(x)) = F_1(t)$, $\phi_2(\psi_2(x)) = \phi_2(F_1(y)) = F_2(F_1(t)) \equiv t \pmod{F(t)}$ and $\phi_2(\psi_2(y)) = \phi_2(y) = F_1(t)$.

15.6.2: Set $b = \lceil \log_q(L_{q^g}(1/2, c))\rceil$. Construct the factor base $\mathcal{B}$ as above, generate random group elements using the algorithm of Section 15.5.1 and use Theorem 15.6.1 to determine the expected number of trials to get a smooth relation. The group operations and polynomial factorisation are all polynomial-time and can be ignored. The algorithm therefore has the usual complexity $\#\mathcal{B}L_{q^g}(1/2, 1/(2c) + o(1)) + (\#\mathcal{B})^{2+o(1)}$ which is $L_{q^g}(1/2, c + 1/(2c) + o(1)) + L_{q^g}(1/2, 2c + o(1))$ when g is sufficiently large. This is optimised by taking $c = 1/\sqrt{2}$, giving the stated running time. For the technical details see Enge and Gaudry [195] or Section VII.6.1 of [65].

15.6.3: See page 36 of Adleman, DeMarrais and Huang [4] for the case of one point at infinity.

15.6.4: Clearly degree 1 prime divisors are points and $\#C(\mathbb{F}_q) = q + 1 + t$ where $|t| \leq 2g\sqrt{q} = o(q)$. As we know, there are approximately q^g divisor classes and $\binom{\#C(\mathbb{F}_q)+g-1}{g} = \binom{q(1+o(1))+g-1}{g} = q^g(1 + o(1))/g!$ divisors formed by taking sums of prime divisors of degree 1 (and subtracting a suitable divisor at infinity to get a degree 0 divisor).

For hyperelliptic curves with a single point at infinity, Lemma 10.3.24 shows the Mumford representation is unique and the above argument therefore proves the result. However, for general hyperelliptic curves uniqueness does not necessarily hold and so this argument needs some care. To deal with this one uses the fact that there are $\#\mathrm{Pic}^0_{\mathbb{F}_q}(C) = q^g(1 + o(1))$ divisor classes and hence only $o(q^g)$ divisor classes contain more than one reduced divisor. It follows that only $o(q^g)$ sums of g points in $C(\mathbb{F}_q)$ can yield divisor classes containing more that one reduced divisor, and so the above arguments do prove what is required.

15.6.5: See [242] or Section VII.6.2 of [65].

15.8.3: One can easily check all three properties for $n = 2$. The case $n = 3$ follows directly from the group law: if $x_1 \neq x_2$, then $x_1 + x_2 + x_3 = \lambda^2$ where $\lambda = (y_2 - y_1)/(x_2 - x_1)$. Expanding gives $2y_1y_2 = y_1^2 + y_2^2 + (x_2 - x_1)(x_1 + x_2 + x_3)$; squaring both sides and substituting $x_i^3 + a_4x_i + a_6$ for y_i^2 gives $(x_1 - x_2)^2$ times the stated equation. The case $x_1 = x_2$ follows by using $\lambda = (3x_1^2 + a_4)/(2y_1)$.

The general case follows since $P_1 + \cdots + P_n = \mathcal{O}_E$ if and only if $P_1 + \cdots + P_{n-2} = -R$ and $P_{n-1} + P_n = R$ for some point R on the curve. In other words, $P_1 + \cdots + P_{n-2} + R =$

$P_{n-1} + P_n + (-R)) = \mathcal{O}_E$. The symmetry is obvious, and the statement about degrees follows by induction and using the fact that the resultant of a quadratic and a degree 2^{n-2} polynomial is a degree 2^{n-1} polynomial.

Chapter 16: Lattices

16.1.4: A hint for last part is that the lattice contains the sublattice with basis $M\underline{e}_i$

16.1.13: $\underline{b}_1 = (1, 1)$ has volume $\sqrt{2}$.

16.2.5: (You need to have studied the proof of Theorem 16.2.3.) A radius $r = \lambda_1 + \epsilon$ hypercube around the origin has volume $(2r)^n$. Taking $\epsilon > 0$ arbitrarily small gives the result. For the second claim, consider the convex region $\{\underline{v} \in \mathbb{R}^n : \|\underline{v}\|_1 \leq r\}$, which is a hyper-tetrahedron of volume $2^n r^n/n!$. The approximation is using Stirling's formula.

16.2.6: Consider the lattice basis $\{(1, a), (0, b)\}$ of rank $n = 2$ and determinant b. Every element of the lattice is of the form $(s, as + bt)$ for some $s, t \in \mathbb{Z}$. By Minkowski, the disk of radius $u = \sqrt{b\sqrt{2}}$ has volume $\pi u^2 > 4b$ and so contains a non-zero lattice point. Hence, $0 < s^2 + r^2 < u^2 = \sqrt{2}b$.

16.3.1: Problem 1 is achieved by solving $\underline{x}B = \underline{v}$ over $\mathbb{Q}$ (or with sufficiently accurate floating point arithmetic, rounding to the nearest integer solution and then checking).

To solve problem 2, compute the HNF of the matrix B whose rows are $\underline{b}_1, \ldots, \underline{b}_n$ and discard the zero rows. For problem 3, write $A' = UA$ be the HNF of A. If the first r rows of A' are zero then the first r rows of U are a basis for $\ker(A)$ (since if $\underline{x}$ is any vector with last $m - r$ entries zero then $0 = \underline{x}A' = (\underline{x}U)A$).

To solve problem 4, concatenate the n rows of the $n \times n$ matrix MI_n to the matrix A to apply an extended matrix A'. Then use the method used to solve problem 3 on the matrix A'. To see this is correct note that $(x_1, \ldots, x_m)A \equiv \underline{0} \pmod{M}$ if and only if there are n integers $x_{n+1}, \ldots, x_{n+m}$ such that then $(x_1, \ldots, x_{n+m})A' = \underline{0}$.

Chapter 17: Lattice Basis Reduction

17.1.6: Clearly each change of basis is invertible and so the output is a basis of the lattice. Since $B_1 \in \mathbb{N}$ is strictly decreasing the algorithm must terminate after a finite number of steps.

17.1.8: $\{(-1, 0), (0, 2)\}$.

17.2.5: Yes, no, yes, no, yes.

17.2.7: An example is $\underline{b}_1 = (1, 0)$ and $\underline{b}_2 = (0.49, 0.8)$.

17.2.10: The proof closely follows the proof of Lemma 17.2.8. For part 2 one should find $\|\underline{b}_i\|^2 \leq (1 + \frac{1}{4}\sum_{k=1}^{i-1} \sqrt{2}^k)B_i \approx (0.146 + \sqrt{2}^i/1.46)B_i$ and one gets the result. Since $1/6 \leq (\sqrt{2} - 1)2^{(i-1)/2}$ for $i \geq 1$ one has $\|\underline{b}_j\|^2 \leq 2^{j/2}B_j$ and part 3 follows.

17.2.16: An example of the situation $\|\underline{v}_1\| \neq \|\underline{b}_1\|$ was seen in Exercise 17.2.5. For the second part, we have $2^{n(n-1)/4} \det(L) \geq \prod_{j=1}^{n} \|\underline{v}_j\| \geq \|\underline{v}_i\|^{n+1-i}$.

17.4.4: See [373] or Section 2.6.1 of [136].

17.5.2: Let L be any lattice of dimension n. We have proved than an LLL-reduced basis for L exists. Hence, by part 5 of Theorem 17.2.12 $\lambda_1 \leq 2^{(n-1)/4} \det(L)^{1/n}$. Also see Section 12.2 of Cassels [121].

Chapter 18: Algorithms for the Closest and Shortest Vector Problem:

18.1.9: The complexity of computing the Gram-Schmidt basis is given by Theorem 17.3.4. Using the same techniques, one can show that $\underline{w}_i$ can be represented using exact $\mathbb{Q}$-arithmetic with denominators bounded by X^{n-1} and numerator bounded by X^n.

18.1.10: The inductive process uses the fact that the orthogonal complement of $\underline{b}_n$ is the span of $\{\underline{b}_1^*, \ldots, \underline{b}_{n-1}^*\}$. If one starts at $\underline{b}_1$ instead of $\underline{b}_n$ then one needs an analogue of Lemma 18.1.1.

18.2.5: If $\underline{w} = \sum_{i=1}^n l_i \underline{b}_i$ and $\underline{u} = \sum_{i=1}^n l_i' \underline{b}_i$ then $\|\underline{w} - \underline{u}\|^2 = \sum_{i=1}^n (l_i - l_i')^2 \|\underline{b}_i\|^2$. The result follows.

18.2.7: $\underline{w} \approx 24.09\underline{b}_1 + 12.06\underline{b}_2 + 26.89\underline{b}_3$ so $\underline{v} = (99, 204, 306)$ and $\|\underline{v} - \underline{w}\| = \|(1, 1, -1)\| = \sqrt{3}$.

18.3.4: $(100, 77, 104)$.

18.4.5: See Figure 1 of Hanrot and Stehlé [275] or Algorithm 10.6 of Joux [317].

18.4.7: See Section 3 (under "Combinatorial methods") of Micciancio and Regev [423].

Chapter 19: Coppersmith's Method and Related Applications

19.1.8: The dimension is $2d$, the determinant is $M^d X^{2d(2d-1)/2}$, the condition (ignoring the constants) $(M^d X^{2d(2d-1)/2})^{1/2d} \leq M$ leads to $X \approx M^{1/(2d-1)}$. See Section 2 of Coppersmith [142].

19.1.14: Set $x_0 = px$ for $x \in \mathbb{Z}$. There is a similar example in Section 3 of Coppersmith [142].

19.4.5: See Section 3.2 of May [410] (pages 34-36).

19.4.6: Set $\epsilon = 1/\log_2(N)$ and apply Theorem 19.4.2 a constant number of times, each with a different guess for the most-significant 2 bits of $p - \tilde{p}$.

19.4.7: Guess all $N^{1/4}$ values for $\tilde{p}$ and try Coppersmith's algorithm (in polynomial-time) on each of them.

19.4.8: Just use $F(x) = (\tilde{p} + x)$ as before and note that the proof of Theorem 19.4.2 does not change. This is mentioned on page 52 of Howgrave-Graham [297].

19.4.9: Assume that $0 \leq \tilde{p} < M$. It follows that $Mx + \tilde{p}$ has a small root modulo p. Hence apply the same methods using the polynomial $F(x) = Mx + \tilde{p}$, which can be made monic as $F(x) = x + (\tilde{p}M^{-1}) \pmod{N}$.

19.4.10: Let $p = \tilde{p} + x_0$ with $0 \leq x_0 < X$ then setting

$$\tilde{q} = \lfloor N/(\tilde{p} + X) \rfloor$$

means $\tilde{q} \leq q \leq N/\tilde{p}$, which is an interval of width $NX/(\tilde{p}(\tilde{p} + X)) < qX/\tilde{p}$. Hence $q = \tilde{q} + y_0$ with $0 \leq y_0 \leq q(X/\tilde{p})$.

19.4.12: Let $\tilde{p} = 5000$ and $X = 10$. We seek a small root of $F(x) = (\tilde{p} + x)^3$ modulo a large factor of N. Reducing the matrix

$$\begin{pmatrix} N & 0 & 0 & 0 & 0 \\ 0 & NX & 0 & 0 & 0 \\ 0 & 0 & NX^2 & 0 & 0 \\ \tilde{p}^3 & 3\tilde{p}^2 X & 3\tilde{p}X^2 & X^3 & 0 \\ 0 & \tilde{p}^3 X & 3\tilde{p}^2 X^2 & 3\tilde{p}X^3 & X^4 \end{pmatrix}$$

yields the row $(1980391527, -16046759730, 20944500000, 35123963000, 35110000)$. This corresponds to the polynomial $3511x^4 + 35123963x^3 + 209445000x^2 - 1604675973x + 1980391527$, which has the root $x = 3$, giving $p = 5003$.

19.4.14: The algorithm requires $O(\binom{n}{e} \log(P)^3)$ bit operations, and at least $\binom{n}{e} > (n/e)^e$ bit operations. The input size is $O(n \log(p_n))$ bits (assuming all $0 \leq r_i < p_i$). The algorithm is not polynomial-time: a polynomial-time algorithm would need $\leq (n \log(p_n))^c$ bit operations for some constant c, and so the logarithm of the running time would be

$\leq c(\log(n)+\log\log(p_n))$; whereas if $e>\log(n)$ then the logarithm of the running time of the algorithm is $\geq \log((n/e)^e) > \log(n)^2 - \log(n)\log\log(n)$.

19.4.16: $p_n \approx n\log(n)$ so $P > n! > (n/e)^n$ (warning: the e here is 2.71828... from Stirling's formula) and so $\log(P) > n(\log(n)-1)$. Then $\sqrt{\log(X)/\log(P)}\log(p_n) \approx \sqrt{\log(X)/(n\log(n))}\log(n) = \sqrt{\log(X)\log(n)/n}$. The claimed value for e follows. This is obviously $>\log(n)$ for large n and sufficiently small X.

19.4.17: Let $m = \lceil \log_2(U) \rceil$. Then $2^m \leq U < 2^{m+1}$ and $2^{m+1} \leq 2U \leq V$.

19.4.19: For the first case we get $x = -347641$ and for the second $x = 512$.

19.5.2: Given q let $p_i = \lfloor q\alpha_i \rceil$ so that $|q\alpha_i - p_i| \leq 1/2$.

19.5.4: The first row output by LLL on the matrix is approximately $(-0.0000225, 0.0002499, 0.0002499, 0.000750$
Now compute $q = 0.0000225Q/\epsilon = 2250$. One finds $p_1 = 3499, p_2 = 1735$, $p_3 = 750$.

19.6.1: Note that $\frac{1}{2}b^{1/3} < q_b < b^{1/3}$ and so $|y| < \frac{1}{2}q_b$ as required. Also, note that the continued fraction method finds q_a/q_b as long as $|(\tilde{a}/\tilde{b}) - (q_a/q_b)| < 1/(2q_b^2)$. First note that $b^{-1/3} < 1/q_b < 2b^{-1/3}$ so $\frac{1}{2}b^{-2/3} < 1/(2q_b^2)$. Now, the difference $(\tilde{a}/\tilde{b}) - (q_a/q_b)$ is given by equation (19.6), whose numerator is bounded by $2\frac{1}{2}b^{1/3}\frac{1}{4}b^{1/3}$. Since $1/q_b < 2b^{-1/3}$ we have the difference bounded by $\frac{1}{2}b^{1/3}/\tilde{b}$. It follows that the difference is less than $1/(2q_b^2)$ as required and so Euclid solves the problem.

19.6.2: If $\alpha < \beta$ then the target gcd is smaller than the errors – one therefore expects very many solutions.

The first condition comes from the Diophantine approximation step: Namely that the right hand side of equation (19.6) (which is $1/\tilde{b}^{1-\beta}$) is at most $1/(2q_b^2) \approx 1/\tilde{b}^{2(1-\alpha)}$. The second condition comes from the requirement that $|y| < \frac{1}{2}q_b$.

19.6.3: The process is the same as the generalisation of Diophantine approximation in Section 19.5. The lattice is $\begin{pmatrix} \tilde{b}^\beta & \tilde{b} \\ 0 & \tilde{a} \end{pmatrix}$ which has determinant roughly $\tilde{b}^{1+\beta}$ and a short vector $(q_a\tilde{b}^\beta, q_b x - q_a y)$ of length roughly $\tilde{b}^{1+\beta-\alpha}$. The result follows.

19.7.4: See [496] for the first reduction. The second is almost immediate, but needs some care.

Chapter 19a: Cryptosystems Based on Lattices

19.9.1: Given a ciphertext $\underline{c}$ one can check if it is an encryption of $\underline{m}$ by testing whether $\underline{c} - \underline{m}G'$ (respectively, $\underline{c} - \underline{m}B'$) is a valid error vector for the system.

19.9.2: Check if $\underline{c}$ is an encryption of $\underline{m}$ by testing if $\underline{c}-\underline{m}$ lies in the code (respectively, lattice) corresponding to the public key.

19.9.3: Given $\underline{c}$ add $\underline{m}'G'$ (respectively, $\underline{m}'B'$) to get a ciphertext $\underline{c}' \neq \underline{c}$ which is an encryption of $\underline{m}+\underline{m}'$. Alternatively, add an extremely small error vector $\underline{e}'$ to get $\underline{c}'$ and call the decryption oracle; hopefully this will return the message $\underline{m}$.

19.9.8: $(2,3)$.

19.9.9: Set $\underline{w} = \underline{v}$ and, for $i = n$ downto 1 do $\underline{w} = \underline{w} - \lfloor \langle \underline{w}, \underline{b}_i^* \rangle / \langle \underline{b}_i^*, \underline{b}_i^* \rangle \rfloor$.

19.10.3: $\underline{m} = (1,2,0), \underline{e} = (1,1,1)$; $\underline{m} = (-1,0,1), \underline{e} = (1,-1,1)$.

19.13.2: There is a solution $s = \sum_{i=1}^n x_i b_i$ if and only if $s' = s - x_n b_n$ is a subset sum of $\{b_1, \ldots, b_{n-1}\}$.

19.13.3: Assume n even. Compute all $2^{n/2}$ integers $\sum_{i=1}^{n/2} x_i b_i$ for $x_i \in \{0,1\}$ and store in a sorted list, binary tree or hash table. Then compute all $2^{n/2}$ values $s - \sum_{i=n/2+1}^n x_i b_i$ and determine whether or not it appears in the list. For details see Algorithm 3.94 of [418].

19.13.4: Just divide everything by the gcd.

19.13.7: Given $s = 112$ we just subtract the largest possible element, in this case 80, which leaves $112 - 80 = 32$. We then subtract the largest element less than 32 to get

$32-20=12$. We then take $12-7=5$. Hence, we have computed that $112=5+7+20+80$, which is the solution vector $(0,1,1,1,0,1,0)$.

19.13.10: $n/(n-1)=1+1/(n-1)$.

19.13.11: $8/\log_2(430)\approx 0.9145$.

19.13.12: By Exercise 19.13.8 $b_n \geq 2^{n-1}$ and so the density is at most $n/(n-1) = 1+1/(n-1)$.

19.13.15: 0110010.

19.13.16: 0.782

19.13.17: $(154,184,43,69,125,62)$, $c=384$.

19.13.18: Encryption is deterministic.

19.13.19: Given a ciphertext c one can call $c+a_1$ and $c-a_1$ to the decryption oracle. One of them is a valid ciphertext and corresponds to the original message with the first bit flipped.

19.13.21: Since $0<a_i<M$ we expect an average ciphertext to be a sum of around $n/2$ integers of size $M/2$. Hence $c\approx nM/4$ on average (and, in all cases, $0\leq c<nM$). Since $M\geq 2^n$ we expect c to require at least $\log_2(nM/4)>\log_2(n)+n-2$ bits.

19.13.22: Take $b_i=2^{i-1}$ for $1\leq i\leq n$, $M=2^n+1$ and any W such that $Wb_i\not\equiv 2^n \pmod M$ for all i. Then the density is >1. Of course, it is easy to compute the private key corresponding to such a public key.

19.13.24: Since the integers $a_{i,j}$ are like random integers modulo M_i we expect $\sum_{j=1}^n a_{i,j}\approx nM_i/2$ and so $M_{i+1}>nM_i/2$. Hence, $M_t>(n/2)^tM_1\geq (n/2)^t2^n$. The ciphertext is expected to be a sum of around $n/2$ integers of size $M_t/2$ and so around $nM_t/4$. Therefore, on average,

$$\log_2(c)=\log_2(n(n/2)^tM_1/4)>\log_2(n)+t(\log_2(n)-1)+n-2.$$

Since the $a_{t,i}$ are somewhat like randomly chosen integers modulo M_t we expect to have $\max\{a_{t,i}\}\approx M_t$. We conservatively assume in what follows that, on average, $\max\{a_{t,i}\}>M_t/2$. Hence the density is at most $n/\log_2(M_t/2)<n/(t(\log_2(n)-1)+n-1)$. For example, $n=200$ and $t=5$ gives expected density less than 0.87; in any case, the density of an iterated Merkle-Hellman knapsack is always significantly less than 1.

19.13.25: From Exercise 19.13.8 we have $b_n>2^{n-2}b_1$ and so $M>(2^{n-2}+\cdots+2+1+1)b_1=2^{n-1}b_1$. So $b_1b_2>M>2^{n-1}b_1$ implies $b_2>2^{n-1}$. Exercise 19.13.8 also shows $M>2^{n-3}b_2$ and so $M>2^{2n-4}$. Then $\log_2(nM/4)>\log_2(n)+(2n-4)-2$.

19.13.26: See if $W^{-1}a_i \pmod M$ are small and allow efficient solution to the subset sum problem using a greedy algorithm.

19.13.28: $a_1b_2-a_2b_1=7\cdot 233\cdot 37589\cdot 143197$. The only factor of size $\approx a_3$ is $M=233\cdot 37589=8758237$. This gives $W=a_1b_1^{-1} \pmod M=5236910$. One verifies that $W^{-1}a_i \pmod M$ is a superincreasing sequence.

19.13.30: Suppose W is known and assume no permutation is used. Note that there are integers k_i for $1\leq i\leq n$ such that

$$a_i=b_iW+k_iM$$

and $k_i<b_i$. So $a_1\equiv k_1M \pmod W$ and $a_2\equiv k_2M \pmod W$. Hence, writing $c=a_2a_1^{-1} \pmod W$, we have $k_1c\equiv k_2 \pmod W$. If $k_1k_2<M$ (which is plausible since $k_1k_2<b_1b_2<M$ and W is usually about the same size as M) one can apply the same methods as used in Example 19.13.29 to find (k_1,k_2) and hence M.

