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

$$2\phi_3(x) = -\widetilde{a}_1\phi_1(x) - \widetilde{a}_3 + (a_1x + a_3)\phi_2(x).$$

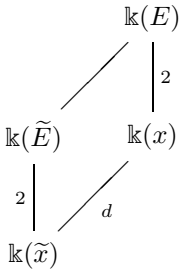
□

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 $y^2 = x^3 + a_4x$ 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 $E : y^2 = x^3 + a_4x$ 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 $x_3 4By_1^2 = (3x_1^2+2Ax_1+1)^2 - (A+2x_1)4By_1^2$, 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.