19.13.32: 11100001.

19.13.33: 10111100.

Chapter 20: The Diffie-Hellman Problem and Cryptographic Applications

20.2.7: Suppose $l \mid n$ is prime and write $g_1 = g^{n/l}$. Then $g^c = g^{ab}$ implies $g^{cn/l} = g^{abn/l}$ and so $(g_1, g_1^a, g_1^b, g_1^c) = (g^{n/l}, (g^a)^{n/l}, (g^b)^{n/l}, (g^c)^{n/l})$ is a valid Diffie-Hellman tuple. If $l = O(\log(n))$ then one can solve the DLP in $\langle g_1 \rangle$ (this is just Pohlig-Hellman) and hence test DDH in $\langle g_1 \rangle$. If (g, g^a, g^b, g^c) is a random tuple in G^4 then with probability $1/l$ the resulting tuple in $\langle g_1 \rangle$ is not a valid Diffie-Hellman tuple. The algorithm therefore has a noticeable advantage in Definition 20.2.4.

20.4.1: In the first case, $\mathsf{c}_2 = \mathsf{m}h^k$ and $\mathsf{c}_2' = \mathsf{m}h^{Ak+B}$. Hence, $\mathsf{c}_2^A h^B / \mathsf{c}_2' = \mathsf{m}^{A-1}$ and so one can compute m assuming that $(A-1)$ is coprime to the order of the group G. In the second case, query the decryption oracle on $(\mathsf{c}_1, \mathsf{c}_2)$ to get m and hence h^k. One can then compute $(h^k)^A h^B$ and decrypt c_2.

20.4.3: As above we can self-correct the CDH oracle to make it reliable. Once one knows g^{ax} then one can decrypt to get M. For the second part: The problem is that given the message M corresponding to the public key (g, h) and ciphertext $(\mathsf{c}_1, \mathsf{c}_2)$ one can compute $M \oplus \mathsf{c}_2 = H(g^{ax})$ but if H is hard to invert then one cannot compute g^{ax}.

20.4.6: Given $(\mathsf{c}_1, \mathsf{c}_2)$ the user returns $\mathsf{m} = \mathsf{c}_2 \mathsf{c}_1^{-a}$ so set $\mathsf{c}_1 = h^{-1}$ and c_2 arbitrary and get $h^a = \mathsf{m}\mathsf{c}_2^{-1}$. If the group contains an element h with relatively small order l then one can easily solve the DLP to get $a \pmod{l}$. If this can be repeated for sufficiently many coprime values l then a can be determined using the Chinese remainder theorem.

20.4.9: See Boneh, Joux and Nguyen [82] for the full details of this attack. The basic idea is as follows: For suitable constant c one has $\mathsf{m} = \mathsf{m}_1 \mathsf{m}_2$ where $1 \leq \mathsf{m}_i \leq c 2^{m/2+\epsilon}$ with a certain noticeable probability (for $c = 1$ [82] states the probability is at least $\log(1 + 2\epsilon)$).

20.5.2: Eve, pretending to be Bob, sends g^y (where y is known to Eve). She makes a corrupt query to Alice and, knowing g^{xy}, can compute g^{ab}. Eve can now compute a shared key with Alice, whereas Alice believes she is sharing with Bob.

Chapter 21: The Diffie-Hellman Problem

21.1.10: For both problems let the space of instances be $(G - \{1\})^2$. Given an Inverse-DH oracle A and instance (g, g^a) one has $g^{a^{-1}} = A(g^x, (g^a)^{xy})^{yx^{-1}}$ for $1 \leq x, y < r$. Given a Square-DH oracle A and instance (g, g^a) one has $g^{a^2} = (A(g^x, (g^a)^{xy})^{(xy^2)^{-1}}$.

For the self-correction: Run the non-perfect Square-DH oracle repeatedly to produce a list L which is expected to contain g^{a^2}. Then choose $0 \leq u < r$ and repeat the process on $(g, g^a g^u)$. This givies a list L' which is expected to contain $g^{(a+u)^2}$. Finally, determine whether there is a unique pair (Z, Z') in $L \times L'$ such that $Z(g^a)^{2u} g^{u^2} = Z'$, and if so return Z. The precise details are similar to Theorem 21.3.8.

21.3.9: Suppose A is correct with noticeable probability ϵ. Since the reduction makes at least $\log_2(r)$ oracle queries, the probability that the result is correct is at most $\epsilon^{\log_2(r)}$ which is negligible. Instead, one should self-correct the oracle A to obtain an oracle A' with success probability greater than $1 - 1/(4\log_2(r))$. By Theorem 21.3.8 this requires $O(\log(\log(r))/\epsilon)$ oracle queries. One can then perform the reduction of Lemma 21.1.13 using A', with success probability $\geq 1/2$.

21.1.19: For the first part, given $(g_1, g_2, g_3) = (g, g^a, g^b)$, call $O_1(g^{r_2}, g_2^{r_2}, g_3^{r_2})$ to get g^{abr_2} and call $O_2(g^{r_1}, g_2^{r_1}, g_3^{r_1})$ to get g^{abr_1}. Finally compute $s, t \in \mathbb{Z}$ such that $r_1 s + r_2 t = 1$ and then $(g^{abr_1})^s (g^{abr_2})^t = g^{ab}$ as required.

For the next part: The problem Inverse-DH is only defined when a is coprime to the group order. If $a = r_1$, as would be required in several places, then we cannot make a meaningful query to an Inverse-DH oracle. Also, in the proof of Lemma 21.1.5 then $g \notin \langle g_1 \rangle$ so a CDH oracle can't work. Indeed, Shoup has shown (Theorem 5 of [553])

that a generic algorithm for Fixed-CDH with respect to g^{r_1}, even when given a perfect Fixed-CDH oracle with respect to g, takes $\Omega(\sqrt{r_2})$ group operations.

21.1.20: For the proof, historical references and a major generalisation of such problems see [102].

21.4.12: For example, with a perfect Fixed-CDH oracle, Pohlig-Hellman only and using projective coordinates the number of oracle queries is $O(\log(r)\log\log(r))$ oracle queries and $O((l_1^2+l_2)\log(r)^2/\log(\max\{l_1,l_2\}))$ group operations.

21.4.13: We give the results only for the case of Pohlig-Hellman combined with exhaustive search. Note that not every $a \in \mathbb{F}_r$ corresponds to an element $a+b\theta$ of $G_{2,r}$, whereas every $a \in \mathbb{A}^1(\mathbb{F}_r)$ corresponds to an element of $T_2(\mathbb{F}_r)$. Hence, embedding the DLP instance into the algebraic group $G_{2,r}$ requires an expected $O(\log(r))$ oracle queries (computing Legendre symbols and taking square roots).

The group operation using the first representation requires no inversions but the group operation for the second representation requires inversions. The number of Fixed-CDH oracle queries respectively is $O(\log(r)\log\log(r))$ and $O(\log(r)^2\log\log(r))$. Hence, the first representation is better. If one has a CDH oracle then inversions are a single oracle query and so the number of oracle queries is $O(\log(r)\log\log(r))$ in both cases.

21.5.5: See Cheon [131].

21.5.9: See Brown and Gallant [111].

21.6.4: See Kaliski [327] or Fischlin and Schnorr [203].

21.6.9: Let A be a perfect oracle which, given $h=g^x$ for $x \in \{0,1,\ldots,r-1\}$ outputs $b(x)$. It suffices to show how to use A to determine the least significant bit of x. We may assume that $h \neq g^{-1}$, since if $h=g^{-1}$ then we know x. If $A(h)=1$ then $(x_1,x_0)=(0,1)$ or $(1,0)$, so $A(gh)$ determines the LSB. Similarly, if $A(h)=0$ then $(x_1,x_0)=(0,0)$ or $(1,1)$ and so $A(gh)$ determines the LSB (since $h \neq g^{-1}$ there is no carry when computing gh).

21.6.11: The integer r in binary begins as $11000\cdots$ so the highest order 2 bits of a random integer modulo r are essentially 00, 01 or 10 with probability close to 1/3 each. Hence, both predicates are 0 with probability close to 2/3.

21.6.13: Let A be an oracle such that $A(g^x)=b(x)$. Let $h=g^a$. Set $j=1$ and if $A(h)=0$ then set $l=1$, and if $A(h)=1$ then set $l=2$. Given, at step j, $(l-1)r/2^j \leq a < lr/2^j$ one calls $A(h^{2^j})$. If $A(h^{2^j})=0$ then $(2l-2)r/2^{j+1} \leq a < (2l-1)r/2^{j+1}$, otherwise, $(2l-1)r/2^{j+1} \leq a < 2lr/2^{j+1}$.

We remark that Blum and Micali [73](generalised by Long and Wigderson [393]) use Legendre symbols and square roots modulo p to show this predicate is hardcore in the group $\mathbb{F}_p^*$ when g is a primitive element (their method does not work in a prime order cyclic subgroup).

21.6.15: See Section 7 of Li, Näslund and Shparlinski [387].

21.7.4: This is the same argument as Exercise 21.6.13. One bounds α as $(l-1)p/2^j \leq \alpha < lp/2^j$ and refines (l,j) by computing $A_1(2^j \pmod p) = \mathrm{MSB}_1(\alpha 2^j \pmod p)$.

21.7.6: Use the same argument as Exercise 21.6.4. See Fischlin and Schnorr [203] for details.

21.7.13: Given a DDH instance (g,g^a,g^b,g^c) one can compute $\mathrm{MSB}_{1+\epsilon}(g^c)$ and compare with the result of the oracle. If $g^c=g^{ab}$ then the results will agree. Repeating for random self-reduced versions of the original DDH instance gives the result. We refer to Blake and Garefelakis [62]and Blake, Garefelakis and Shparlinski [63]for details and generalisation to small subgroups of $\mathbb{F}_p^*$ and to elliptic curve groups.

21.7.14: Just call $A(g,(g^a)^{2^i},g^b)$ to get the i-th bit of the representation of g^{ab}.

21.7.15: Call $A(g,g^ag^z,g^b)$ about m times for uniformly random z. Each output yields a linear equation over $\mathbb{F}_2$ in the unknown bits of g^{ab}. Solving the system of linear

equations over $\mathbb{F}_2$ gives g^{ab}.

Chapter 22: Digital Signatures Based on Discrete Logarithms

22.1.2: The second and fourth are valid transcripts (i.e., the equation (22.1) is satisfied). In the third case one even has $\mathsf{s}_0 \notin \langle g \rangle$.

22.1.3: $A\mathsf{s}_2 + B - \mathsf{s}_2' \equiv a(A\mathsf{s}_1 - \mathsf{s}_1') \pmod{r}$ which can be solved for a.

22.1.6: If s_1 can be guessed then choose any $0 \leq \mathsf{s}_2 < r$ and set $\mathsf{s}_0 = g^{\mathsf{s}_2} h^{-\mathsf{s}_1}$. Send s_0 in the first stage of the protocol and respond to the challenge s_1 with s_2.

22.1.8: We need a multi-exponentiation (in equation (22.1)) and this is not well-defined in algebraic group quotients.

22.1.11: If m is a message and $(\mathsf{s}_1, \mathsf{s}_2)$ is a signature which is valid for two distinct public keys h_A and h_B then we have

$$\mathsf{s}_1 = H(\mathsf{m} \| g^{\mathsf{s}_2} h_A^{-\mathsf{s}_1}) = H(\mathsf{m} \| g^{\mathsf{s}_2} h_B^{-\mathsf{s}_1}).$$

If $\mathsf{s}_1 = 0$ then the signature is valid for all public keys. If $\mathsf{s}_1 \neq 0$ then $h_A^{-\mathsf{s}_1} \neq g^{\mathsf{s}_2} h_B^{-\mathsf{s}_1}$ and so we have a hash collision of a very special form: namely $H(\mathsf{m} \| R_1) = H(\mathsf{m} \| R_2)$ where R_1 and R_2 are distinct elements of $\langle g \rangle$. If the bit-length of the hash output is l such that $2^l < r$ then, by the pigeonhole principle, there must be distinct $R_1, R_2 \in \langle g \rangle$ such that $H(\mathsf{m} \| R_1) = H(\mathsf{m} \| R_2)$. Indeed, one expects many such pairs if 2^l is significantly smaller than r.

Even when 2^l is significantly larger than r then, by the birthday paradox, one expects there to be a collision of the form $H(\mathsf{m} \| R_1) = H(\mathsf{m} \| R_2)$. However, if 2^l is larger than r^2 then the probability of such a collision is rather low.

As for security, the existence of two keys for which the same signature is valid on the same message is not considered to lead to any practical attack in any real-world application. In any case, it appears to be impossible to construct the actual signatures, given the hash collision $H(\mathsf{m} \| R_1) = H(\mathsf{m} \| R_2)$, without solving at least two instances of the discrete logarithm problem.

22.1.12: Change s_2 to $k - a\mathsf{s}_1 \pmod{r}$. All the security arguments are unchanged by this.

22.2.2: Write the verification equation as

$$h^{F(\mathsf{s}_1)} \mathsf{s}_1^{\mathsf{s}_2} g^{r - H(\mathsf{m})} = 1.$$

If $\gcd(\mathsf{s}_2, \#G) = 1$, and h is known to lie in $\langle g \rangle$ then this equation (together with the possibly simpler check that $\mathsf{s}_1 \in G$) implies $\mathsf{s}_1 \in \langle g \rangle$.

One sees that Verify is computing a 3-dimensional multi-exponentiation with exponents all general elements of $\mathbb{Z}/r\mathbb{Z}$ and only one base fixed. Using basic methods (i.e., not windows or signed expansions) this computation will require roughly twice the cost of the computation in Example 22.1.13. Even when using more advanced methods such as windows, the fact that s_1 is a variable base in the multi-exponentiation is always a disadvantage. An additional cost in Elgamal signature verification (also for signing) is computing a hash function whose image is $\mathbb{Z}/r\mathbb{Z}$ rather than $\{0,1\}^l$.

22.2.3: Hint: Set $\mathsf{s}_1 = g^u h$ for random $0 \leq u < r$.

Set $\mathsf{s}_1 = g^u h$ for random $0 \leq u < r$. and $\mathsf{s}_2 = -F(\mathsf{s}_1) \pmod{r}$. One checks that

$$h^{F(\mathsf{s}_1)} \mathsf{s}_1^{\mathsf{s}_2} = h^{F(\mathsf{s}_1)} g^{-uF(\mathsf{s}_1)} h^{-F(\mathsf{s}_1)} = g^{-uF(\mathsf{s}_1)}.$$

Hence, taking $\mathsf{m} = -uF(\mathsf{s}_1) \pmod{r}$ gives the existential forgery, More elaborate versions of this attack are given in Section 4.2.3 of Elgamal [192].

22.2.4: Hint: Use the Chinese remainder theorem.

Given the public key h and a message with hash $H(\mathsf{m})$ the adversary chooses a random $1 \leq \mathsf{s}_1', \mathsf{s}_2 < r$ and computes $\mathsf{s}_1'' = (g^{H(\mathsf{m})} h^{-\mathsf{s}_1'})^{\mathsf{s}_2^{-1}} \pmod p$. Now, compute an integer s_1 using the Chinese remainder theorem so that

$$\mathsf{s}_1 \equiv \mathsf{s}_1'' \pmod p \quad \text{and} \quad \mathsf{s}_1 \equiv \mathsf{s}_1' \pmod r.$$

Note that, under our assumptions, $F(\mathsf{s}_1) = \mathsf{s}_1'$ and that $\mathsf{s}_1^r \equiv 1 \pmod p$. Then $h^{F(\mathsf{s}_1)} \mathsf{s}_1^{\mathsf{s}_2} = h^{\mathsf{s}_1'} g^{H(\mathsf{m})} h^{-\mathsf{s}_1'} \equiv g^{H(\mathsf{m})} \pmod p$ as required.

22.2.6: Hint: If $\mathsf{s}_1 = ur$ for any $u \in \mathbb{N}$ then $h^{F(\mathsf{s}_1)} = 1$.

Set $\mathsf{s}_1 = ur$ where $u \in \mathbb{N}$ is such that r divides the order of s_1 modulo p (this is easy). The trick is to set

$$g = \mathsf{s}_1^{(p-1)/r} \pmod p$$

which is a generator for the subgroup of order r. Use g as part of the system parameters of the scheme. The signature forgeries will all use the same value for s_1 (actually, s_1 can be varied by multiplying s_1 by any integer of order dividing $(p-1)/r$ modulo p, as long as one always treats s_1 as an integer and does not reduce modulo p). Note that, for any public key h, we have $h^{F(\mathsf{s}_1)} = 1$. Finally, set $\mathsf{s}_2 = H(\mathsf{m})(p-1)/r \in \mathbb{N}$ so that

$$h^{F(\mathsf{s}_1)} \mathsf{s}_1^{\mathsf{s}_2} \equiv \mathsf{s}_1^{\mathsf{s}_2} \equiv g^{H(\mathsf{m})} \pmod p.$$

A nice extension of the attack, which works even when the checks on s_1 and s_2 are performed, is to choose $\mathsf{s}_1 = ur$ so that $1 < \mathsf{s}_1 < p$ and so that the order of s_1 modulo p is equal to r. One can then take $g = \mathsf{s}_1$. Though it is easy to arrange that the order of s_1 equals r, it does not seem to be easy to do this while still keeping the integer ur less than p.

More details of these attacks, and variants in the case where g is a primitive root, are given in Bleichenbacher [66].

22.2.7: Try random $\mathsf{m}_1, \mathsf{m}_2$ until $r = |H(\mathsf{m}_1) - H(\mathsf{m}_2)|$ is prime. See Vaudenay [615].

22.2.8: The signatures are all valid with probability at most $1/r$. So suppose signature j is not valid. Choose all w_i for $i \neq j$ randomly. Then there is at most a $1/(r-1)$ chance that w_j is chosen so that the equation is satisfied.

When all $h_i = h$ just replace $\prod_{i=1}^t h_i^{w_i F(\mathsf{s}_{1,i})}$ by $h^{\sum_{i=1}^t w_i F(\mathsf{s}_{1,i})}$. One can now break the equation into $t/3$ 3-dimensional multi-exponentiations, so the total cost is about $1/3$ of the naive case.

For the third part see Yen and Laih [637].

It seems to be impossible to do something similar for Schnorr signatures since each $g^{\mathsf{s}_2} h^{-\mathsf{s}_1}$ needs to be computed separately.

22.2.12: First, precompute and store $g_1 = g^{\lceil \sqrt{r} \rceil}$. Then, for each signature $(\mathsf{s}_0, \mathsf{s}_2)$ to be verified run Euclid's algorithm on inputs $u_2 = F(\mathsf{s}_0)\mathsf{s}_2^{-1} \pmod r$ and r until the current remainder is approximately $\sqrt{r}$. Write v for the resulting coefficient of u_2 (in the notation of Section 2.3 this is $v = \mathsf{s}_i$ which clashes horribly with the notation of this chapter). By part 6 of Lemma 2.3.3 it follows that $v, vu_2 \pmod r \approx \sqrt{r}$. Also, write $u_1 v \equiv w_0 + w_1 \lceil \sqrt{r} \rceil \pmod r$ with $0 \leq w_0, w_1 < \sqrt{r}$. Equation 22.6 can therefore be written as

$$g^{w_0} g_1^{w_1} h^{u_2 v} \mathsf{s}_0^{-v} = 1$$

All exponents in this 4-dimensional multi-exponentiation are of size roughly $\sqrt{r}$. For further details see Antipa et al [11]. A further improvement in [11] (assuming the public key also contains a suitable power of h) leads to a 6-dimensional multi-exponentiation with exponents of size $r^{1/3}$.

22.2.13: There is no algorithm to generate signatures!

22.2.18: For example, to check that g^{a^2} is correct one can test whether $e(g_1, g_2^{a^2}) = e(\psi(g_2^a), g_2^a)$. The other elements are tested similarly. For the second part, $e\left(g_1^{(m+a)^{-1}}, g_2^a, g_2^m\right)$ should equal z.

Chapter 23: Public Key Encryption Based on Discrete Logarithms

23.1.5: The proof proceeds almost identically to the previous case, except that when a decryption query is made then only one call to the oracle is required. This variant is studied in Section 10.4 of Cramer and Shoup [161].

23.1.7: Given a Hash-DH instance (g, g^a, g^b), if one can compute g^{ab} then one can compute $\mathsf{kdf}(g^{ab})$. Given a DDH instance (g, g^a, g^b, g^c) one can compute $K = \mathsf{kdf}(g^c)$ and, using an oracle for Hash-DH, distinguish it from $\mathsf{kdf}(g^{ab})$.

23.2.2: For the first statement note that for each $0 \leq z_1 < r$ there is a unique choice for z_2. The second statement is straightforward. For the final statement write $g_2 = g_1^w$, $h = g_1^v$ and $u_2 = g^{k'}$ with $0 \leq k' < r$ and $k' \neq k$. The fact that $(z_1, z_2) \in \mathcal{X}_{g_1,g_2,h}$ imposes the linear equation $z_1 + wz_2 \equiv v \pmod{r}$. To prove the result we need to show that one can simultaneously solve $kz_1 + k'wz_2 \equiv x \pmod{r}$ for any $0 \leq x < r$. The result follows since the determinant of the matrix $\left(\begin{smallmatrix} 1 & w \\ k & k'w \end{smallmatrix}\right)$ is not zero modulo r.

23.2.7: First has $v \notin G$, second does not satisfy equation (23.1), third has message $\mathsf{m} = 1$.

23.2.11: The adversary returns $eu_1^{-z_1}u_2^{-z_2}$ just as the Decrypt algorithm does.

23.2.12: Given a challenge ciphertext (u_1, u_2, e, v) compute $u_1' = u_1 g_1, u_2' = u_2 g_2$ and $e' = eh$ (these are g_1^{k+1}, g_2^{k+1} and $\mathsf{m}h^{k+1}$ respectively). Then compute $\alpha' = H(u_1', u_2', e')$ and set $v = (u_1')^{x_1+y_1\alpha'}(u_2')^{x_2+y_2\alpha'}$. Calling the decryption oracle on (u_1', u_2', e', v') gives m.

23.2.13: Let u_1 be a random element of $\mathbb{F}_p^*$ of order l. Set $u_2 = u_1^a$ and $v = u_1^b$ for random $1 \leq a, b < l$ and choose any $e \in \mathbb{F}_p^*$. Call the decryption oracle on (u_1, u_2, e, v). With probability $1/l$ the decryption oracle does not return $\perp$, and indeed returns some message m. One therefore has

$$u_1^{r-z_1+a(r-z_2)} = \mathsf{m}e^{-1}.$$

Since it is easy to compute the discrete logarithm of $\mathsf{m}e^{-1}$ to the base u_1 when l is small one obtains a linear equation in z_1 and z_2 modulo l. Repeating the attack and solving gives $z_1 \pmod{l}$ and $z_2 \pmod{l}$.

If $p-1$ has distinct small prime factors $l_1, \ldots, l_t$ so that $\prod_{i=1}^t l_i > r$ then, by repeating the above attack, one can determine the private key uniquely using the Chinese remainder theorem.

23.3.7: Just set $\mathsf{c}_2' = \mathsf{c}_2 \oplus s$ for some non-zero string $s \in \{0,1\}^l$ and query the decryption oracle on $(\mathsf{c}_1, \mathsf{c}_2')$ to get $\mathsf{m} \oplus s$.

23.3.8: Given $Q_{\mathsf{id}} = H_1(\mathsf{id})$ set $R = \psi(g)Q_{\mathsf{id}}$. Invert the hash function to find an identity id' such that $H_1(\mathsf{id}') = R$. Then request the private key for identity id' to receive $R' = R^s = (\psi(g)Q_{\mathsf{id}})^s$. One can obtain $Q_{\mathsf{id}}' = Q_{\mathsf{id}}^s$ as $R'\psi(g')^{-1}$.

23.3.10: If one can solve CDH in G_T then compute $z = e(Q, g)$, $z_1 = e(Q, g^a) = z^a$ and $z_2 = e(Q, g^b) = z^b$. Then the solution to the CDH instance (z, z_1, z_2) is the required value. The case of CDH in G_2 is similar.

Chapter 24: The RSA and Rabin Cryptosystems

24.1.1: Repeatedly choose random primes p such that $2^{\kappa/2-1} < p < 2^{\kappa/2}$ and let $q = \lceil u2^{\kappa-l}/p \rceil + \epsilon$ (where $\epsilon \in \mathbb{Z}_{\geq 0}$ is small, possibly just always zero) until q is prime and the top l bits of pq are equal to u.

24.1.3: Generate random primes r_2 and r_3 of the required size. Generate a random prime r_1 of the form $2r_3x + 1$ for suitably sized $x \in \mathbb{N}$. Solve $p_0 \equiv 1 \pmod{r_1}$ and $p_0 \equiv -1 \pmod{r_2}$ using the Chinese remainder theorem. Try random $y \in \mathbb{N}$ of the appropriate size until $p = p_0 + r_1r_2y$ is prime. This algorithm is due to Gordon [264].

24.1.5: See Galbraith, Heneghan and McKee [220]. For parameter restrictions see [220] and [69].

24.1.7: One finds that $\mathsf{m} \equiv 385699 \pmod{p}$ and $\mathsf{m} \equiv 344504 \pmod{q}$. Solving $(385699 + px)^3 \equiv \mathsf{c} \pmod{p^2}$ gives $x = 1177$ and $\mathsf{m} \equiv 1234567890 \pmod{p^2}$. Performing another iteration of Hensel lifting gives the same value for m, as does the CRT. Hence, $\mathsf{m} = 1234567890$.

24.1.10: Instead of computing $\mathsf{c}^{d_p} \pmod{p}$ and $\mathsf{c}^{d_q} \pmod{q}$ for two primes $p, q \approx 2^{2500}$ we compute one exponentiation where p and d_p are 1/5 the size. Hence the cost is about $\frac{1}{2}(\frac{1}{5})^{2.58} \approx 0.008$ the time.

For the attack, choose an integer $\mathsf{m} > p$ (e.g., $\mathsf{m} = 2^{600}$), compute $\mathsf{c} = \mathsf{m}^e \pmod{N}$ and then ask for c to be decrypted. On receipt of the message $1 < \mathsf{m}' < p$ one knows $\mathsf{m}^e \equiv (\mathsf{m}')^e \pmod{p}$ and so $\mathsf{m}' \equiv \mathsf{m} \pmod{p}$. Hence, $\gcd(N, \mathsf{m} - \mathsf{m}')$ yields p.

24.1.11: An adversary can choose messages m_0 and m_1 such that $(\frac{\mathsf{m}_0}{N}) = -1$ and $(\frac{\mathsf{m}_1}{N}) = 1$ and then compute the Jacobi symbol of the challenge ciphertext to decide which message was encrypted.

24.1.18: Suppose A is a perfect algorithm that, on input an RSA public key (N, e), outputs the private key d. Let $N = pq$ be an integer to be factored. Choose $1 < e < N$ uniformly at random. If $A(N, e) = \perp$ then repeat for another choice of e (in this case one knows that $\gcd(e, \varphi(N)) \neq 1$; this information is potentially useful, but we ignore it in our proof). Let $d = A(N, e)$. It follows that $ed - 1$ is a multiple of $\lambda(N)$ and so the result follows from Lemma 24.1.17.

The expected number of trials to find e coprime to $\varphi(N)$ is bounded by $O(\log(N))$ (since that is the number of trials to choose a prime value $e > \sqrt{N}$). The reduction therefore requires at most polynomially many queries to the oracle A and at most polynomially many bit operations.

24.1.19: The idea is to note that $\varphi(N) = N - (p + q) + 1$ so one can compute p and q by taking the roots of the quadratic $x^2 + (\varphi(N) - N - 1)x + N$ (which can be done deterministically using numerical analysis).

24.1.20: Let $N = pq$ where p and q are odd. We use the same ideas as Lemma 24.1.17. One chooses a random $1 < g < N$ and computes $\gcd(g, N)$ (if this is not equal to 1 then we have factored N). Use A to determine the order M of g modulo N. With probability at least 3/4 one has M even (so if M is odd then repeat for a different choice of g). Now, with probability at least 1/2, $\gcd((g^{M/2} \pmod{N}) - 1, N)$ factors N (this final argument uses careful analysis of the 2-adic valuations of $p - 1$ and $q - 1$).

24.1.24: Given a small number of message-signature pairs $(\mathsf{m}_i, \mathsf{s}_i)$ one expects to find two messages $\mathsf{m}_i, \mathsf{m}_j$ such that $\gcd(H(\mathsf{m}_i), H(\mathsf{m}_j)) = 1$ (by Theorem A.14.4, the probabilty for each pair is at least 0.6). Euclid gives integers s, t such that $sH(\mathsf{m}_i) + tH(\mathsf{m}_j) = 1$. If s_i and s_j are the corresponding signatures then

$$(\mathsf{s}_i^s \mathsf{s}_j^t)^e \equiv a \pmod{N}$$

and so an e-th root of a has been computed. One can then forge signatures for any message.

24.2.5: $\mathsf{m} = 1234567890$ in all three cases.

24.2.6: One determines b_2 by computing $(\frac{\mathsf{c}}{N})$. One then computes $\mathsf{c}' = \mathsf{c}u_2^{-b_2}$ and determines b_1 by computing $(\frac{\mathsf{c}'}{p})$.

24.2.7: The advantage is that one speeds up the square roots modulo p, q and r since the primes are smaller (see Example 24.1.4). The main disadvantage is that there are now 8 square roots, in general, to choose from.

24.2.8: There are still only four square roots (two square roots modulo p, which correspond via Hensel lifting to two square roots modulo p^r, and similarly for q). Hence, one can use exactly the same type of redundancy schemes as standard Rabin. One speeds up computing square roots by using the Chinese remainder theorem and Hensel lifting as in Example 24.1.6. Hence, there is a significant advantage of using Rabin in this way.

24.2.17: Choose random $1 < x < N$, call oracle on $(x^2 \pmod N, -(\frac{x}{N}), 0)$ to get x' and compute $\gcd(x' - x, N)$.

24.2.21: Now there are nine possible roots to choose from. Redundancy in the message can be used in this case (the other two redundancy schemes are more directly related to square roots and cannot be used in this case).

For the security, choose a random integer $1 < x < N$ that does not satisfy the redundancy scheme and compute $\mathsf{c} = x^3 \pmod N$. Suppose a decryption oracle outputs a solution x' to $(x')^3 \equiv \mathsf{c} \pmod N$ so that x' satisfies the redundancy scheme. (This happens with probability at least $(1 - 1/2^l)^7 1/2^l$.)

Now $(x')^3 - x^3 = (x' - x)((x')^2 + x'x + x^2) \equiv 0 \pmod N$. If, say, $x' \equiv x \pmod p$ and $x' \not\equiv x \pmod q$ then one can split N. This situation occurs with probability 2/9. The idea of cubing is mentioned in Rabin [494].

24.2.23: Choose random x such that $(\frac{x}{N}) = -1$ and set $y = A(x^4, x^2, x^2)$. Then $\gcd(x - y, N)$ splits N with probability 1/2. This argument is due to Shmuely [552]. For precise details see Biham, Boneh and Reingold [57].

24.2.24: Compute $\varphi(N) = 2(N + 2) - M$ and then solve a quadratic equation to get p and q.

24.2.26: Use the same method as Exercise 24.2.23.

24.2.27: Since it is hard to choose random points in $E(\mathbb{Z}/N\mathbb{Z})$ one cannot apply the method of Shmuely with the first oracle. For the second oracle one can choose P and then fit the curve through it. Shmuely's method then applies.

24.3.1: Obviously, $(\mathsf{m}_1\mathsf{m}_2)^2 \equiv \mathsf{m}_1^2\mathsf{m}_2^2 \pmod N$. But we need to ensure that decryption of the product of the ciphertexts really does return the product of the messages. Since there is no guarantee that $\mathsf{m}_1\mathsf{m}_2 \pmod N$ has the correct bit pattern in the l least significant bits, redundancy in the message is not suitable for homomorphic encryption.

The "extra bits" redundancy does not work either, since the least significant bit of $\mathsf{m}_1\mathsf{m}_2 \pmod N$ may not be the product (or any other easily computable function) of the least significant bits of m_1 and m_2.

Finally, the Williams redundancy scheme is also not compatible with homomorphic encryption, since $P(\mathsf{m}_1)P(\mathsf{m}_2) \pmod N$ is almost always not equal to $P(\mathsf{m}_1\mathsf{m}_2) \pmod N$.

24.3.5: See Paillier [474].

24.3.7: One computes $\mathsf{c}^{p-1} \pmod{p^2}$ to get $1 + pq(p-1)\mathsf{m} \equiv 1 + p(-q\mathsf{m}) \pmod{p^2}$ and hence $\mathsf{m} \pmod p$. Similarly one computes $\mathsf{m} \pmod q$ and hence $\mathsf{m} \pmod N$. As with standard RSA decryption using the CRT, we replace one modular exponentiation with two modular exponentiations where the exponents and moduli are half the size. Hence, the new method is about 3 times faster than the old one.

24.3.8: The security depends on the decisional problem: Given y, is $y \equiv h^x \pmod{N^2}$ for some integer $0 \leq x < 2^k$. This problem is a variant of composite residuosity, and

also similar to the discrete logarithm problem in an interval; see Exercise 13.3.6 and Section 14.5 for algorithms to solve this problem in $O(2^{k/2})$ multiplications.

Suppose a user's public key consists of elements $h_i = u_i^N \pmod{N^2}$ for $1 \leq i \leq l$ (where the u_i are all random, or perhaps $u_i = u^{\lfloor N^{(i-1)/l} \rfloor} \pmod{N^2}$ for a randomly chosen $1 < u < N$). To encrypt to the user one could compute $\mathsf{c} = (1+N\mathsf{m})h_1^{a_1} \cdots h_l^{a_l} \pmod{N^2}$ using a sliding window multi-exponentiation method, where $0 \leq a_1, \ldots, a_l < 2^k$ for some value k (one possibility would be $2^k \approx N^{1/l}$).

24.3.11: One encrypts $0 \leq \mathsf{m} < N^k$ as

$$\mathsf{c} = (1 + \mathsf{m}N)u^{N^k} \pmod{N^{k+1}}$$

where $1 < u < N^k$ is chosen randomly. Decryption requires some care since

$$\mathsf{c}^{\lambda(N)} \equiv 1 + \lambda(N)\mathsf{m}N + \binom{\lambda(N)}{2}\mathsf{m}^2N^2 + \cdots \pmod{N^{k+1}}.$$

Hence, one first determines $\mathsf{m} \pmod{N}$ from the coefficient $\lambda(N)\mathsf{m}N$, and then $\mathsf{m} \pmod{N^2}$ from the coefficients of N and N^2, and so on. This variant is not used in practice, since messages are usually small for public key encryption.

24.3.12: Since $(u^N)^{p-1} \equiv 1 \pmod{p^2}$ for any $u \in (\mathbb{Z}/N\mathbb{Z})^*$ we have

$$g^{p-1} \equiv (1-p)^{p-1} \equiv 1 - (p-1)p \equiv 1 + p \pmod{p^2}.$$

It follows that $\mathsf{c}^{p-1} \equiv (1+p)^{\mathsf{m}} \equiv 1 + p\mathsf{m} \pmod{p^2}$. The homomorphic property follows since $g^{\mathsf{m}_1}u_1^N g^{\mathsf{m}_2}u_2^N = g^{\mathsf{m}_1+\mathsf{m}_2}(u_1u_2)^N$.

Let G be the subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ of order $(p-1)(q-1)$ containing all p-th powers in $(\mathbb{Z}/N\mathbb{Z})^*$. In other words, $g \notin G$. This subgroup is unique. Determining whether a ciphertext c encrypts a message m is precisely determining whether $\mathsf{c}g^{-\mathsf{m}} \in G$. Okamoto and Uchiyama call this the **p-subgroup problem**.

Finally, suppose one has a decryption oracle for this scheme. Choose an integer $x > N^{1/3}$, compute $\mathsf{c} = g^x \pmod{N}$, and let m be the message returned by the decryption oracle. Then $\mathsf{m} \equiv x \pmod{p}$ and so $p = \gcd(x - \mathsf{m}, N)$.

24.4.4: One uses the formula $\mathsf{c}(\mathsf{m}_1^{-1})^e \equiv \mathsf{m}_2^e \pmod{N}$ to obtain a time/memory tradeoff. We refer to [82] for discussion of the success probability of this attack.

24.4.5: 535573983004, 7873538602921, 8149260569118, 3195403782370.

24.4.6: Either set $F_1(x) = x^e - \mathsf{c}_1$ and $F_2(x) = (ax+b)^e - \mathsf{c}_2$ as before, or reduce to the previous case by multiplying c_2 by $a^{-e} \pmod{N}$.

24.4.7: To find m we construct the polynomials $F_1(x) = x^3 - \mathsf{c}_1$ and $F_2(x) = (x + 2^{10})^3 - \mathsf{c}_2$ and compute their gcd as polynomials in the ring $\mathbb{Z}_N[x]$. The result is

$$G(x) = x - 1234567890$$

from which we deduce that $\mathsf{m} = 1234567890$.

24.4.8: Write $F_1(x) = x^e - \mathsf{c}_1$ and $F_2(y) = y^e - \mathsf{c}_2$. Take the resultant of $F_1(x)$ and $P(x,y)$ with respect to x to obtain a polynomial $F(y)$ of degree de in y. Then compute the gcd of $F(y)$ and $F_2(y)$. The complexity is dominated by the computation of the resultant, which is the determinant of a $(d+e) \times (d+e)$ matrix whose entries are polynomials of degree at most d. Using naive Gaussian elimination gives the result. For further details see Coppersmith et al [144].

24.4.11: Let m be the message to forge and try to find $x, y \approx \sqrt{N}$ such that

$$(P + x) \equiv (P + \mathsf{m})(P + y) \pmod{N}.$$

Then x and y satisfy $x - y(P + \mathsf{m}) \equiv P^2 - P + P\mathsf{m} \pmod{N}$. In other words, we seek a small solution to $x - Ay \equiv B \pmod{N}$ for fixed A, B and N. We have seen how to solve such a problem in Section 11.3.2 under the name "Gallant-Lambert-Vanstone method".

24.4.12: Take $P = A^{-1}B \pmod{N}$.

24.5.1: One checks a guess for d by testing whether $y^d \equiv x \pmod{N}$ for some pre-computed pair $1 < x < N$ and $y = x^e \pmod{N}$. If one precomputes $y^2 \pmod{N}$ then one can compute the next value $y^{d+2} \pmod{N}$ using a single modular multiplication as $y^d y^2 \pmod{N}$. The total complexity is therefore $O(dM(\log(N)))$ bit operations.

24.5.5: Write $\lambda(N) = \varphi(N)/r$ where $r = \gcd(p-1, q-1)$ so that the equation $ed = 1 + k\lambda(N)$ corresponds to the equation $-edr + krN \approx kru$ (with $u \approx \sqrt{N}$). The Wiener method computes dr, as long as the condition $drkru < N$ holds or, in other words, if $d < N^{1/4}/(\sqrt{3}\, r)$. One can determine r as $\gcd(dr, N-1)$ and hence determine d.

24.5.6: One finds $\gcd(p-1, q-1) = 10$ and $d = 97$.

24.5.7: If (e, k) satisfy $ed = 1 + k\varphi(N)$ then so do $(e', k') = (e + l\varphi(N), k + ld)$. Taking l large enough one can ensure that $duk' > N$ and so the attack does not apply.

24.5.8: Choose random $1 < x < N$, set $y = x^e \pmod{N}$ and, for each odd integer $1 < d_p$ in turn, compute $\gcd(x - y^{d_p} \pmod{N}, N)$.

24.5.10: Since $0 \leq p + q < 3\sqrt{N}$ we have $0 \leq x + y \leq (p + q - 2)/r < \sqrt{3}N^{1/4}$ and so v and u give $x + y$ and xy exactly. One can therefore solve the quadratic equation $x^2 - vx + u$ to find x and hence p.

24.5.11: The first calculations are straightforward. The exhaustive search is performed by trying each value for c and testing whether $r^2c^2 + (2rv + 4)c + v^2 - 4u$ is a perfect square (for example, using the method of Exercise 2.4.9).

24.5.12: The exponent is $\mathrm{lcm}(p-1, q-1) = \mathrm{lcm}(xr, yr)$. Choose random $1 < z < N$, let $g = z^r \pmod{N}$ and $h = z^{ur} \pmod{N}$ we have $h \equiv g^c \pmod{N}$ where $0 \leq c < \sqrt{N}/r^2$. One therefore applies standard algorithms for the discrete logarithm problem, such as in Exercise 13.3.6 or Section 14.5. This gives c modulo the order of g. With overwhelming probability the order of g is much larger than $\sqrt{N}$ and so c is found.

24.5.13: Since we may assume one can factor $N - 1$ in under 2^{128} bit operations, it follows that a list of possible values for r is known. Assuming this list is short, one can apply the attack in Exercise 24.5.12 for each possible value for r, to compute p. The cost of the attack for a given guess for r is $O(N^{1/4}/r)$ modular multiplications. To have $N^{1/4}/r > 2^{128}$ means $r < 2^{3072/4-128} = 2^{640}$.

24.5.14: Small r can be found by factoring $N - 1$. Large r make N vulnerable to Pollard rho. with the map

$$x \mapsto x^{N-1} + 1 \pmod{N}.$$

If r is known then one can determine $p + q$ modulo r, and hence perform a similar attack to Exercise 24.5.12 that will split N in $O(N^{1/4}/r)$ ring operations if p and q are of similar size.

24.6.2: See Appendix A of Coron [149].

24.6.3: If $(\frac{h}{N}) = -1$ then set $f = 2$, otherwise $f = 1$. Then $(\frac{fh}{N}) = 1$. Now, if $(\frac{fh}{p}) = -1$ then set $e = -1$, otherwise $e = 1$. It follows that $(\frac{efh}{p}) = 1$ and $(\frac{efh}{q}) = 1$.

24.6.5: Use the fact that, for any $1 \leq a < p$, $(a^{(p+1)/4})^2 \equiv (\frac{a}{p})a \pmod{p}$.

24.6.13: If $e \mid H_2(\mathsf{m} \| \mathsf{s}_1)$ then one can compute the e-th root of $H_1(\mathsf{id})$, which is the private key of the user.

24.6.14: Generating a signature is the same as the original Shamir scheme. For the selective forgery, suppose $(\mathsf{s}_1, \mathsf{s}_2)$ is a valid signature for identity id on a message m where $\gcd(e, H_2(\mathsf{m})) = 1$. Let m' be the message to forge. There are integers $a, b \in \mathbb{Z}$ such that

$ae - bH_2(\mathsf{m}') = -H_2(\mathsf{m})$. Set $\mathsf{s}_1' = \mathsf{s}_1^b$ and $\mathsf{s}_2' = \mathsf{s}_2\mathsf{s}_1^a$ so that $(\mathsf{s}_1', \mathsf{s}_2')$ is a valid signature on m'.

24.6.15: The signature is $\mathsf{s} = s_{\mathsf{id}}^{H_2(\mathsf{m})} \pmod N$.

For the attack, suppose s_1 and s_2 are valid signatures for identity id on messages m_1 and m_2 such that $\gcd(H_2(\mathsf{m}_1), H_2(\mathsf{m}_2)) = 1$. Let $a, b \in \mathbb{Z}$ be such that $aH_2(\mathsf{m}_1)+bH_2(\mathsf{m}_2) = 1$. Then

$$\left(\mathsf{s}_1^a\mathsf{s}_2^b\right)^e \equiv H_1(\mathsf{id}) \pmod N$$

and the user's private key is obtained.

24.7.2: In the case where both top and bottom bits are 1 then let $\mathsf{c}' = \mathsf{c}2^e \pmod N$. Depending on the precise sizes of N and r, the decryption oracle on c' returns either $\mathsf{m}' = 2 + 4\mathsf{m} + 2^{258}r + 2^{3072}$ or $\mathsf{m}' - N$. Since N is odd it is easy to determine which case has arisen and, in the latter case, one simply adds N back again. Solving for m is immediate.

24.7.6: For the proof to go through it is necessary that $\kappa_1 > 2(\kappa + 2)/3$ and $n = \kappa - \kappa_0 - \kappa_1 < \kappa/9$. For full details see Boneh [74].

Chapter 25: Isogenies of Elliptic Curves

25.1.1: Since $\lambda(P) = \mathcal{O}_{\widetilde{E}}$ if and only if $P = \mathcal{O}_{\widetilde{E}}$ it follows that $\ker(\lambda \circ \phi) = \ker(\phi)$. On the other hand, $\ker(\phi \circ \lambda) = \lambda^{-1}(\ker(\phi))$. So if λ does not fix $\ker(\phi)$ then the isogenies are not equivalent.

25.1.3: Just add composition with a power of Frobenius.

25.1.4: The existence of ψ_1 and ψ_2 follows from applying Theorem 9.6.18 to $\phi_2 \circ \phi_1 : E \to E_2$.

25.1.9: The kernel of ϕ is a group of order G. Apply Vélu's formula and write the function X as a rational function in x. Once the result for $\phi_1(x)$ is proved the result for $\phi_2(x, y)$ follows from Theorem 9.7.5.

25.1.11: The calculation is essentially the same as a calculation in the proof of Theorem 9.7.5.

25.1.14: One performs d steps, each step being some arithmetic operations in $\mathbb{F}_{q^n}$. The x-coordinates of points in G are all roots of a polynomial of degree $(d-1)/2$ when d is odd or roots of $yF(x)$ where $\deg(F(x)) < d/2$. The y-coordinates are defined over quadratic extensions.

It is not quite true that $n < d$ in general. Indeed, $\mathbb{F}_{q^n}$ is a compositum of fields of degrees corresponding to the degrees of irreducible factors. Hence n can be bigger than d (e.g., $d = 5$ where the polynomial splits as quadratic times cubic). When d is prime then there are no such problems as the kernel subgroup is generated by a single x-coordinate and a quadratic extension for y.

25.1.17: Note that $t(Q) = 2F_x(Q) - a_1F_y(Q) = 2(3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q) - a_1(-2y_Q - a_1x_Q - a_3)$, and re-arranging gives the result. Similarly, $u(Q) = F_y(Q)^2 = (2y_Q + a_1x_Q + a_3)^2 = 4(y_Q^2 + y_Q(a_1x_Q + a_3)) + (a_1x_Q + a_3)^2$, and one can replace $y_Q^2 + y_Q(a_1x_Q + a_3)$ by $x_Q^3 + a_2x_Q^2 + a_4x_Q + a_6$.

25.1.18: The first statement is using $x_Q = x - (x - x_Q)$ the rest are equally easy. For example, the final statement follows from $x_Q^3 = x^3 - 3x^2x_Q + 3xx_Q^2 - (x - x_Q)^3$ together with some of the earlier cases.

25.1.20: Combine Theorem 25.1.6 with Exercise 25.1.17. Then simplify the formulae using Exercises 25.1.18 and 25.1.19. For details see pages 80-81 of [383].

25.2.2: One computes the powers of $j(E)$ in $\mathbb{F}_q$ in $O(\ell M(\log(q)))$ bit operations. In the polynomial $\Phi_\ell(x, y)$ there are $O(\ell^2)$ terms to consider and the coefficients are of size $O(\ell \log(\ell))$ and so reducing each coefficient to an element of $\mathbb{F}_q$ requires (the hardest

case being when q is prime and large) $O(\ell \log(\ell) \log(q))$ or $O(M(\ell \log(\ell)))$ bit operations. We also need to multiply each coefficient by a suitable power of $j(E)$. The total cost is therefore $O(\ell^2(\ell \log(\ell) \log(q) + M(\log(q)))$ bit operations. The resulting polynomial requires $O(\ell \log(q))$ bits. The claim about root finding is immediate from Exercise 2.12.5.

25.2.3: The first statement follows since $j(E) = j(E')$ and the $\mathbb{F}_q$-rational ℓ-isogenies are given by the roots of $\Phi_\ell(j(E), y)$. For the second statement, let $\phi : E \to E'$ be the isomorphism and consider the map $\mathrm{End}_{\overline{\mathbb{F}}_q}(E) \to \mathrm{End}_{\overline{\mathbb{F}}_q}(E')$ given by $\psi \mapsto \phi \circ \psi \circ \phi^{-1}$. One can check that this is a ring homomorphism and, since ϕ is an isomorphism, it is surjective.

25.3.15: The eigenvalues are $3, \sqrt{2}, 1, 0, -\sqrt{2}, -2$. We have $\lambda(X) = 2 < 2\sqrt{3-1}$ so the graph is Ramanujan. We have $\delta_v(\{1\}) = \{2, 4\}$, $\delta_v(\{1, 2\}) = \{3, 4, 5\}$ and $\delta_v(\{1, 3\}) = \{2, 4, 6\}$. The expander property is easy to verify. It also follows from equation (25.5) and $\lambda_1(X) = \sqrt{2}$; giving $\#\delta_v(A) \geq (3 - \sqrt{2})/6\#A > 0.26\#A$.

25.3.16: Let $n > 2/c$ be even and let X be the 2-regular "line" on n vertices (vertex $1 < i < n$ connected to vertex $i - 1$ and $i + 1$, and vertices 1 and n having single loops). Let $A = \{1, \ldots, n/2\}$ so that $\#A = n/2$ and $c\#A > 1$. But $\delta_v(A) = \{n/2 + 1\}$.

25.3.18: We have $h(-p) = 5$ and $\lfloor p/12 \rfloor + 1 = 9$, so there are nine isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$, five of which are defined over $\mathbb{F}_p$.

Label the vertices of the graph as $24, 80, 23, 69, 34, \alpha, \overline{\alpha}, \beta$ and $\overline{\beta}$. The values α and $\overline{\alpha}$ are the roots of $t^2 + 84t + 73$, while β and $\overline{\beta}$ are roots of $t^2 + 63t + 69$. The graph is 3-regular. Vertices 24 and 80 have two loops, and an edge to 23. Vertex 23 has an edge to 69. Vertex 69 has a loop and an edge to 34. Vertex 34 has edges to α and $\overline{\alpha}$. Vertex α has edges to $\overline{\alpha}$ and β. Vertex $\overline{\alpha}$ has edges to α and $\overline{\beta}$. Finally, vertex β has two edges to $\overline{\beta}$.

25.3.19: The graph has $\lfloor p/12 \rfloor + 1 = 2$ vertices. So the vertices are $j = 0$ and $j = 1728 \equiv 1 \pmod{11}$. Using the modular polynomial $\Phi_2(x, y)$ one finds there are three edges from 0 to 1 and two edges from 1 to 0 (and a loop from 1 to itself). Hence, at least two of the three isogenies from 0 to 1 have the same dual isogeny.

25.3.20: Take $p = 131$. There are 10 supersingular j-invariants in $\mathbb{F}_p$. Taking 2-isogenies gives two components: one containing the j-invariants $\{25, 82\}$ and the other with $\{0, 10, 28, 31, 50, 62, 94, 113\}$.

25.4.9: The graph has two components. Both are trees with a root and 4 leaves. One component has root 42 and leaves $33, 51, 35, 57$. The other component has root 14 and leaves $44, 4, 18, 32$. The diameter of $X_{E,\mathbb{F}_q,\{2,3\}}$ is 2.

25.4.10: Clearly, $j = 11$ and $j = 31$ are on the floor. It follows that $\mathrm{End}(E)$ is the order of index 2 in $\mathbb{Z}[(1 + \sqrt{-7})/2]$. Hence, $\mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-7}]$.

Since the isogenies from $j = 10$ to 11 and 31 are descending it follows that the ascending isogeny is to $j = 29$ and so this curve is on the surface.

25.5.2: The solution to the isogeny problem is a chain of length $O(\log(q))$ of prime-degree isogenies. Assuming that the chain is represented as a sequence of j-invariants, the cost of the Elkies and Vélu steps is $O(\ell^{2+\epsilon} \log(q)^{1+\epsilon})$ bit operations. Since $\ell = O(\log(q)^m)$ the cost for each isogeny is bounded by $O(\ell^{2m+1+\epsilon})$ bit operations. The total cost is therefore $O(\ell^{2m+2+\epsilon})$ bit operations.

25.5.3: Dijsktra's algorithm has complexity linear in the number of vertices, so it needs more than $\sqrt{q}$ operations to find the chain. The advantage is that the isogeny itself can be computed faster, but probably only by a constant factor.

Chapter 26: Pairings on Elliptic Curves

26.1.1: A function f such that $\mathrm{div}(f) = D_1$ is defined up to multiplication by an element of $\overline{\mathbb{k}}^*$. So let f be such a function and write $f(D_2) = \prod_P f(P)^{n_P}$. Then $(uf)(D_2) = u^{\sum_P n_P} f(D_2)$. The term $u^{\sum_P n_P}$ is 1 for all $u \in \overline{\mathbb{k}}^*$ if and only if $\deg(D_2) = 0$.

26.3.5: The fact that the divisors of the functions are correct is immediate. To show the functions are normalised at infinity it is necessary to show that the functions y and x are normalised at infinity. To see this note that $t_\infty^{-3} = (y/x)^3 = y^3/x^3 = y(x^3 + a_2x^2 + a_4x + a_6 - a_1xy - a_3y)/x^3 = y(1+u)$ where u is zero at $\mathcal{O}_E$. Hence, y is normalised at infinity. Similarly, $t_\infty^{-2} = (y/x)^2 = (x^3 + a_2x^2 + a_4x + a_6 - a_1xy - a_3y)/x^2 = x + u$ where $u(\mathcal{O}_E) = a_2$ and so x is normalised at infinity too. It follows that $l(x,y) = y - \lambda_x + c$ and $v(x,y) = x - c$ are normalised at infinity.

26.3.8: This follows since if $\mathrm{div}(f_{n,P}) = n(P) - n(\mathcal{O}_E)$ then $\mathrm{div}(f_{n,P}^m) = mn(P) - mn(\mathcal{O}_E)$. So take $m = N/n$.

26.3.10: Let $Q_1, Q_2 \in E[r]$ be such that $Q_1 \neq Q_2$. Suppose Q_1 and Q_2 were in the same class in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$. Then $Q_1 - Q_2 = [r]R$ for some $R \in E(\mathbb{F}_{q^k})$. It would follow that R has order r^2, but the conditions imply that no such group element exists.

26.3.12: If $v(x) = (x-a)$ is a vertical line function over $\mathbb{F}_q$ then $v(Q) = x_Q - a \in \mathbb{F}_{q^{k/2}}$. It follows that $v(Q)^{(q^k-1)/r} = 1$.

26.3.17: The first statement follows directly from the definition. To show part 2, first note that $\mathrm{div}(f_{s,x-s,Q}) = ([s]Q) - s(Q) + (s-1)(\mathcal{O}_E) = \mathrm{div}(f_{s,Q}^{-1})$. Now, $s \equiv q^m \equiv T^m \pmod r$ and so, by Exercise 26.3.14, we have a power of the ate pairing. Part 3 follows from

$$\mathrm{div}(f_{s,h(x)x,Q}) = \sum_{i=0}^{d} h_i(([s^{i+1}]Q) - (\mathcal{O}_E)) = \sum_{i=0}^{d} h_i(([s^i][s]Q) - (\mathcal{O}_E)) = \mathrm{div}(f_{s,h(x),[s]Q})$$

and the facts that

$$a_{s,h(x)}([s]Q, P) = a_{s,h(x)}(\pi_q^m(Q), P) = a_{s,h(x)}(Q,P)^{q^m} = a_{s,h(x)}(Q,P)^s$$

(this is essentially the same argument as in equation (26.5)). The additive property follows from the fact that the divisor of a product is the sum of the divisors. The multiplicative property follows from the additive property and from part 3.

26.5.3: Given $P, [a]P, [b]P$ choose a point Q such that $e(P,Q) \neq 1$ and one can invert pairings with respect to that point Q. Compute $z = e(P,Q)^{ab}$ as in Lemma 26.5.2, then call the pairing inversion oracle on (Q,z) to get $[ab]P$.

Bibliography

[1] M. Abdalla, M. Bellare, and P. Rogaway, *DHIES: An encryption scheme based on the Diffie-Hellman problem*, Preprint, 2001.

[2] L. M. Adleman and J. DeMarrais, *A subexponential algorithm for discrete logarithms over all finite fields*, Math. Comp. **61** (1993), no. 203, 1–15.

[3] L. M. Adleman, K. L. Manders, and G. L. Miller, *On taking roots in finite fields*, Foundations of Computer Science (FOCS), IEEE, 1977, pp. 175–178.

[4] L.M. Adleman, J. DeMarrais, and M.-D. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, ANTS I (L. M. Adleman and M.-D. Huang, eds.), LNCS, vol. 877, Springer, 1994, pp. 28–40.

[5] G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone, *An implementation for a fast public-key cryptosystem*, J. Crypt. **3** (1991), no. 2, 63–79.

[6] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Ann. of Math **160** (2004), no. 2, 781–793.

[7] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, *Closest point search in lattices*, IEEE Trans. Inf. Theory **48** (2002), no. 8, 2201–2214.

[8] A. Akavia, *Solving hidden number problem with one bit oracle and advice*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 337–354.

[9] W. Alexi, B. Chor, O. Goldreich, and C.-P. Schnorr, *RSA and Rabin functions: Certain parts are as hard as the whole*, SIAM J. Comput. **17** (1988), no. 2, 194–209.

[10] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), no. 3, 703–722.

[11] A. Antipa, D. R. L. Brown, R. P. Gallant, R. J. Lambert, R. Struik, and S. A. Vanstone, *Accelerated verification of ECDSA signatures*, SAC 2005 (B. Preneel and S. E. Tavares, eds.), LNCS, vol. 3897, Springer, 2006, pp. 307–318.

[12] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler, *Faster computation of the Tate pairing*, J. Number Theory **131** (2011), no. 5, 842–857.

[13] J. Arney and E. D. Bender, *Random mappings with constraints on coalescence and number of origins*, Pacific J. Math. **103** (1982), 269–294.

[14] E. Artin, *Galois theory*, 2nd ed., Notre Dame, 1959.

[15] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[16] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic cryptography*, Chapman and Hall/CRC, 2006.

[17] R. M. Avanzi, *A note on the signed sliding window integer recoding and a left-to-right analogue*, SAC 2004 (H. Handschuh and M. A. Hasan, eds.), LNCS, vol. 3357, Springer, 2004, pp. 130–143.

[18] L. Babai, *On Lovász lattice reduction and the nearest lattice point problem*, Combinatorica **6** (1986), no. 1, 1–13.

[19] L. Babai and E. Szemerédi, *On the complexity of matrix group problems I*, Foundations of Computer Science (FOCS) (1996), 229–240.

[20] E. Bach, *Bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380.

[21] ———, *Toward a theory of Pollard's rho method*, Inf. Comput. **90** (1991), no. 2, 139–155.

[22] E. Bach and J. Shallit, *Algorithmic number theory*, MIT press, 1996.

[23] E. Bach and J. Sorenson, *Sieve algorithms for perfect power testing*, Algorithmica **9** (1993), 313–328.

[24] S. Bai and R. P. Brent, *On the efficiency of Pollard's rho method for discrete logarithms*, CATS 2008 (J. Harland and P. Manyem, eds.), Australian Computer Society, 2008, pp. 125–131.

[25] D. V. Bailey, L. Batina, D. J. Bernstein, P. Birkner, J. W. Bos, H.-C. Chen, C.-M. Cheng, G. van Damme, G. de Meulenaer, L. Julian Dominguez Perez, J. Fan, T. Güneysu, F. Gurkaynak, T. Kleinjung, T. Lange, N. Mentens, R. Niederhagen, C. Paar, F. Regazzoni, P. Schwabe, L. Uhsadel, A. Van Herrewege, and B.-Y. Yang, *Breaking ECC2K-130*, Cryptology ePrint Archive, Report 2009/541, 2009.

[26] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Crypt. **11** (1998), no. 2, 141–145.

[27] W. D. Banks and I. E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. **173** (2009), 253–277.

[28] P. S. L. M. Barreto, S. D. Galbraith, C. Ó hÉigeartaigh, and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, Des. Codes Crypt. **42** (2007), no. 3, 239–271.

[29] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, CRYPTO 2002 (M. Yung, ed.), LNCS, vol. 2442, Springer, 2002, pp. 354–369.

[30] P. S. L. M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, SAC 2005 (B. Preneel and S. E. Tavares, eds.), LNCS, vol. 3897, Springer, 2006, pp. 319–331.

[31] A. Bauer, *Vers une généralisation rigoureuse des méthodes de Coppersmith pour la recherche de petites racines de polynômes*, Ph.D. thesis, Université de Versailles Saint-Quentin-en-Yvelines, 2008.

[32] M. Bellare, R. Canetti, and H. Krawczyk, *A modular approach to the design and analysis of authentication and key exchange protocols*, Symposium on the Theory of Computing (STOC), ACM, 1998, pp. 419–428.

[33] M. Bellare, J. A. Garay, and T. Rabin, *Fast batch verification for modular exponentiation and digital signatures*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 236–250.

[34] M. Bellare, S. Goldwasser, and D. Micciancio, *"Pseudo-Random" number generation within cryptographic algorithms: The DSS case*, CRYPTO 1997 (B. S. Kaliski Jr., ed.), LNCS, vol. 1294, Springer, 1997, pp. 277–291.

[35] M. Bellare, C. Namprempre, and G. Neven, *Security proofs for identity-based identification and signature schemes*, J. Crypt. **22** (2009), no. 1, 1–61.

[36] M. Bellare and G. Neven, *Multi-signatures in the plain public-key model and a general forking lemma*, CCS 2006 (A. Juels, R. N. Wright, and S. De Capitani di Vimercati, eds.), ACM, 2006, pp. 390–399.

[37] M. Bellare, D. Pointcheval, and P. Rogaway, *Authenticated key exchange secure against dictionary attacks*, EUROCRYPT 2000 (B. Preneel, ed.), LNCS, vol. 1807, Springer, 2000, pp. 139–155.

[38] M. Bellare and P. Rogaway, *Random oracles are practical: A paradigm for designing efficient protocols*, CCS 1993, ACM, 1993, pp. 62–73.

[39] ———, *Entity authentication and key distribution*, CRYPTO 1993 (D. R. Stinson, ed.), LNCS, vol. 773, Springer, 1994, pp. 232–249.

[40] ———, *Optimal asymmetric encryption - How to encrypt with RSA*, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol. 950, Springer, 1995, pp. 92–111.

[41] ———, *The exact security of digital signatures – how to sign with RSA and Rabin*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 399–416.

[42] K. Bentahar, *The equivalence between the DHP and DLP for elliptic curves used in practical applications, revisited*, IMA Cryptography and Coding (N. P. Smart, ed.), LNCS, vol. 3796, Springer, 2005, pp. 376–391.

[43] ———, *Theoretical and practical efficiency aspects in cryptography*, Ph.D. thesis, University of Bristol, 2008.

[44] D. J. Bernstein, *Faster square roots in annoying finite fields*, Preprint, 2001.

[45] ———, *Pippenger's exponentiation algorithm*, Preprint, 2002.

[46] ———, *Curve 25519: New Diffie-Hellman speed records*, PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), LNCS, vol. 3958, Springer, 2006, pp. 207–228.

[47] ———, *Proving tight security for Rabin-Williams signatures*, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 70–87.

[48] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves*, Africacrypt 2008 (S. Vaudenay, ed.), LNCS, vol. 5023, Springer, 2008, pp. 389–405.

[49] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters, *ECM using Edwards curves*, Cryptology ePrint Archive, Report 2008/016, 2008.

[50] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post quantum cryptography*, Springer, 2008.

[51] D. J. Bernstein and T. Lange, *Explicit formulas database*, 2007.

[52] ———, *Faster addition and doubling on elliptic curves*, ASIACRYPT 2007 (K. Kurosawa, ed.), LNCS, vol. 4833, Springer, 2007, pp. 29–50.

[53] ———, *Analysis and optimization of elliptic-curve single-scalar multiplication*, Contemporary Mathematics **461** (2008), 1–19.

[54] ———, *Type-II optimal polynomial bases*, WAIFI 2010 (M. A. Hasan and T. Helleseth, eds.), LNCS, vol. 6087, Springer, 2010, pp. 41–61.

[55] D. J. Bernstein, T. Lange, and R. R. Farashahi, *Binary Edwards curves*, CHES 2008, (E. Oswald and P. Rohatgi, eds.), LNCS, vol. 5154, Springer, 2008, pp. 244–265.

[56] D. J. Bernstein, T. Lange, and P. Schwabe, *On the correct use of the negation map in the Pollard rho method*, PKC 2011 (D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds.), LNCS, vol. 6571, Springer, 2011, pp. 128–146.

[57] E. Biham, D. Boneh, and O. Reingold, *Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring*, Inf. Process. Lett. **70** (1999), no. 2, 83–87.

[58] G. Bisson and A. V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **131** (2011), no. 5, 815–831.

[59] S. R. Blackburn and S. Murphy, *The number of partitions in Pollard rho*, unpublished manuscript, 1998.

[60] S. R. Blackburn and E. Teske, *Baby-step giant-step algorithms for non-uniform distributions*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 153–168.

[61] I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, *Computing logarithms in finite fields of characteristic two*, SIAM J. Algebraic and Discrete Methods **5** (1984), no. 2, 272–285.

[62] I. F. Blake and T. Garefalakis, *On the complexity of the discrete logarithm and Diffie-Hellman problems*, J. Complexity **20** (2004), no. 2-3, 148–170.

[63] I. F. Blake, T. Garefalakis, and I. E. Shparlinski, *On the bit security of the Diffie-Hellman key*, Appl. Algebra Eng. Commun. Comput. **16** (2006), no. 6, 397–404.

[64] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic curves in cryptography*, Cambridge, 1999.

[65] ———, *Advances in elliptic curve cryptography*, Cambridge, 2005.

[66] D. Bleichenbacher, *Generating ElGamal signatures without knowing the secret key*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 10–18.

[67] ———, *Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 1–12.

[68] ———, *Compressing Rabin signatures*, CT-RSA 2004 (T. Okamoto, ed.), LNCS, vol. 2964, Springer, 2004, pp. 126–128.

[69] D. Bleichenbacher and A. May, *New attacks on RSA with small secret CRT-exponents*, PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), LNCS, vol. 3958, Springer, 2006, pp. 1–13.

[70] D. Bleichenbacher and P. Q. Nguyen, *Noisy polynomial interpolation and noisy Chinese remaindering*, EUROCRYPT 2000 (B. Preneel, ed.), LNCS, vol. 1807, Springer, 2000, pp. 53–69.

[71] J. Blömer and A. May, *Low secret exponent RSA revisited*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 4–19.

[72] J. Blömer and A. May, *A tool kit for finding small roots of bivariate polynomials over the integers*, EUROCRYPT 2005 (R. Cramer, ed.), LNCS, vol. 3494, Springer, 2005, pp. 251–267.

[73] M. Blum and S. Micali, *How to generate cryptographically strong sequences of pseudo-random bits*, SIAM J. Comput. **13** (1984), no. 4, 850–864.

[74] D. Boneh, *Simplified OAEP for the RSA and Rabin functions*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 275–291.

[75] ———, *Finding smooth integers in short intervals using CRT decoding*, J. Comput. Syst. Sci. **64** (2002), no. 4, 768–784.

[76] D. Boneh and X. Boyen, *Short signatures without random oracles*, EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), LNCS, vol. 3027, Springer, 2004, pp. 56–73.

[77] ———, *Short signatures without random oracles and the SDH assumption in bilinear groups*, J. Crypt. **21** (2008), no. 2, 149–177.

[78] D. Boneh and G. Durfee, *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, IEEE Trans. Inf. Theory **46** (2000), no. 4, 1339–1349.

[79] D. Boneh, G. Durfee, and N. Howgrave-Graham, *Factoring* $N = p^r q$ *for large* r, CRYPTO 1999 (M. J. Wiener, ed.), LNCS, vol. 1666, Springer, 1999, pp. 326–337.

[80] D. Boneh and M. K. Franklin, *Identity based encryption from the Weil pairing*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 213–229.

[81] ———, *Identity based encryption from the Weil pairing*, SIAM J. Comput. **32** (2003), no. 3, 586–615.

[82] D. Boneh, A. Joux, and P. Nguyen, *Why textbook ElGamal and RSA encryption are insecure*, ASIACRYPT 2000 (T. Okamoto, ed.), LNCS, vol. 1976, Springer, 2000, pp. 30–43.

[83] D. Boneh and R. J. Lipton, *Algorithms for black-box fields and their application to cryptography*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 283–297.

[84] D. Boneh and I. E. Shparlinski, *On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 201–212.

[85] D. Boneh and R. Venkatesan, *Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 129–142.

[86] ———, *Rounding in lattices and its cryptographic applications*, Symposium on Discrete Algorithms (SODA), ACM/SIAM, 1997, pp. 675–681.

[87] ———, *Breaking RSA may not be equivalent to factoring*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 59–71.

[88] A. Borodin and I. Munro, *The computational complexity of algebraic and numeric problems*, Elsevier, 1975.

[89] J. W. Bos, M. E. Kaihara, and T. Kleinjung, *Pollard rho on elliptic curves*, Preprint, 2009.

[90] J. W. Bos, M. E. Kaihara, and P. L. Montgomery, *Pollard rho on the playstation 3*, Handouts of SHARCS 2009, 2009, pp. 35–50.

[91] J. W. Bos, T. Kleinjung, and A. K. Lenstra, *On the use of the negation map in the Pollard Rho method*, ANTS IX (G. Hanrot, F. Morain, and E. Thomé, eds.), LNCS, vol. 6197, Springer, 2010, pp. 66–82.

[92] W. Bosma and H. W. Lenstra Jr., *Complete systems of two addition laws for elliptic curves*, J. Number Theory **53** (1995), 229–240.

[93] A. Bostan, F. Morain, B. Salvy, and E. Schost, *Fast algorithms for computing isogenies between elliptic curves*, Math. Comp. **77** (2008), no. 263, 1755–1778.

[94] C. Boyd and A. Mathuria, *Protocols for authentication and key establishment*, Information Security and Cryptography, Springer, 2003.

[95] X. Boyen, *The uber-assumption family*, Pairing 2008 (S. D. Galbraith and K. G. Paterson, eds.), LNCS, vol. 5209, Springer, 2008, pp. 39–56.

[96] V. Boyko, M. Peinado, and R. Venkatesan, *Speeding up discrete log and factoring based schemes via precomputations*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 221–235.

[97] S. Brands, *An efficient off-line electronic cash system based on the representation problem*, Tech. report, CWI Amsterdam, 1993, CS-R9323.

[98] R. P. Brent, *An improved Monte Carlo factorization algorithm*, BIT (1980), 176–184.

[99] R. P. Brent and J. M. Pollard, *Factorization of the eighth Fermat number*, Math. Comp. **36** (1981), no. 154, 627–630.

[100] R. P. Brent and P. Zimmermann, *Modern computer arithmetic*, Cambridge, 2010.

[101] ———, *An $O(M(n)\log n)$ algorithm for the Jacobi symbol*, ANTS IX (G. Hanrot, F. Morain, and E. Thomé, eds.), LNCS, vol. 6197, Springer, 2010, pp. 83–95.

[102] E. Bresson, Y. Lakhnech, L. Mazaré, and B. Warinschi, *A generalization of DDH with applications to protocol analysis and computational soundness*, CRYPTO 2007 (A. J. Menezes, ed.), LNCS, vol. 4622, Springer, 2007, pp. 482–499.

[103] E. F. Brickell, *Breaking iterated knapsacks*, CRYPTO 1984 (G. R. Blakley and D. Chaum, eds.), LNCS, vol. 196, Springer, 1985, pp. 342–358.

[104] E. F. Brickell and A. M. Odlyzko, *Cryptanalysis: A survey of recent results*, Contemporary Cryptology (G. J. Simmons, ed.), IEEE, 1991, pp. 501–540.

[105] E. F. Brickell, D. Pointcheval, S. Vaudenay, and M. Yung, *Design validations for discrete logarithm based signature schemes*, PKC 2000 (H. Imai and Y. Zheng, eds.), LNCS, vol. 1751, Springer, 2000, pp. 276–292.

[106] E. Brier, C. Clavier, and D. Naccache, *Cryptanalysis of RSA signatures with fixed-pattern padding*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 433–439.

[107] R. Bröker, *Constructing supersingular elliptic curves*, J. Comb. Number Theory **1** (2009), no. 3, 269–273.

[108] R. Bröker, D. X. Charles, and K. Lauter, *Evaluating large degree isogenies and applications to pairing based cryptography*, Pairing 2008 (S. D. Galbraith and K. G. Paterson, eds.), LNCS, vol. 5209, Springer, 2008, pp. 100–112.

[109] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231.

[110] R. Bröker and A. V. Sutherland, *An explicit height bound for the classical modular polynomial*, The Ramanujan Journal **22** (2010), no. 3, 293–313.

[111] D. R. L. Brown and R. P. Gallant, *The static Diffie-Hellman problem*, Cryptology ePrint Archive, Report 2004/306, 2004.

[112] B. B. Brumley and K. U. Järvinen, *Koblitz curves and integer equivalents of Frobenius expansions*, SAC 2007 (C. M. Adams, A. Miri, and M. J. Wiener, eds.), LNCS, vol. 4876, Springer, 2007, pp. 126–137.

[113] J. P. Buhler and P. Stevenhagen, *Algorithmic number theory*, MSRI publications, Cambridge, 2008.

[114] M. Burmester and Y. Desmedt, *A secure and efficient conference key distribution system*, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol. 950, Springer, 1995, pp. 267–275.

[115] R. Canetti, O. Goldreich, and S. Halevi, *The random oracle model, revisited*, Symposium on the Theory of Computing (STOC), ACM, 1998, pp. 209–218.

[116] R. Canetti and H. Krawczyk, *Analysis of key-exchange protocols and their use for building secure channels*, EUROCRYPT 2001 (B. Pfitzmann, ed.), LNCS, vol. 2045, Springer, 2001, pp. 453–474.

[117] E. R. Canfield, P. Erdös, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, J. Number Theory **17** (1983), no. 1, 1–28.

[118] D. G. Cantor, *Computing in the Jacobian of an hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101.

[119] ———, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145.

[120] D. Cash, E. Kiltz, and V. Shoup, *The twin Diffie-Hellman problem and applications*, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 127–145.

[121] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer, 1959.

[122] ———, *Lectures on elliptic curves*, Cambridge, 1991.

[123] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, Cambridge, 1996.

[124] J. W. S. Cassels and A. Frölich, *Algebraic number theory*, Academic Press, 1967.

[125] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Q. Nguyen, *Paillier's cryptosystem revisited*, CCS 2001, ACM, 2001, pp. 206–214.

[126] L. S. Charlap and R. Coley, *An elementary introduction to elliptic curves II*, CCR Expository Report 34, Institute for Defense Analysis, 1990.

[127] L. S. Charlap and D. P. Robbins, *An elementary introduction to elliptic curves*, CRD Expository Report 31, 1988.

[128] D. X. Charles, K. E. Lauter, and E. Z. Goren, *Cryptographic hash functions from expander graphs*, J. Crypt. **22** (2009), no. 1, 93–113.

[129] M. Chateauneuf, A. C. H. Ling, and D. R. Stinson, *Slope packings and coverings, and generic algorithms for the discrete logarithm problem*, Journal of Combinatorial Designs **11** (2003), no. 1, 36–50.

[130] D. Chaum, E. van Heijst, and B. Pfitzmann, *Cryptographically strong undeniable signatures, unconditionally secure for the signer*, CRYPTO 1991 (J. Feigenbaum, ed.), LNCS, vol. 576, Springer, 1992, pp. 470–484.

[131] J.-H. Cheon, *Security analysis of the strong Diffie-Hellman problem*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 1–11.

[132] ———, *Discrete logarithm problem with auxiliary inputs*, J. Crypt. **23** (2010), no. 3, 457–476.

[133] J. H. Cheon, J. Hong, and M. Kim, *Speeding up the Pollard rho method on prime fields*, ASIACRYPT 2008 (J. Pieprzyk, ed.), LNCS, vol. 5350, Springer, 2008, pp. 471–488.

[134] J. H. Cheon and H.-T. Kim, *Analysis of low Hamming weight products*, Discrete Applied Mathematics **156** (2008), no. 12, 2264–2269.

[135] M. A. Cherepnev, *On the connection between the discrete logarithms and the Diffie-Hellman problem*, Discr. Math. Appl. **6** (1996), no. 4, 341–349.

[136] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer, 1993.

[137] ———, *Analysis of the sliding window powering algorithm*, J. Crypt. **18** (2005), no. 1, 63–76.

[138] P. Cohen, *On the coefficients of the transformation polynomials for the elliptic modular function*, Math. Proc. Cambridge Philos. Soc. **95** (1984), no. 3, 389–402.

[139] S. A. Cook, *An overview of computational complexity*, Commun. ACM **26** (1983), no. 6, 400–408.

[140] D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic 2*, IEEE Trans. Inf. Theory **30** (1984), no. 4, 587–594.

[141] ———, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Crypt. **10** (1997), no. 4, 233–260.

[142] ———, *Finding small solutions to small degree polynomials*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 20–31.

[143] D. Coppersmith, J.-S. Coron, F. Grieu, S. Halevi, C. Jutla, D. Naccache, and J. P. Stern, *Cryptanalysis of ISO/IEC 9796-1*, J. Crypt. **21** (2008), no. 1, 27–51.

[144] D. Coppersmith, M. K. Franklin, J. Patarin, and M. K. Reiter, *Low-exponent RSA with related messages*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 1–9.

[145] D. Coppersmith, A. M. Odlzyko, and R. Schroeppel, *Discrete logarithms in GF(p)*, Algorithmica **1** (1986), no. 1-4, 1–15.

[146] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*, 2nd ed., MIT press, 2001.

[147] G. Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. **77** (2001), no. 3, 241–246.

[148] J.-S. Coron, *On the exact security of full domain hash*, CRYPTO 2000 (M. Bellare, ed.), LNCS, vol. 1880, Springer, 2000, pp. 229–235.

[149] ———, *Optimal security proofs for PSS and other signature schemes*, EUROCRYPT 2002 (L. R. Knudsen, ed.), LNCS, vol. 2332, Springer, 2002, pp. 272–287.

[150] ———, *Finding small roots of bivariate integer polynomial equations: A direct approach*, CRYPTO 2007 (A. Menezes, ed.), LNCS, vol. 4622, Springer, 2007, pp. 379–394.

[151] J.-S. Coron and A. May, *Deterministic polynomial-time equivalence of computing the RSA secret key and factoring*, J. Crypt. **20** (2007), no. 1, 39–50.

[152] J.-S. Coron, D. M'Raïhi, and C. Tymen, *Fast generation of pairs* $(k, [k]P)$ *for Koblitz elliptic curves*, SAC 2001 (S. Vaudenay and A. M. Youssef, eds.), LNCS, vol. 2259, Springer, 2001, pp. 151–164.

[153] J.-S. Coron, D. Naccache, M. Tibouchi, and R.-P. Weinmann, *Practical cryptanalysis of ISO/IEC 9796-2 and EMV signatures*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 428–444.

[154] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, and J. Stern, *Improved low-density subset sum algorithms*, Computational Complexity **2** (1992), 111–128.

[155] J.-M. Couveignes, *Computing l-isogenies with the p-torsion*, ANTS II (H. Cohen, ed.), LNCS, vol. 1122, Springer, 1996, pp. 59–65.

[156] J.-M. Couveignes, L. Dewaghe, and F. Morain, *Isogeny cycles and the Schoof-Elkies-Atkin algorithm*, Research Report LIX/RR/96/03, 1996.

[157] D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, 1989.

[158] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties and algorithms: An introduction to computational algebraic geometry and commutative algebra*, 2nd ed., Springer, 1997.

[159] R. Cramer and V. Shoup, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 13–25.

[160] ———, *Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption*, EUROCRYPT 2002 (L. R. Knudsen, ed.), LNCS, vol. 2332, Springer, 2002, pp. 45–64.

[161] ———, *Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack*, SIAM J. Comput. **33** (2003), no. 1, 167–226.

[162] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, 2nd ed., Springer, 2005.

[163] C. W. Curtis, *Linear algebra: An introductory approach*, Undergraduate Texts in Mathematics, Springer, 1984.

[164] I. Damgård, *On the randomness of Legendre and Jacobi sequences*, CRYPTO 1988 (S. Goldwasser, ed.), LNCS, vol. 403, Springer, 1990, pp. 163–172.

[165] I. Damgård and M. Jurik, *A generalisation, a simplification and some applications of Paillier's probabilistic public-key system*, PKC 2001 (K. Kim, ed.), LNCS, vol. 1992, Springer, 2001, pp. 119–136.

[166] G. Davidoff, P. Sarnak, and A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, Cambridge, 2003.

[167] M. Davis and E. J. Weyuker, *Computability, complexity and languages*, Academic Press, 1983.

[168] P. de Rooij, *On Schnorr's preprocessing for digital signature schemes*, J. Crypt. **10** (1997), no. 1, 1–16.

[169] B. den Boer, *Diffie-Hellman is as strong as discrete log for certain primes*, CRYPTO 1988 (S. Goldwasser, ed.), LNCS, vol. 403, Springer, 1990, pp. 530–539.

[170] Y. Desmedt and A. M. Odlyzko, *A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes*, CRYPTO 1985 (H. C. Williams, ed.), LNCS, vol. 218, Springer, 1986, pp. 516–522.

[171] L. Dewaghe, *Un corollaire aux formules de Vélu*, Preprint, 1995.

[172] C. Diem, *The GHS-attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32.

[173] ———, *On the discrete logarithm problem in elliptic curves over non-prime finite fields*, Lecture at ECC 2004, 2004.

[174] ———, *An index calculus algorithm for non-singular plane curves of high genus*, Talk at ECC 2006, 2006.

[175] ———, *An index calculus algorithm for plane curves of small degree*, ANTS VII (F. Hess, S. Pauli, and M. E. Pohst, eds.), LNCS, vol. 4076, Springer, 2006, pp. 543–557.

[176] ———, *On the discrete logarithm problem in class groups of curves*, Math. Comp. **80** (2011), no. 273, 443–475.

[177] ———, *On the discrete logarithm problem in elliptic curves*, Compositio Math. **147** (2011), 75–104.

[178] C. Diem and E. Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Crypt. **21** (2008), no. 4, 593–611.

[179] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory **22** (1976), 644–654.

[180] V. S. Dimitrov, K. U. Järvinen, M. J. Jacobson, W. F. Chan, and Z. Huang, *Provably sublinear point multiplication on Koblitz curves and its hardware implementation*, IEEE Trans. Computers **57** (2008), no. 11, 1469–1481.

[181] V. S. Dimitrov, G. A. Jullien, and W. C. Miller, *Theory and applications of the double-base number system*, IEEE Trans. Computers **48** (1999), no. 10, 1098–1106.

[182] S. A. DiPippo and E. W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory **73** (1998), no. 2, 426–450.

[183] C. Doche, T. Icart, and D. R. Kohel, *Efficient scalar multiplication by isogeny decompositions*, PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), LNCS, vol. 3958, Springer, 2006, pp. 191–206.

[184] A. Dujella, *A variant of Wiener's attack on RSA*, Computing **85** (2009), no. 1-2, 77–83.

[185] I. M. Duursma, *Class numbers for some hyperelliptic curves*, Arithmetic, Geometry and Coding Theory (R. Pellikaan, M. Perret, and S.G. Vladut, eds.), Walter de Gruyter, 1996, pp. 45–52.

[186] I. M. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, ASIACRYPT 1999 (K.Y. Lam, E. Okamoto, and C. Xing, eds.), LNCS, vol. 1716, Springer, 1999, pp. 103–121.

[187] I. M. Duursma and H.-S. Lee, *Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$*, ASIACRYPT 2003 (C.-S. Laih, ed.), LNCS, vol. 2894, Springer, 2003, pp. 111–123.

[188] P. N. J. Eagle, S. D. Galbraith, and J. Ong, *Point compression for Koblitz elliptic curves*, Advances in Mathematics of Communication **5** (2011), no. 1, 1–10.

[189] S. Edixhoven, *Le couplage Weil: de la géométrie à l'arithmétique*, Notes from a seminar in Rennes, 2002.

[190] H. M. Edwards, *A normal form for elliptic curves*, Bulletin of the AMS **44** (2007), 393–422.

[191] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, GTM, vol. 150, Springer, 1999.

[192] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, CRYPTO 1984 (G. R. Blakley and D. Chaum, eds.), LNCS, vol. 196, Springer, 1985, pp. 10–18.

[193] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, AMS, 1998, pp. 21–76.

[194] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. **78** (2009), no. 267, 1809–1824.

[195] A. Enge and P. Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arith. **102** (2002), 83–103.

[196] ———, *An $L(1/3 + \epsilon)$ algorithm for the discrete logarithm problem for low degree curves*, EUROCRYPT 2007 (M. Naor, ed.), LNCS, vol. 4515, Springer, 2007, pp. 379–393.

[197] A. Enge, P. Gaudry, and E. Thomé, *An $L(1/3)$ discrete logarithm algorithm for low degree curves*, J. Crypt. **24** (2011), no. 1, 24–41.

[198] A. Enge and A. Stein, *Smooth ideals in hyperelliptic function fields*, Math. Comp. **71** (2002), no. 239, 1219–1230.

[199] S. Erickson, M. J. Jacobson Jr., N. Shang, S. Shen, and A. Stein, *Explicit formulas for real hyperelliptic curves of genus 2 in affine representation*, WAIFI 2007 (C. Carlet and B. Sunar, eds.), LNCS, vol. 4547, Springer, 2007, pp. 202–218.

[200] H. M. Farkas and I. Kra, *Riemann surfaces*, GTM, vol. 71, Springer, 1980.

[201] U. Feige, A. Fiat, and A. Shamir, *Zero-knowledge proofs of identity*, J. Crypt. **1** (1988), no. 2, 77–94.

[202] L. De Feo, *Fast algorithms for towers of finite fields and isogenies*, Ph.D. thesis, L'École Polytechnique, 2010.

[203] R. Fischlin and C.-P. Schnorr, *Stronger security proofs for RSA and Rabin bits*, J. Crypt. **13** (2000), no. 2, 221–244.

[204] P. Flajolet and A. M. Odlyzko, *Random mapping statistics*, EUROCRYPT 1989 (J.-J.Quisquater and J. Vandewalle, eds.), LNCS, vol. 434, Springer, 1990, pp. 329–354.

[205] P. Flajolet and R. Sedgewick, *Analytic combinatorics*, Cambridge, 2009.

[206] R. Flassenberg and S. Paulus, *Sieving in function fields*, Experiment. Math. **8** (1999), no. 4, 339–349.

[207] K. Fong, D. Hankerson, J. López, and A. J. Menezes, *Field inversion and point halving revisited*, IEEE Trans. Computers **53** (2004), no. 8, 1047–1059.

[208] C. Fontaine and F. Galand, *A survey of homomorphic encryption for nonspecialists*, EURASIP Journal on Information Security **2007** (2007), no. 15, 1–10.

[209] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, ANTS V (C. Fieker and D. R. Kohel, eds.), LNCS, vol. 2369, Springer, 2002, pp. 276–291.

[210] D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Crypt. **23** (2010), no. 2, 224–280.

[211] D. M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, *More constructions of lossy and correlation-secure trapdoor functions*, PKC 2010 (P. Q. Nguyen and D. Pointcheval, eds.), LNCS, vol. 6056, Springer, 2010, pp. 279–295.

[212] G. Frey, *How to disguise an elliptic curve*, Talk at ECC 1998, Waterloo, 1998.

[213] G. Frey and H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Math. Comp. **62** (1994), no. 206, 865–874.

[214] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Springer, 2008.

[215] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, *RSA-OAEP is secure under the RSA assumption*, J. Crypt. **17** (2004), no. 2, 81–104.

[216] W. Fulton, *Algebraic curves*, Addison-Wesley, 1989, Out of print, but freely available here: `http://www.math.lsa.umich.edu/~wfulton/`.

[217] S. D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138.

[218] ———, *Supersingular curves in cryptography*, ASIACRYPT 2001 (C. Boyd, ed.), LNCS, vol. 2248, Springer, 2001, pp. 495–513.

[219] S. D. Galbraith, M. Harrison, and D. J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, ANTS VIII (A. J. van der Poorten and A. Stein, eds.), LNCS, vol. 5011, Springer, 2008, pp. 342–356.

[220] S. D. Galbraith, C. Heneghan, and J. F. McKee, *Tunable balancing of RSA*, ACISP 2005 (C. Boyd and J. M. González Nieto, eds.), LNCS, vol. 3574, Springer, 2005, pp. 280–292.

[221] S. D. Galbraith, F. Hess, and N. P. Smart, *Extending the GHS Weil descent attack*, EUROCRYPT 2002 (L. R. Knudsen, ed.), LNCS, vol. 2332, Springer, 2002, pp. 29–44.

[222] S. D. Galbraith, F. Hess, and F. Vercauteren, *Aspects of pairing inversion*, IEEE Trans. Inf. Theory **54** (2008), no. 12, 5719–5728.

[223] S. D. Galbraith and M. Holmes, *A non-uniform birthday problem with applications to discrete logarithms*, Cryptology ePrint Archive, Report 2010/616, 2010.

[224] S. D. Galbraith, X. Lin, and M. Scott, *Endomorphisms for faster elliptic curve cryptography on a large class of curves*, EUROCRYPT 2009 (A. Joux, ed.), LNCS, vol. 5479, Springer, 2009, pp. 518–535.

[225] S. D. Galbraith and J. F. McKee, *The probability that the number of points on an elliptic curve over a finite field is prime*, Journal of the Lond. Math. Soc. **62** (2000), no. 3, 671–684.

[226] S. D. Galbraith, J. M. Pollard, and R. S. Ruprai, *Computing discrete logarithms in an interval*, 2013, pp. 1181–1195.

[227] S. D. Galbraith and R. S. Ruprai, *An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems*, IMA Cryptography and Coding (M. G. Parker, ed.), LNCS, vol. 5921, Springer, 2009, pp. 368–382.

[228] ———, *Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval*, PKC 2010 (P. Q. Nguyen and D. Pointcheval, eds.), LNCS, vol. 6056, Springer, 2010, pp. 368–383.

[229] S. D. Galbraith and N. P. Smart, *A cryptographic application of Weil descent*, IMA Cryptography and Coding (M. Walker, ed.), LNCS, vol. 1746, Springer, 1999, pp. 191–200.

[230] S. D. Galbraith and A. Stolbunov, *Improved algorithm for the isogeny problem for ordinary elliptic curves*, Applicable Algebra in Engineering, Communication and Computing **24** (2013), no. 2, 107–131.

[231] S. D. Galbraith and E. R. Verheul, *An analysis of the vector decomposition problem*, PKC 2008 (R. Cramer, ed.), LNCS, vol. 4939, Springer, 2008, pp. 308–327.

[232] R. P. Gallant, R. J. Lambert, and S. A. Vanstone, *Improving the parallelized Pollard lambda search on binary anomalous curves*, Math. Comp. **69** (2000), no. 232, 1699–1705.

[233] ———, *Faster point multiplication on elliptic curves with efficient endomorphisms*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 190–200.

[234] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen, *Symplectic lattice reduction and NTRU*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 233–253.

[235] N. Gama, P. Q. Nguyen, and O. Regev, *Lattice enumeration using extreme pruning*, EUROCRYPT 2010 (H. Gilbert, ed.), LNCS, vol. 6110, Springer, 2010, pp. 257–278.

[236] S. Gao, *Normal bases over finite fields*, Ph.D. thesis, Waterloo, 1993.

[237] T. Garefalakis, *The generalised Weil pairing and the discrete logarithm problem on elliptic curves*, Theor. Comput. Sci. **321** (2004), no. 1, 59–72.

[238] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge, 1999.

[239] J. von zur Gathen and M. Giesbrecht, *Constructing normal bases in finite fields*, J. Symb. Comput. **10** (1990), no. 6, 547–570.

[240] J. von zur Gathen, I. E. Shparlinski, and A. Sinclair, *Finding points on curves over finite fields*, SIAM J. Comput. **32** (2003), no. 6, 1436–1448.

[241] P. Gaudry, *Courbes hyperelliptiques et cryptologie*, MSc thesis, L'École Polytechnique, 1995.

[242] ———, *An algorithm for solving the discrete log problem on hyperelliptic curves*, EUROCRYPT 2000 (B. Preneel, ed.), LNCS, vol. 1807, Springer, 2000, pp. 19–34.

[243] ———, *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*, Ph.D. thesis, L'École Polytechnique, 2000.

[244] ———, *Fast genus 2 arithmetic based on theta functions*, J. Math. Crypt. **1** (2007), no. 3, 243–265.

[245] ———, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, Journal of Symbolic Computation **44** (2009), no. 12, 1690–1702.

[246] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Crypt. **15** (2002), no. 1, 19–46.

[247] P. Gaudry and D. Lubicz, *The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines*, Finite Fields Appl. **15** (2009), no. 2, 246–260.

[248] P. Gaudry and É. Schost, *Construction of secure random curves of genus 2 over prime fields*, EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), LNCS, vol. 3027, Springer, 2004, pp. 239–256.

[249] ———, *A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm*, ANTS VI (D. A. Buell, ed.), LNCS, vol. 3076, Springer, 2004, pp. 208–222.

[250] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76** (2007), no. 257, 475–492.

[251] C. Gentry, *Key recovery and message attacks on NTRU-composite*, EUROCRYPT 2001 (B. Pfitzmann, ed.), LNCS, vol. 2045, Springer, 2001, pp. 182–194.

[252] ———, *The geometry of provable security: Some proofs of security in which lattices make a surprise appearance*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 391–426.

[253] C. Gentry, C. Peikert, and V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, Symposium on the Theory of Computing (STOC) (R. E. Ladner and C. Dwork, eds.), ACM, 2008, pp. 197–206.

[254] M. Girault, *An identity-based identification scheme based on discrete logarithms modulo a composite number*, EUROCRYPT 1990 (I. Damgård, ed.), LNCS, vol. 473, Springer, 1991, pp. 481–486.

[255] M. Girault, G. Poupard, and J. Stern, *On the fly authentication and signature schemes based on groups of unknown order*, J. Crypt. **19** (2006), no. 4, 463–487.

[256] O. Goldreich, S. Goldwasser, and S. Halevi, *Public-key cryptosystems from lattice reduction problems*, CRYPTO 1997 (B. S. Kaliski Jr., ed.), LNCS, vol. 1294, Springer, 1997, pp. 112–131.

[257] O. Goldreich, D. Ron, and M. Sudan, *Chinese remaindering with errors*, IEEE Trans. Inf. Theory **46** (2000), no. 4, 1330–1338.

[258] S. Goldwasser, S. Micali, and R. L. Rivest, *A digital signature scheme secure against adaptive chosen-message attacks*, SIAM J. Comput. **17** (1988), no. 2, 281–308.

[259] G. Gong and L. Harn, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inf. Theory **45** (1999), no. 7, 2601–2605.

[260] M. I. González Vasco, M. Näslund, and I. E. Shparlinski, *New results on the hardness of Diffie-Hellman bits*, PKC 2004 (F. Bao, R. H. Deng, and J. Zhou, eds.), LNCS, vol. 2947, Springer, 2004, pp. 159–172.

[261] M. I. González Vasco and I. E. Shparlinski, *On the security of Diffie-Hellman bits*, Cryptography and Computational Number Theory (H. Wang K. Y. Lam, I. E. Shparlinski and C. Xing, eds.), Progress in Computer Science and Applied Logic, Birkhäuser, 2001, pp. 257–268.

[262] D. M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. **52** (1989), no. 185, 231–245.

[263] D. M. Gordon and K. S. McCurley, *Massively parallel computation of discrete logarithms*, CRYPTO 1992 (E. F. Brickell, ed.), LNCS, vol. 740, Springer, 1993, pp. 312–323.

[264] J. Gordon, *Strong primes are easy to find*, EUROCRYPT 1984 (T. Beth, N. Cot, and I. Ingemarsson, eds.), LNCS, vol. 209, Springer, 1985, pp. 216–223.

[265] R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren, *Ate pairing on hyperelliptic curves*, EUROCRYPT 2007 (M. Naor, ed.), LNCS, vol. 4515, Springer, 2007, pp. 430–447.

[266] R. Granger and F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, CRYPTO 2005 (V. Shoup, ed.), LNCS, vol. 3621, Springer, 2005, pp. 66–85.

[267] A. Granville, *Smooth numbers: Computational number theory and beyond*, Algorithmic number theory (J. P. Buhler and P. Stevenhagen, eds.), MSRI Proceedings, vol. 44, Cambridge, 2008, pp. 267–323.

[268] B. H. Gross, *Heights and the special values of L-series*, Number theory, CMS Conf. Proc., vol. 7, AMS, 1987, pp. 115–187.

[269] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer, 1993.

[270] J. Guarjardo and C. Paar, *Itoh-Tsujii inversion in standard basis and its application in cryptography and codes*, Des. Codes Crypt. **25** (2002), no. 2, 207–216.

[271] L. C. Guillou and J.-J. Quisquater, *A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory*, EUROCRYPT 1988 (C. G. Günther, ed.), LNCS, vol. 330, Springer, 1988, pp. 123–128.

[272] R. K. Guy, *Unsolved problems in number theory*, 2nd ed., Springer, 1994.

[273] J. L. Hafner and K. S. McCurley, *Asymptotically fast triangularization of matrices over rings*, SIAM J. Comput. **20** (1991), no. 6, 1068–1083.

[274] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, Springer, 2004.

[275] G. Hanrot and D. Stehlé, *Improved analysis of Kannan's shortest lattice vector algorithm*, CRYPTO 2007 (A. Menezes, ed.), LNCS, vol. 4622, Springer, 2007, pp. 170–186.

[276] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford, 1980.

[277] R. Harley, *Fast arithmetic on genus two curves*, Preprint, 2000.

[278] R. Hartshorne, *Algebraic geometry*, GTM, vol. 52, Springer, 1977.

[279] J. Håstad and M. Näslund, *The security of all RSA and discrete log bits*, J. ACM **51** (2004), no. 2, 187–230.

[280] G. Havas, B. S. Majewski, and K. R. Matthews, *Extended GCD and Hermite normal form algorithms via lattice basis reduction*, Experimental Math. **7** (1998), no. 2, 125–136.

[281] B. Helfrich, *Algorithms to construct Minkowski reduced and Hermite reduced lattice bases*, Theor. Comput. Sci. **41** (1985), 125–139.

[282] F. Hess, *A note on the Tate pairing of curves over finite fields*, Arch. Math. **82** (2004), 28–32.

[283] ———, *Pairing lattices*, Pairing 2008 (S. D. Galbraith and K. G. Paterson, eds.), LNCS, vol. 5209, Springer, 2008, pp. 18–38.

[284] F. Hess, N. Smart, and F. Vercauteren, *The eta pairing revisited*, IEEE Trans. Inf. Theory **52** (2006), no. 10, 4595–4602.

[285] N. J. Higham, *Accuracy and stability of numerical algorithms*, 2nd ed., SIAM, 2002.

[286] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, *Jacobi quartic curves revisited*, ACISP 2009 (C. Boyd and J. M. González Nieto, eds.), LNCS, vol. 5594, Springer, 2009, pp. 452–468.

[287] Y. Hitchcock, P. Montague, G. Carter, and E. Dawson, *The efficiency of solving multiple discrete logarithm problems and the implications for the security of fixed elliptic curves*, Int. J. Inf. Secur. **3** (2004), 86–98.

[288] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A ring-based public key cryptosystem*, ANTS III (J. Buhler, ed.), LNCS, vol. 1423, Springer, 1998, pp. 267–288.

[289] ———, *An introduction to mathematical cryptography*, Springer, 2008.

[290] J. Hoffstein and J. H. Silverman, *Random small Hamming weight products with applications to cryptography*, Discrete Applied Mathematics **130** (2003), no. 1, 37–49.

[291] D. Hofheinz and E. Kiltz, *The group of signed quadratic residues and applications*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 637–653.

[292] S. Hohenberger and B. Waters, *Short and stateless signatures from the RSA assumption*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 654–670.

[293] J. E. Hopcroft and J. D. Ullman, *Introduction to automata theory, languages and computation*, Addison-Wesley, 1979.

[294] J. Horwitz and R. Venkatesan, *Random Cayley digraphs and the discrete logarithm*, ANTS V (C. Fieker and D. R. Kohel, eds.), LNCS, vol. 2369, Springer, 2002, pp. 416–430.

[295] E. W. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Mathematica **85** (1993), 229–247.

[296] N. Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, IMA Cryptography and Coding (M. Darnell, ed.), LNCS, vol. 1355, Springer, 1997, pp. 131–142.

[297] ———, *Approximate integer common divisors*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 51–66.

[298] N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. Whyte, *The impact of decryption failures on the security of NTRU encryption*, CRYPTO 2003 (D. Boneh, ed.), LNCS, vol. 2729, Springer, 2003, pp. 226–246.

[299] N. Howgrave-Graham and N. P. Smart, *Lattice attacks on digital signature schemes*, Des. Codes Crypt. **23** (2001), 283–290.

[300] N. A. Howgrave-Graham and A. Joux, *New generic algorithms for hard knapsacks*, Eurocrypt 2010 (H. Gilbert, ed.), LNCS, vol. 6110, Springer, 2010, pp. 235–256.

[301] T. W. Hungerford, *Algebra*, GTM 73, Springer, 1974.

[302] D. Husemöller, *Elliptic curves*, 2nd ed., GTM, vol. 111, Springer, 2004.

[303] T. Icart, *How to hash into elliptic curves*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 303–316.

[304] J.-I. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. **72** (1960), no. 3, 612–649.

[305] T. Iijima, K. Matsuo, J. Chao, and S. Tsujii, *Construction of Frobenius maps of twist elliptic curves and its application to elliptic scalar multiplication*, Symposium on Cryptography and Information Security (SCIS) 2002, IEICE Japan, 2002, pp. 699–702.

[306] A. Islam, *Products of three pairwise coprime integers in short intervals*, LMS J. Comput. Math. **15** (2012), 59–70.

[307] T. Itoh and S. Tsujii, *A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases*, Information and Computation **78** (1988), no. 3, 171–177.

[308] T. Jager and J. Schwenk, *On the equivalence of generic group models*, ProvSec 2008 (K. Chen J. Baek, F. Bao and X. Lai, eds.), LNCS, vol. 5324, Springer, 2008, pp. 200–209.

[309] D. Jao, D. Jetchev, and R. Venkatesan, *On the bits of elliptic curve Diffie-Hellman keys*, INDOCRYPT 2007 (K. Srinathan, C. Pandu Rangan, and M. Yung, eds.), LNCS, vol. 4859, Springer, 2007, pp. 33–47.

[310] D. Jao, S. D. Miller, and R. Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, ASIACRYPT 2005 (B. K. Roy, ed.), LNCS, vol. 3788, Springer, 2005, pp. 21–40.

[311] ———, *Expander graphs based on GRH with an application to elliptic curve cryptography*, J. Number Theory **129** (2009), no. 6, 1491–1504.

[312] D. Jao and V. Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, ANTS IX (G. Hanrot, F. Morain, and E. Thomé, eds.), LNCS, vol. 6197, Springer, 2010, pp. 219–233.

[313] D. Jao and K. Yoshida, *Boneh-Boyen signatures and the strong Diffie-Hellman problem*, Pairing 2009 (H. Shacham and B. Waters, eds.), LNCS, vol. 5671, Springer, 2009, pp. 1–16.

[314] D. Jetchev and R. Venkatesan, *Bits security of the elliptic curve Diffie-Hellman secret keys*, CRYPTO 2008 (D. Wagner, ed.), LNCS, vol. 5157, Springer, 2008, pp. 75–92.

[315] Z.-T. Jiang, W.-L. Xu, and Y.-M. Wang, *Polynomial analysis of DH secrete key and bit security*, Wuhan University Journal of Natural Sciences **10** (2005), no. 1, 239–242.

[316] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 385–393.

[317] ———, *Algorithmic cryptanalysis*, Chapman & Hall/CRC, 2009.

[318] A. Joux and R. Lercier, *The function field sieve in the medium prime case*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 254–270.

[319] A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren, *The number field sieve in the medium prime case*, CRYPTO 2006 (C. Dwork, ed.), LNCS, vol. 4117, Springer, 2006, pp. 326–344.

[320] M. Joye and G. Neven, *Identity-based cryptography*, Cryptology and Information Security, vol. 2, IOS Press, 2008.

[321] M. Joye and S.-M. Yen, *Optimal left-to-right binary signed-digit recoding*, IEEE Trans. Computers **49** (2000), no. 7, 740–748.

[322] M. J. Jacobson Jr., N. Koblitz, J. H. Silverman, A. Stein, and E. Teske, *Analysis of the Xedni calculus attack*, Des. Codes Crypt. **20** (2000), no. 1, 41–64.

[323] M. J. Jacobson Jr. and A. J. van der Poorten, *Computational aspects of NUCOMP*, ANTS V (C. Fieker and D. R. Kohel, eds.), LNCS, vol. 2369, Springer, 2002, pp. 120–133.

[324] C. S. Jutla, *On finding small solutions of modular multivariate polynomial equations*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 158–170.

[325] M. Kaib and H. Ritter, *Block reduction for arbitrary norms*, Technical Report, Universität Frankfurt am Main, 1994.

[326] M. Kaib and C.-P. Schnorr, *The generalized Gauss reduction algorithm*, Journal of Algorithms **21** (1996), no. 3, 565–578.

[327] B. S. Kaliski Jr., *Elliptic curves and cryptography: A pseudorandom bit generator and other tools*, Ph.D. thesis, MIT, 1988.

[328] W. van der Kallen, *Complexity of the Havas, Majewski, Matthews LLL Hermite normal form algorithm*, Journal of Symbolic Computation **30** (2000), no. 3, 329–337.

[329] R. Kannan, *Improved algorithms for integer programming and related lattice problems*, Symposium on the Theory of Computing (STOC), ACM, 1983, pp. 193–206.

[330] ———, *Minkowski's convex body theorem and integer programming*, Mathematics of Operations Research **12** (1987), no. 3, 415–440.

[331] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput. **8** (1979), 499–507.

[332] M. Katagi, T. Akishita, I. Kitamura, and T. Takagi, *Some improved algorithms for hyperelliptic curve cryptosystems using degenerate divisors*, ICISC 2004 (C. Park and S. Chee, eds.), LNCS, vol. 3506, Springer, 2004, pp. 296–312.

[333] M. Katagi, I. Kitamura, T. Akishita, and T. Takagi, *Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors*, WISA 2004 (C.-H. Lim and M. Yung, eds.), LNCS, vol. 3325, Springer, 2004, pp. 345–359.

[334] J. Katz and Y. Lindell, *Introduction to modern cryptography*, Chapman & Hall/CRC, 2008.

[335] E. Kiltz and G. Neven, *Identity-based signatures*, Identity-Based Cryptography (M. Joye and G. Neven, eds.), Cryptology and Information Security Series, vol. 2, IOS Press, 2008, pp. 31–44.

[336] J. H. Kim, R. Montenegro, Y. Peres, and P. Tetali, *A birthday paradox for Markov chains, with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm*, ANTS VIII (A. J. van der Poorten and A. Stein, eds.), LNCS, vol. 5011, Springer, 2008, pp. 402–415.

[337] J. H. Kim, R. Montenegro, and P. Tetali, *Near optimal bounds for collision in Pollard rho for discrete log*, Foundations of Computer Science (FOCS), IEEE, 2007, pp. 215–223.

[338] S. Kim and J.-H. Cheon, *A parameterized splitting system and its application to the discrete logarithm problem with low Hamming weight product exponents*, PKC 2008 (R. Cramer, ed.), LNCS, vol. 4939, Springer, 2008, pp. 328–343.

[339] B. King, *A point compression method for elliptic curves defined over GF(2^n)*, PKC 2004 (F. Bao, R. H. Deng, and J. Zhou, eds.), LNCS, vol. 2947, Springer, 2004, pp. 333–345.

[340] J. F. C. Kingman and S. J. Taylor, *Introduction to measure theory and probability*, Cambridge, 1966.

[341] P. N. Klein, *Finding the closest lattice vector when it's unusually close*, Symposium on Discrete Algorithms (SODA), ACM/SIAM, 2000, pp. 937–941.

[342] E. W. Knudsen, *Elliptic scalar multiplication using point halving*, ASIACRYPT 1999 (K.-Y. Lam, E. Okamoto, and C. Xing, eds.), LNCS, vol. 1716, Springer, 1999, pp. 135–149.

[343] D. E. Knuth, *Art of computer programming, Volume 2: semi-numerical algorithms*, 3rd ed., Addison-Wesley, 1997.

[344] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209.

[345] ———, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165.

[346] ———, *Hyperelliptic cryptosystems*, J. Crypt. **1** (1989), 139–150.

[347] ———, *CM curves with good cryptographic properties*, CRYPTO 1991 (J. Feigenbaum, ed.), LNCS, vol. 576, Springer, 1992, pp. 279–287.

[348] ———, *A course in number theory and cryptography*, 2nd ed., GTM 114, Springer, 1994.

[349] C. K. Koç and T. Acar, *Montgomery multplication in GF(2^k)*, Des. Codes Crypt. **14** (1998), no. 1, 57–69.

[350] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.

[351] ———, *Constructive and destructive facets of torus-based cryptography*, Preprint, 2004.

[352] D. R. Kohel and I. E. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 395–404.

[353] S. Kozaki, T. Kutsuma, and K. Matsuo, *Remarks on Cheon's algorithms for pairing-related problems*, Pairing 2007 (T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, eds.), LNCS, vol. 4575, Springer, 2007, pp. 302–316.

[354] M. Kraitchik, *Théorie des nombres, Vol. 1*, Gauthier-Villars, Paris, 1922.

[355] F. Kuhn and R. Struik, *Random walks revisited: Extensions of Pollard's rho algorithm for computing multiple discrete logarithms*, SAC 2001 (S. Vaudenay and A. M. Youssef, eds.), LNCS, vol. 2259, Springer, 2001, pp. 212–229.

[356] R. M. Kuhn, *Curves of genus 2 with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49.

[357] R. Kumar and D. Sivakumar, *Complexity of SVP – a reader's digest*, SIGACT News Complexity Theory Column 32 (2001), 13.

[358] N. Kunihiro and K. Koyama, *Equivalence of counting the number of points on elliptic curve over the ring Z_n and factoring n*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 47–58.

[359] K. Kurosawa and Y. Desmedt, *A new paradigm of hybrid encryption scheme*, CRYPTO 2004 (M. K. Franklin, ed.), LNCS, vol. 3152, Springer, 2004, pp. 426–442.

[360] J. C. Lagarias, *Knapsack public key cryptosystems and diophantine approximation*, CRYPTO 1983 (D. Chaum, ed.), Plenum Press, 1984, pp. 3–23.

[361] J. C. Lagarias, H. W. Lenstra Jr., and C.-P. Schnorr, *Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice*, Combinatorica **10** (1990), no. 4, 333–348.

[362] J. C. Lagarias and A. M. Odlyzko, *Solving low-density subset sum problems*, J. ACM **32** (1985), no. 1, 229–246.

[363] C. Lanczos, *Solution of systems of linear equations by minimized iterations*, J. Res. Nat. Bureau of Standards **49** (1952), 33–53.

[364] S. Lang, *Introduction to algebraic geometry*, Wiley, 1964.

[365] ———, *Algebraic number theory*, GTM, vol. 110, Springer, 1986.

[366] ———, *Elliptic functions*, 2nd ed., GTM, vol. 112, Springer, 1987.

[367] ———, *Algebra*, 3rd ed., Addison-Wesley, 1993.

[368] T. Lange, *Koblitz curve cryptosystems*, Finite Fields Appl. **11** (2005), no. 2, 200–229.

[369] E. Lee, H.-S. Lee, and C.-M. Park, *Efficient and generalized pairing computation on abelian varieties*, IEEE Trans. Information Theory **55** (2009), no. 4, 1793–1803.

[370] A. K. Lenstra, *Factorization of polynomials*, Computational methods in number theory (H. W. Lenstra Jr. and R. Tijdeman, eds.), Mathematical Center Tracts 154, Mathematisch Centrum Amsterdam, 1984, pp. 169–198.

[371] ———, *Integer factoring*, Des. Codes Crypt. **19** (2000), no. 2/3, 101–128.

[372] A. K. Lenstra and H. W. Lenstra Jr., *The development of the number field sieve*, LNM, vol. 1554, Springer, 1993.

[373] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[374] A. K. Lenstra and I. E. Shparlinski, *Selective forgery of RSA signatures with fixed-pattern padding*, PKC 2002 (D. Naccache and P. Paillier, eds.), LNCS, vol. 2274, Springer, 2002, pp. 228–236.

[375] A. K. Lenstra and E. R. Verheul, *The XTR public key system*, CRYPTO 2000 (M. Bellare, ed.), LNCS, vol. 1880, Springer, 2000, pp. 1–19.

[376] ———, *Fast irreducibility and subgroup membership testing in XTR*, PKC 2001 (K. Kim, ed.), LNCS, vol. 1992, Springer, 2001, pp. 73–86.

[377] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), no. 3, 649–673.

[378] ———, *Elliptic curves and number theoretic algorithms*, Proc. International Congr. Math., Berkeley 1986, AMS, 1988, pp. 99–120.

[379] ———, *Finding isomorphisms between finite fields*, Math. Comp. **56** (1991), no. 193, 329–347.

[380] H. W. Lenstra Jr., J. Pila, and C. Pomerance, *A hyperelliptic smoothness test I*, Phil. Trans. R. Soc. Lond. A **345** (1993), 397–408.

[381] H. W. Lenstra Jr. and C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516.

[382] R. Lercier, *Computing isogenies in* F_{2^n}, ANTS II (H. Cohen, ed.), LNCS, vol. 1122, Springer, 1996, pp. 197–212.

[383] R. Lercier and F. Morain, *Algorithms for computing isogenies between elliptic curves*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, vol. 7, AMS, 1998, pp. 77–96.

[384] R. Lercier and T. Sirvent, *On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 783–797.

[385] G. Leurent and P. Q. Nguyen, *How risky is the random oracle model?*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 445–464.

[386] K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, LNM, vol. 1680, Springer, 1998.

[387] W.-C. Li, M. Näslund, and I. E. Shparlinski, *Hidden number problem with the trace and bit security of XTR and LUC*, CRYPTO 2002 (M. Yung, ed.), LNCS, vol. 2442, Springer, 2002, pp. 433–448.

[388] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge, 1994.

[389] ———, *Finite fields*, Cambridge, 1997.

[390] R. Lindner and C. Peikert, *Better key sizes (and attacks) for LWE-based encryption*, CT-RSA 2011 (A. Kiayias, ed.), LNCS, vol. 6558, Springer, 2011, pp. 1–23.

[391] J. H. van Lint, *Introduction to coding theory*, 3rd ed., GTM, vol. 86, Springer, 1999.

[392] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752.

[393] D. L. Long and A. Wigderson, *The discrete logarithm hides O(log n) bits*, SIAM J. Comput. **17** (1988), no. 2, 363–372.

[394] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 106, AMS, 1993.

[395] L. Lovász, *An algorithmic theory of numbers, graphs and convexity*, SIAM, 1986.

[396] L. Lovász and H. E. Scarf, *The generalized basis reduction algorithm*, Mathematics of Operations Research **17** (1992), no. 3, 751–764.

[397] R. Lovorn Bender and C. Pomerance, *Rigorous discrete logarithm computations in finite fields via smooth polynomials*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, vol. 7, AMS, 1998, pp. 221–232.

[398] M. Luby, *Pseudorandomness and cryptographic applications*, Princeton, 1996.

[399] H. Lüneburg, *On a little but useful algorithm*, AAECC-3, 1985 (J. Calmet, ed.), LNCS, vol. 229, Springer, 1986, pp. 296–301.

[400] S. Martín Molleví, P. Morillo, and J. L. Villar, *Computing the order of points on an elliptic curve modulo N is as difficult as factoring N*, Appl. Math. Lett. **14** (2001), no. 3, 341–346.

[401] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.

[402] U. M. Maurer, *Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms*, CRYPTO 1994 (Y. Desmedt, ed.), LNCS, vol. 839, Springer, 1994, pp. 271–281.

[403] ———, *Fast generation of prime numbers and secure public-key cryptographic parameters*, J. Crypt. **8** (1995), no. 3, 123–155.

[404] ———, *Abstract models of computation in cryptography*, IMA Int. Conf. (N. P. Smart, ed.), LNCS, vol. 3796, Springer, 2005, pp. 1–12.

[405] U. M. Maurer and S. Wolf, *Diffie-Hellman oracles*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 268–282.

[406] ———, *On the complexity of breaking the Diffie-Hellman protocol*, Technical Report 244, Institute for Theoretical Computer Science, ETH Zurich, 1996.

[407] ———, *Lower bounds on generic algorithms in groups*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 72–84.

[408] ———, *The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms*, SIAM J. Comput. **28** (1999), no. 5, 1689–1721.

[409] ———, *The Diffie-Hellman protocol*, Des. Codes Crypt. **19** (2000), no. 2/3, 147–171.

[410] A. May, *New RSA vulnerabilities using lattice reduction methods*, Ph.D. thesis, Paderborn, 2003.

[411] ———, *Using LLL-reduction for solving RSA and factorization problems: A survey*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 315–348.

[412] A. May and J. H. Silverman, *Dimension reduction methods for convolution modular lattices*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, Springer, 2001, pp. 110–125.

[413] J. F. McKee, *Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field*, J. London Math. Soc. **59** (1999), no. 2, 448–460.

[414] J. F. McKee and R. G. E. Pinch, *Further attacks on server-aided RSA cryptosystems*, unpublished manuscript, 1998.

[415] W. Meier and O. Staffelbach, *Efficient multiplication on certain non-supersingular elliptic curves*, CRYPTO 1992 (E. F. Brickell, ed.), LNCS, vol. 740, Springer, 1993, pp. 333–344.

[416] A. Menezes and S. A. Vanstone, *The implementation of elliptic curve cryptosystems*, AUSCRYPT 1990 (J. Seberry and J. Pieprzyk, eds.), LNCS, vol. 453, Springer, 1990, pp. 2–13.

[417] A. J. Menezes, T. Okamoto, and S. A. Vanstone, *Reducing elliptic curve logarithms to a finite field*, IEEE Trans. Inf. Theory **39** (1993), no. 5, 1639–1646.

[418] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.

[419] J.-F. Mestre, *La méthode des graphes. exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., 1986, pp. 217–242.

[420] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in algebraic geometry (T. Mora and C. Traverso, eds.), Progress in Mathematics, Birkhäuser, 1991, pp. 313–334.

[421] D. Micciancio, *Improving lattice based cryptosystems using the Hermite normal form*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 126–145.

[422] D. Micciancio and S. Goldwasser, *Complexity of lattice problems: A cryptographic perspective*, Kluwer, 2002.

[423] D. Micciancio and O. Regev, *Lattice-based cryptography*, Post Quantum Cryptography (D. J. Bernstein, J. Buchmann, and E. Dahmen, eds.), Springer, 2009, pp. 147–191.

[424] D. Micciancio and P. Voulgaris, *Faster exponential time algorithms for the shortest vector problem*, SODA (M. Charikar, ed.), SIAM, 2010, pp. 1468–1480.

[425] D. Micciancio and B. Warinschi, *A linear space algorithm for computing the Hermite normal form*, ISSAC, 2001, pp. 231–236.

[426] S. D. Miller and R. Venkatesan, *Spectral analysis of Pollard rho collisions*, ANTS VII (F. Hess, S. Pauli, and M. E. Pohst, eds.), LNCS, vol. 4076, Springer, 2006, pp. 573–581.

[427] V. S. Miller, *Short programs for functions on curves*, Unpublished manuscript, 1986.

[428] ———, *Use of elliptic curves in cryptography*, CRYPTO 1985 (H. C. Williams, ed.), LNCS, vol. 218, Springer, 1986, pp. 417–426.

[429] ———, *The Weil pairing, and its efficient calculation*, J. Crypt. **17** (2004), no. 4, 235–261.

[430] A. Miyaji, T. Ono, and H. Cohen, *Efficient elliptic curve exponentiation*, ICICS 1997 (Y. Han, T. Okamoto, and S. Qing, eds.), LNCS, vol. 1334, Springer, 1997, pp. 282–291.

[431] B. Möller, *Algorithms for multi-exponentiation*, SAC 2001 (S. Vaudenay and A. M. Youssef, eds.), LNCS, vol. 2259, Springer, 2001, pp. 165–180.

[432] ———, *Improved techniques for fast exponentiation*, ICISC 2002 (P.-J. Lee and C.-H. Lim, eds.), LNCS, vol. 2587, Springer, 2003, pp. 298–312.

[433] ———, *Fractional windows revisited: Improved signed-digit representations for efficient exponentiation*, ICISC 2004 (C. Park and S. Chee, eds.), LNCS, vol. 3506, Springer, 2005, pp. 137–153.

[434] R. Montenegro and P. Tetali, *How long does it take to catch a wild kangaroo?*, Symposium on Theory of Computing (STOC), 2009, pp. 553–559.

[435] P. L. Montgomery, *Modular multiplication without trial division*, Math. Comp. **44** (1985), no. 170, 519–521.

[436] ———, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243–264.

[437] F. Morain and J.-L. Nicolas, *On Cornacchia's algorithm for solving the Diophantine equation* $u^2 + dv^2 = m$, Preprint, 1990.

[438] F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, Theoretical Informatics and Applications, vol. 24, 1990, pp. 531–543.

[439] C. J. Moreno, *Algebraic curves over finite fields*, Cambridge, 1991.

[440] W. H. Mow, *Universal lattice decoding: principle and recent advances*, Wireless Communications and Mobile Computing **3** (2003), no. 5, 553–569.

[441] J. A. Muir and D. R. Stinson, *New minimal weight representations for left-to-right window methods*, CT-RSA 2005 (A. Menezes, ed.), LNCS, vol. 3376, Springer, 2005, pp. 366–383.

[442] ———, *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. **75** (2006), no. 253, 369–384.

[443] V. Müller, *Fast multiplication on elliptic curves over small fields of characteristic two*, J. Crypt. **11** (1998), no. 4, 219–234.

[444] D. Mumford, *Abelian varieties*, Oxford, 1970.

[445] ———, *Tata lectures on theta II*, Progess in Mathematics, vol. 43, Birkhäuser, 1984.

[446] M. R. Murty, *Ramanujan graphs*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–20.

[447] R. Murty and I. E. Shparlinski, *Group structure of elliptic curves over finite fields and applications*, Topics in Geometry, Coding Theory and Cryptography (A. Garcia and H. Stichtenoth, eds.), Springer-Verlag, 2006, pp. 167–194.

[448] A. Muzereau, N. P. Smart, and F. Vercauteren, *The equivalence between the DHP and DLP for elliptic curves used in practical applications*, LMS J. Comput. Math. **7** (2004), 50–72.

[449] D. Naccache, D. M'Raïhi, S. Vaudenay, and D. Raphaeli, *Can D.S.A. be improved? Complexity trade-offs with the digital signature standard*, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol. 950, Springer, 1995, pp. 77–85.

[450] D. Naccache and I. E. Shparlinski, *Divisibility, smoothness and cryptographic applications*, Algebraic Aspects of Digital Communications (T. Shaska and E. Hasimaj, eds.), NATO Science for Peace and Security Series, vol. 24, IOS Press, 2009, pp. 115–173.

[451] N.Courtois, M. Finiasz, and N. Sendrier, *How to achieve a McEliece-based digital signature scheme*, ASIACRYPT 2001 (C. Boyd, ed.), LNCS, vol. 2248, Springer, 2001, pp. 157–174.

[452] V. I. Nechaev, *Complexity of a determinate algorithm for the discrete logarithm*, Mathematical Notes **55** (1994), no. 2, 165–172.

[453] G. Neven, N. P. Smart, and B. Warinschi, *Hash function requirements for Schnorr signatures*, J. Math. Crypt. **3** (2009), no. 1, 69–87.

[454] P. Nguyen and D. Stehlé, *Floating-point LLL revisited*, EUROCRYPT 2005 (R. Cramer, ed.), LNCS, vol. 3494, Springer, 2005, pp. 215–233.

[455] ———, *Low-dimensional lattice basis reduction revisited*, ACM Transactions on Algorithms **5** (2009), no. 4:46, 1–48.

[456] P. Q. Nguyen, *Public key cryptanalysis*, Recent Trends in Cryptography (I. Luengo, ed.), AMS, 2009, pp. 67–119.

[457] P. Q. Nguyen and O. Regev, *Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 271–288.

[458] ———, *Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures*, J. Crypt. **22** (2009), no. 2, 139–160.

[459] P. Q. Nguyen and I. E. Shparlinski, *The insecurity of the digital signature algorithm with partially known nonces*, J. Crypt. **15** (2002), no. 3, 151–176.

[460] ———, *The insecurity of the elliptic curve digital signature algorithm with partially known nonces*, Des. Codes Crypt. **30** (2003), no. 2, 201–217.

[461] P. Q. Nguyen and D. Stehlé, *Low-dimensional lattice basis reduction revisited*, ANTS VI (D. A. Buell, ed.), LNCS, vol. 3076, Springer, 2004, pp. 338–357.

[462] P. Q. Nguyen and J. Stern, *Lattice reduction in cryptology: An update*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 85–112.

[463] ———, *The two faces of lattices in cryptology*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 146–180.

[464] P. Q. Nguyen and B. Vallée, *The LLL algorithm: Survey and applications*, Information Security and Cryptography, Springer, 2010.

[465] P. Q. Nguyen and T. Vidick, *Sieve algorithms for the shortest vector problem are practical*, J. Math. Crypt. **2** (2008), no. 2, 181–207.

[466] H. Niederreiter, *A new efficient factorization algorithm for polynomials over small finite fields*, Applicable Algebra in Engineering, Communication and Computing **4** (1993), no. 2, 81–87.

[467] G. Nivasch, *Cycle detection using a stack*, Inf. Process. Lett. **90** (2004), no. 3, 135–140.

[468] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, 1991.

[469] A. M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, EUROCRYPT 1984 (T. Beth, N. Cot, and I. Ingemarsson, eds.), LNCS, vol. 209, Springer, 1985, pp. 224–314.

[470] ———, *The rise and fall of knapsack cryptosystems*, Cryptology and Computational Number Theory (C. Pomerance, ed.), Proc. Symp. Appl. Math., vol. 42, Am. Math. Soc., 1990, pp. 75–88.

[471] T. Okamoto and S. Uchiyama, *A new public-key cryptosystem as secure as factoring*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 308–318.

[472] P. C. van Oorschot and M. J. Wiener, *On Diffie-Hellman key agreement with short exponents*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 332–343.

[473] ———, *Parallel collision search with cryptanalytic applications*, J. Crypt. **12** (1999), no. 1, 1–28.

[474] P. Paillier, *Public-key cryptosystems based on composite degree residuosity classes*, EUROCRYPT 1999 (J. Stern, ed.), LNCS, vol. 1592, Springer, 1999, pp. 223–238.

[475] ———, *Impossibility proofs for RSA signatures in the standard model*, CT-RSA 2007 (M. Abe, ed.), LNCS, vol. 4377, Springer, 2007, pp. 31–48.

[476] P. Paillier and D. Vergnaud, *Discrete-log-based signatures may not be equivalent to discrete log*, ASIACRYPT 2005 (B. K. Roy, ed.), LNCS, vol. 3788, Springer, 2005, pp. 1–20.

[477] P. Paillier and J. L. Villar, *Trading one-wayness against chosen-ciphertext security in factoring-based encryption*, ASIACRYPT 2006 (X. Lai and K. Chen, eds.), LNCS, vol. 4284, Springer, 2006, pp. 252–266.

[478] S. Patel and G. S. Sundaram, *An efficient discrete log pseudo random generator*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 304–317.

[479] S. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp. **68** (1999), no. 227, 1233–1241.

[480] R. Peralta, *Simultaneous security of bits in the discrete log*, EUROCRYPT 1985 (F. Pichler, ed.), LNCS, vol. 219, Springer, 1986, pp. 62–72.

[481] A. K. Pizer, *Ramanujan graphs*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, vol. 7, AMS, 1998, pp. 159–178.

[482] S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Trans. Inf. Theory **24** (1978), 106–110.

[483] D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, J. Crypt. **13** (2000), no. 3, 361–396.

[484] D. Pointcheval and S. Vaudenay, *On provable security for digital signature algorithms*, Technical report LIENS 96-17, École Normale Supérieure, 1996.

[485] J. M. Pollard, *Theorems on factorisation and primality testing*, Proc. Camb. Phil. Soc. **76** (1974), 521–528.

[486] ———, *A Monte Carlo method for factorization*, BIT **15** (1975), 331–334.

[487] ———, *Monte Carlo methods for index computation (mod p)*, Math. Comp. **32** (1978), no. 143, 918–924.

[488] ———, *Kangaroos, Monopoly and discrete logarithms*, J. Crypt. **13** (2000), no. 4, 437–447.

[489] C. Pomerance, *A tale of two sieves*, Notices of the Amer. Math. Soc. **43** (1996), 1473–1485.

[490] V. R. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1974), no. 3, 214–220.

[491] X. Pujol and D. Stehlé, *Rigorous and efficient short lattice vectors enumeration*, ASIACRYPT 2008 (J. Pieprzyk, ed.), LNCS, vol. 5350, Springer, 2008, pp. 390–405.

[492] G. Qiao and K.-Y. Lam, *RSA signature algorithm for microcontroller implementation*, CARDIS 1998 (J.-J. Quisquater and B. Schneier, eds.), LNCS, vol. 1820, Springer, 2000, pp. 353–356.

[493] J. J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electronics Letters (1982), no. 21, 905–907.

[494] M.O. Rabin, *Digitalized signatures and public-key functions as intractable as factorization*, Tech. Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[495] J.-F. Raymond and A. Stiglic, *Security issues in the Diffie-Hellman key agreement protocol*, Preprint, 2000.

[496] O. Regev, *The learning with errors problem (Invited survey)*, 25th Annual IEEE Conference on Computational Complexity, IEEE, 2010, pp. 191–204.

[497] M. Reid, *Undergraduate algebraic geometry*, Cambridge, 1988.

[498] ———, *Graded rings and varieties in weighted projective space*, Chapter of unfinished book, 2002.

[499] G. Reitwiesner, *Binary arithmetic*, Advances in Computers **1** (1960), 231–308.

[500] P. Rogaway, *Formalizing human ignorance*, VIETCRYPT 2006 (P. Q. Nguyen, ed.), LNCS, vol. 4341, Springer, 2006, pp. 211–228.

[501] P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Zeit. **117** (1970), 157–163.

[502] S. Ross, *A first course in probability (6th ed.)*, Prentice Hall, 2001.

[503] K. Rubin and A. Silverberg, *Torus-based cryptography*, CRYPTO 2003 (D. Boneh, ed.), LNCS, vol. 2729, Springer, 2003, pp. 349–365.

[504] ———, *Compression in finite fields and torus-based cryptography*, SIAM J. Comput. **37** (2008), no. 5, 1401–1428.

[505] H.-G. Rück, *A note on elliptic curves over finite fields*, Math. Comp. **49** (1987), no. 179, 301–304.

[506] ———, *On the discrete logarithm in the divisor class group of curves*, Math. Comp. **68** (1999), no. 226, 805–806.

[507] A. Rupp, G. Leander, E. Bangerter, A. W. Dent, and A.-R. Sadeghi, *Sufficient conditions for intractability over black-box groups: Generic lower bounds for generalized DL and DH problems*, ASIACRYPT 2008 (J. Pieprzyk, ed.), LNCS, vol. 5350, Springer, 2008, pp. 489–505.

[508] A.-R. Sadeghi and M. Steiner, *Assumptions related to discrete logarithms: Why subtleties make a real difference*, EUROCRYPT 2001 (B. Pfitzmann, ed.), LNCS, vol. 2045, Springer, 2001, pp. 244–261.

[509] R. Sakai, K. Ohgishi, and M. Kasahara, *Cryptosystems based on pairing*, Symposium on Cryptography and Information Security (SCIS), Okinawa, Japan, 2000.

[510] A. Sárközy and C. L. Stewart, *On pseudorandomness in families of sequences derived from the Legendre symbol*, Periodica Math. Hung. **54** (2007), no. 2, 163–173.

[511] T. Satoh, *On generalization of Cheon's algorithm*, Cryptology ePrint Archive, Report 2009/058, 2009.

[512] T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Comment. Math. Univ. St. Paul. **47** (1998), no. 1, 81–92.

[513] J. Sattler and C.-P. Schnorr, *Generating random walks in groups*, Ann. Univ. Sci. Budapest. Sect. Comput. **6** (1985), 65–79.

[514] A. Schinzel and M. Skałba, *On equations $y^2 = x^n + k$ in a finite field*, Bull. Polish Acad. Sci. Math. **52** (2004), no. 3, 223–226.

[515] O. Schirokauer, *Using number fields to compute logarithms in finite fields*, Math. Comp. **69** (2000), no. 231, 1267–1283.

[516] ———, *The special function field sieve*, SIAM J. Discrete Math **16** (2002), no. 1, 81–98.

[517] ———, *The impact of the number field sieve on the discrete logarithm problem in finite fields*, Algorithmic Number Theory (J. Buhler and P. Stevenhagen, eds.), MSRI publications, vol. 44, Cambridge, 2008, pp. 397–420.

[518] ———, *The number field sieve for integers of low weight*, Math. Comp. **79** (2010), no. 269, 583–602.

[519] O. Schirokauer, D. Weber, and T. F. Denny, *Discrete logarithms: The effectiveness of the index calculus method*, ANTS II (H. Cohen, ed.), LNCS, vol. 1122, Springer, 1996, pp. 337–361.

[520] K. Schmidt-Samoa, O. Semay, and T. Takagi, *Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems*, IEEE Trans. Computers **55** (2006), no. 1, 48–57.

[521] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theor. Comput. Sci. **53** (1987), 201–224.

[522] ———, *Efficient identification and signatures for smart cards*, CRYPTO 1989 (G. Brassard, ed.), LNCS, vol. 435, Springer, 1990, pp. 239–252.

[523] ———, *Efficient signature generation by smart cards*, J. Crypt. **4** (1991), no. 3, 161–174.

[524] ———, *Security of almost all discrete log bits*, Electronic Colloquium on Computational Complexity (ECCC) **5** (1998), no. 33, 1–13.

[525] ———, *Progress on LLL and lattice reduction*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 145–178.

[526] C.-P. Schnorr and M. Euchner, *Lattice basis reduction: Improved practical algorithms and solving subset sum problems*, Math. Program. **66** (1994), 181–199.

[527] C.-P. Schnorr and H. W. Lenstra Jr., *A Monte Carlo factoring algorithm with linear storage*, Math. Comp. **43** (1984), no. 167, 289–311.

[528] R. Schoof, *Elliptic curves over finite fields and the computation of square roots* (mod *) p*, Math. Comp. **44** (1985), no. 170, 483–494.

[529] ———, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), 183–211.

[530] ———, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), 219–254.

[531] A. Schrijver, *Theory of linear and integer programming*, Wiley, 1986.

[532] R. Schroeppel, H. K. Orman, S. W. O'Malley, and O. Spatscheck, *Fast key exchange with elliptic curve systems*, CRYPTO 1995 (D. Coppersmith, ed.), LNCS, vol. 963, Springer, 1995, pp. 43–56.

[533] E. Schulte-Geers, *Collision search in a random mapping: Some asymptotic results*, Presentation at ECC 2000, Essen, Germany, 2000.

[534] M. Scott, *Faster pairings using an elliptic curve with an efficient endomorphism*, INDOCRYPT 2005 (S. Maitra, C. E. V. Madhavan, and R. Venkatesan, eds.), LNCS, vol. 3797, Springer, 2005, pp. 258–269.

[535] R. Sedgewick, T. G. Szymanski, and A. C.-C. Yao, *The complexity of finding cycles in periodic functions*, SIAM J. Comput. **11** (1982), no. 2, 376–390.

[536] B. I. Selivanov, *On waiting time in the scheme of random allocation of coloured particles*, Discrete Math. Appl. **5** (1995), no. 1, 73–82.

[537] I. A. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. **67** (1998), no. 221, 353–356.

[538] ———, *A 3-dimensional lattice reduction algorithm*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 181–193.

[539] ———, *Summation polynomials and the discrete logarithm problem on elliptic curves*, Cryptology ePrint Archive, Report 2004/031, 2004.

[540] G. Seroussi, *Compact representation of elliptic curve points over F_{2^n}*, Hewlett-Packard Labs technical report HPL-98-94, 1998.

[541] J.-P. Serre, *Sur la topologie des variétés algébriques en charactéristique p*, Symp. Int. Top. Alg., Mexico, 1958, pp. 24–53.

[542] ———, *Local fields*, GTM, vol. 67, Springer, 1979.

[543] I. R. Shafarevich, *Basic algebraic geometry*, 2nd ed., Springer, 1995.

[544] J. O. Shallit, *A primer on balanced binary representations*, Preprint, 1992.

[545] A. Shallue and C. E. van de Woestijne, *Construction of rational points on elliptic curves over finite fields*, ANTS VII (F. Hess, S. Pauli, and M. E. Pohst, eds.), LNCS, vol. 4076, Springer, 2006, pp. 510–524.

[546] A. Shamir, *A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem*, IEEE Trans. Inf. Theory **30** (1984), no. 5, 699–704.

[547] ———, *Identity based cryptosystems and signature schemes*, CRYTO 1984 (G. R. Blakley and D. Chaum, eds.), LNCS, vol. 196, Springer, 1985, pp. 47–53.

[548] ———, *RSA for paranoids*, Cryptobytes **1** (1995), no. 3, 1–4.

[549] D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, Congressus Numerantium, No. VII, Utilitas Math., Winnipeg, Man., 1973, pp. 51–70.

[550] T. Shioda, *On the graded ring of invariants of binary octavics*, Am. J. Math. **89** (1967), no. 4, 1022–1046.

[551] M. Shirase, D.-G. Han, Y. Hibino, H.-W. Kim, and T. Takagi, *Compressed XTR*, ACNS 2007 (J. Katz and M. Yung, eds.), LNCS, vol. 4521, Springer, 2007, pp. 420–431.

[552] Z. Shmuely, *Composite Diffie-Hellman public-key generating systems are hard to break*, Technical report No. 356, Computer Science Department, Technion, 1985.

[553] V. Shoup, *Lower bounds for discrete logarithms and related problems*, EUROCRYPT 1997 (W. Fumy, ed.), LNCS, vol. 1233, Springer, 1997, pp. 256–266.

[554] ———, *On formal models for secure key exchange (version 4), November 15, 1999*, Tech. report, IBM, 1999, Revision of Report RZ 3120.

[555] ———, *OAEP reconsidered*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 239–259.

[556] ———, *A computational introduction to number theory and algebra*, Cambridge, 2005.

[557] I. E. Shparlinski, *Computing Jacobi symbols modulo sparse integers and polynomials and some applications*, J. Algorithms **36** (2000), 241–252.

[558] ———, *Cryptographic applications of analytic number theory*, Birkhauser, 2003.

[559] ———, *Playing "hide-and-seek" with numbers: The hidden number problem, lattices and exponential sums*, Public-Key Cryptography (P. Garrett and D. Lieman, eds.), Proceedings of Symposia in Applied Mathematics, vol. 62, AMS, 2005, pp. 153–177.

[560] I. E. Shparlinski and A. Winterhof, *A nonuniform algorithm for the hidden number problem in subgroups*, PKC 2004 (F. Bao, R. H. Deng, and J. Zhou, eds.), LNCS, vol. 2947, Springer, 2004, pp. 416–424.

[561] ———, *A hidden number problem in small subgroups*, Math. Comp. **74** (2005), no. 252, 2073–2080.

[562] A. Sidorenko, *Design and analysis of provably secure pseudorandom generators*, Ph.D. thesis, Eindhoven, 2007.

[563] C. L. Siegel, *Lectures on the geometry of numbers*, Springer, 1989.

[564] J. H. Silverman, *The arithmetic of elliptic curves*, GTM, vol. 106, Springer, 1986.

[565] ———, *Advanced topics in the arithmetic of elliptic curves*, GTM, vol. 151, Springer, 1994.

[566] J. H. Silverman and J. Suzuki, *Elliptic curve discrete logarithms and the index calculus*, ASIACRYPT 1998 (K. Ohta and D. Pei, eds.), LNCS, vol. 1514, Springer, 1998, pp. 110–125.

[567] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, 1994.

[568] M. Sipser, *Introduction to the theory of computation*, Course Technology, 2005.

[569] M. Skałba, *Points on elliptic curves over finite fields*, Acta Arith. **117** (2005), no. 3, 293–301.

[570] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, J. Cryptology **12** (1999), no. 3, 193–196.

[571] ———, *Elliptic curve cryptosystems over small fields of odd characteristic*, J. Crypt. **12** (1999), no. 2, 141–151.

[572] ———, *Cryptography: An introduction*, McGraw-Hill, 2004.

[573] B. A. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, J. Crypt. **22** (2009), no. 4, 505–529.

[574] P. J. Smith and M. J. J. Lennon, *LUC: A new public key system*, International Conference on Information Security (E. Graham Dougall, ed.), IFIP Transactions, vol. A-37, North-Holland, 1993, pp. 103–117.

[575] P. J. Smith and C. Skinner, *A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms*, ASIACRYPT 1994 (J. Pieprzyk and R. Safavi-Naini, eds.), LNCS, vol. 917, Springer, 1994, pp. 357–364.

[576] J. A. Solinas, *Efficient arithmetic on Koblitz curves*, Des. Codes Crypt. **19** (2000), 195–249.

[577] ———, *Low-weight binary representations for pairs of integers*, Technical Report CORR 2001-41, 2001.

[578] M. Stam, *On Montgomery-like representations of elliptic curves over GF*(2^k), PKC 2003 (Y. G. Desmedt, ed.), LNCS, vol. 2567, Springer, 2003, pp. 240–253.

[579] ———, *Speeding up subgroup cryptosystems*, Ph.D. thesis, Eindhoven, 2003.

[580] M. Stam and A. K. Lenstra, *Speeding up XTR*, ASIACRYPT 2001 (C. Boyd, ed.), LNCS, vol. 2248, Springer, 2001, pp. 125–143.

[581] H. M. Stark, *Class-numbers of complex quadratic fields*, Modular Functions of One Variable I (W. Kuyk, ed.), LNM, vol. 320, Springer, 1972, pp. 153–174.

[582] D. Stehlé, *Floating point LLL: Theoretical and practical aspects*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 179–213.

[583] D. Stehlé and P. Zimmermann, *A binary recursive GCD algorithm*, ANTS VI (D. A. Buell, ed.), LNCS, vol. 3076, Springer, 2004, pp. 411–425.

[584] P. Stevenhagen, *The number field sieve*, Algorithmic number theory (J. Buhler and P. Stevenhagen, eds.), MSRI publications, Cambridge, 2008, pp. 83–99.

[585] I. Stewart, *Galois theory*, 3rd ed., Chapman & Hall, 2003.

[586] I. Stewart and D. Tall, *Algebraic number theory and Fermat's last theorem*, 3rd ed., AK Peters, 2002.

[587] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. **24** (1973), 527–544.

[588] ———, *Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers*, Arch. Math. **33** (1979), 357–360.

[589] ———, *Algebraic function fields and codes*, Springer, 1993.

[590] H. Stichtenoth and C. Xing, *On the structure of the divisor class group of a class of curves over finite fields*, Arch. Math, **65** (1995), 141–150.

[591] D. R. Stinson, *Some baby-step giant-step algorithms for the low Hamming weight discrete logarithm problem*, Math. Comp. **71** (2001), no. 237, 379–391.

[592] ———, *Cryptography: Theory and practice*, 3rd ed., Chapman & Hall/CRC, 2005.

[593] A. Storjohann and G. Labahn, *Asymptotically fast computation of Hermite normal forms of integer matrices*, ISSAC 1996, ACM Press, 1996, pp. 259–266.

[594] E. G. Straus, *Addition chains of vectors*, American Mathematical Monthly **71** (1964), no. 7, 806–808.

[595] A. H. Suk, *Cryptanalysis of RSA with lattice attacks*, MSc thesis, University of Illinois at Urbana-Champaign, 2003.

[596] A. V. Sutherland, *Order computations in generic groups*, Ph.D. thesis, MIT, 2007.

[597] ———, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538.

[598] ———, *Structure computation and discrete logarithms in finite abelian p-groups*, Math. Comp. **80** (2011), no. 273, 477–500.

[599] T. Takagi, *Fast RSA-type cryptosystem modulo $p^k q$*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 318–326.

[600] J. Talbot and D. Welsh, *Complexity and cryptography: An introduction*, Cambridge, 2006.

[601] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[602] ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminarie Bourbaki 1968/69, LNM, vol. 179, Springer, 1971, pp. 95–109.

[603] E. Teske, *A space efficient algorithm for group structure computation*, Math. Comp. **67** (1998), no. 224, 1637–1663.

[604] ———, *Speeding up Pollard's rho method for computing discrete logarithms*, ANTS III (J. P. Buhler, ed.), LNCS, vol. 1423, Springer, 1998, pp. 541–554.

[605] ———, *On random walks for Pollard's rho method*, Math. Comp. **70** (2001), no. 234, 809–825.

[606] ———, *Computing discrete logarithms with the parallelized kangaroo method*, Discrete Applied Mathematics **130** (2003), 61–82.

[607] N. Thériault, *Index calculus attack for hyperelliptic curves of small genus*, ASIACRYPT 2003 (C.-S. Laih, ed.), LNCS, vol. 2894, Springer, 2003, pp. 75–92.

[608] E. Thomé, *Algorithmes de calcul de logarithmes discrets dans les corps finis*, Ph.D. thesis, L'École Polytechnique, 2003.

[609] W. Trappe and L. C. Washington, *Introduction to cryptography with coding theory*, 2nd ed., Pearson, 2005.

[610] M. A. Tsfasman, *Group of points of an elliptic curve over a finite field*, Theory of numbers and its applications,. Tbilisi, 1985, pp. 286–287.

[611] J. W. M. Turk, *Fast arithmetic operations on numbers and polynomials*, Computational methods in number theory, Part 1 (H. W. Lenstra Jr. and R. Tijdeman, eds.), Mathematical Centre Tracts 154, Amsterdam, 1984.

[612] M. Ulas, *Rational points on certain hyperelliptic curves over finite fields*, Bull. Pol. Acad. Sci. Math. **55** (2007), no. 2, 97–104.

[613] B. Vallée, *Une approche géométrique de la réduction de réseaux en petite dimension*, Ph.D. thesis, Université de Caen, 1986.

[614] ———, *Gauss' algorithm revisited*, J. Algorithms **12** (1991), no. 4, 556–572.

[615] S. Vaudenay, *Hidden collisions on DSS*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 83–88.

[616] ———, *A classical introduction to cryptography*, Springer, 2006.

[617] J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris **273** (1971), 238–241.

[618] F. Vercauteren, *Optimal pairings*, IEEE Trans. Inf. Theory **56** (2010), no. 1, 455–461.

[619] E. R. Verheul, *Certificates of recoverability with scale recovery agent security*, PKC 2000 (H. Imai and Y. Zheng, eds.), LNCS, vol. 1751, Springer, 2000, pp. 258–275.

[620] ———, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Crypt. **17** (2004), no. 4, 277–296.

[621] E. R. Verheul and H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Applicable Algebra in Engineering, Communication and Computing **8** (1997), no. 5, 425–435.

[622] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, LNM, vol. 800, Springer, 1980.

[623] J. F. Voloch, *A note on elliptic curves over finite fields*, Bulletin de la Société Mathématique de France **116** (1988), no. 4, 455–458.

[624] ———, *Jacobians of curves over finite fields*, Rocky Mountain Journal of Math. **30** (2000), no. 2, 755–759.

[625] D. Wagner, *A generalized birthday problem*, CRYPTO 2002 (M. Yung, ed.), LNCS, vol. 2442, Springer, 2002, pp. 288–303.

[626] L. C. Washington, *Elliptic curves: Number theory and cryptography*, 2nd ed., CRC Press, 2008.

[627] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560.

[628] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458.

[629] D. H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inf. Theory **32** (1986), 54–62.

[630] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inf. Theory **36** (1990), no. 3, 553–558.

[631] ———, *Bounds on birthday attack times*, Cryptology ePrint Archive, Report 2005/318, 2005.

[632] M. J. Wiener and R. J. Zuccherato, *Faster attacks on elliptic curve cryptosystems*, SAC 1998 (S. E. Tavares and H. Meijer, eds.), LNCS, vol. 1556, Springer, 1998, pp. 190–200.

[633] H. C. Williams, *A modification of the RSA public key encryption procedure*, IEEE Trans. Inf. Theory **26** (1980), no. 6, 726–729.

[634] ———, *A $p+1$ method of factoring*, Math. Comp. **39** (1982), no. 159, 225–234.

[635] D. J. Winter, *The structure of fields*, GTM 16, Springer, 1974.

[636] M. Woodroofe, *Probability with applications*, McGraw-Hill, 1975.

[637] S.-M. Yen and C.-S. Laih, *Improved digital signature suitable for batch verification*, IEEE Trans. Computers **44** (1995), no. 7, 957–959.

[638] S.-M. Yen, C.-S. Laih, and A. K. Lenstra, *Multi-exponentiation*, IEEE Proceedings Computers and Digital Techniques **141** (1994), no. 6, 325–326.

[639] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$*, J. Algebra **52** (1978), 378–410.

[640] O. Zariski and P. Samuel, *Commutative algebra (Vol. I and II)*, Van Nostrand, Princeton, 1960.

[641] N. Zierler, *A conversion algorithm for logarithms on $GF(2^n)$*, Journal of Pure and Applied Algebra **4** (1974), 353–356.

[642] P. Zimmermann, *Private communication*, March 10, 2009.

Author Index

Subject Index