Limitations of Constructive Weil Descent

Steven D. Galbraith *
Department of Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Rd, Bristol BS8 1UB, UK.
steven@cs.bris.ac.uk

1991 Mathematics Subject Classification: 11G20, 14G15, 14G50

Abstract. Weil restriction of scalars can be used to construct curves suitable for cryptography whose Jacobian has known group order. The description given by Hess, Seroussi and Smart shows how to construct hyperelliptic curves of genus two or three over finite fields of characteristic two. One drawback of their method is discussed, namely that only a small proportion of the set of all curves can be constructed in this way. We also indicate that the method cannot be generalised to overcome this drawback.

1. Introduction

Jacobians of hyperelliptic curves (and also some more general higher genus curves) have been proposed for use in public key cryptography. However, an impediment to their use has been the problem of computing the number of points on the Jacobian variety of a curve. The currently available methods for finding a curve of genus $2 \leq g \leq 4$ over a finite field whose Jacobian has known order are:

- Using subfield curves (i.e., curves C defined over a small field $\mathbb{F}_q$ but considering their Jacobian as a group over some larger extension field $\mathbb{F}_{q^l}$).
- Using curves with known endomorphism structure.
- Choosing curves at random and counting points using baby-step-giant-step, Pollard or Schoof style methods.

*This research was supported by the NRW-Initiative für Wissenschaft und Wirtschaft “Innovationscluster für Neue Medien” and cv cryptovision gmbh (Gelsenkirchen).

- Using modular curves.
- Constructive Weil descent.

The first method was initially described by Koblitz [12] and has since been used in several other papers. As a means of computing the number of points on a Jacobian it is very effective.

The second method appears in several forms. The most advanced is the method of Spallek [14] (also see Weng [17]) which is an analogue of the CM method for elliptic curves. This method has only been developed over fields of odd characteristic. Nevertheless, it has been used to generate curves suitable for cryptography. There are many other papers which give methods for counting points on certain curves which have a special endomorphism structure.

The main drawback of both of these methods is that the curves have special properties and are thus treated with some suspicion by the community. Admittedly the only known weakness of these curves is that their automorphism structures allow the use of equivalence classes to speed up the Pollard methods (see [2]).

The third method would allow the choice of truly random curves. In the elliptic curve case there are efficient methods for counting points and so this is the method which is used in most applications. Unfortunately, despite the best efforts of Gaudry and Harley [8], this method is not practical when the genus is two or more.

Modular curves have a lot of structure which can be used to help count their points (see [4]). The algorithms for computing the coefficients of weight two modular forms have exponential complexity in terms of q so, in the case of genus less than or equal to four, modularity alone is not enough for efficient point counting. Gaudry (see Section 6.2 of [10]) has used the real multiplication structure of modular curves to accelerate point counting. Nevertheless, modular curves are special and so these methods cannot be used to produce random curves.

The fifth method, that of constructive Weil descent, seems to be an excellent solution to the problem. The seeds for this idea were sown by Frey [3]. The paper of Hess, Seroussi and Smart [11] gives a construction for genus two and three curves over fields of characteristic two and this is the only known method for generating curves over such fields (i.e., not subfield curves) with known group order. Furthermore, constructive Weil descent can produce $O(q^{g/2})$ curves of genus $g \in \{2, 3\}$ whereas the CM and subfield curve methods produce what is, in practice, essentially a constant number of curves.

Unfortunately, the curves which arise from constructive Weil descent do have special properties and are not 'random hyperelliptic curves' in the most general sense. The goal of this paper to give evidence that only a small proportion of all isogeny classes of Jacobians of hyperelliptic curves can be constructed using Weil descent.

Furthermore, we hope to convince the reader that any generalisation of constructive Weil descent to produce curves of any form (i.e., not necessarily hyperelliptic) will also only produce a small proportion of the available isogeny classes of curves. Indeed, our results suggest that most isogeny classes of Jacobians of curves do not arise as a sub-abelian-variety of the Weil restriction of an elliptic curve.

In conclusion, though constructive Weil descent is an interesting new technique, it cannot provide a general solution to the problem of constructing curves of genus $g \geq 2$ suitable for cryptography.

2. Summary of constructive Weil descent

Frey [3] was the first to observe that Weil restriction of scalars could be used as a tool to find curves whose Jacobian has known order (for details about Weil descent see [3], [4], [5], [9]). From a practical point of view the decisive step is the paper of Hess, Seroussi and Smart [11], which we now outline.

In [11] the goal is to find a hyperelliptic curve C over a finite field $\mathbb{F}_q$ of genus $g \in \{2, 3\}$ where $q = 2^l$. The method proceeds as follows:

- Choose non-supersingular elliptic curves E over $\mathbb{F}_{q^g}$ at random (though there are some restrictions on E in the case of $g = 3$) and count their points (using the Schoof-Elkies-Atkin algorithm or Satoh's algorithm) until one is found such that the number of points on E is a product of a small number and a large prime.
- Construct a curve C of genus g on the Weil restriction of scalars A of E with respect to the extension $\mathbb{F}_{q^g}/\mathbb{F}_q$ using the method of Gaudry, Hess and Smart [9].

One then knows the order of $\mathrm{Jac}(C)(\mathbb{F}_q)$ as it will be the same as the number of points on $E(\mathbb{F}_{q^g})$.

The main drawback of this method is that the Jacobians produced are isogenous to the Weil restriction of the elliptic curve E. In other words, they are essentially a different way of writing down the elliptic curve group $E(\mathbb{F}_{q^g})$ and their security is no more than the security of the original elliptic curve discrete logarithm problem.

3. The curves produced by constructive Weil descent

We now give several reasons why constructive Weil descent as above produces curves which are very special compared with a general hyperelliptic curve. These ideas are well known to researchers in algebraic geometry, but we feel it is worth explaining them to the wider cryptographic community.

First consider the number of isomorphism classes of curves produced by this method. We get only one isomorphism class of curves C from each isomorphism class of elliptic curves E, since the function field of C is determined up to isomorphism. The moduli space of hyperelliptic curves of genus g has dimension $2g-1$. It is difficult to derive precise estimates about the number of points on a space solely by considering its dimension. We estimate the number of hyperelliptic curves of genus g over a field $\mathbb{F}_q$ to be $\Omega(q^{2g-1})$. There are roughly $2q^n$ isomorphism classes of elliptic curves over $\mathbb{F}_{q^n}$. We therefore conclude that the proportion of isomorphism classes of genus two curves which can arise from constructive Weil descent is at most c/q for some constant c. For genus three curves we expect that at most c'/q^2 of all genus three curves can arise in this way for some constant c'.

The difficulty of the discrete logarithm problem seems to be more closely related to the isogeny class than the isomorphism class, therefore it makes more sense to estimate the proportion of isogeny classes which can be produced by constructive Weil descent. We study these questions via the characteristic polynomial of Frobenius.

Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$. Associated to A is the characteristic polynomial $P_A(T)$ of the Frobenius endomorphism. Tate's isogeny theorem [15] implies that two abelian varieties A and B over a finite field $\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if the polynomials $P_A(T)$ and $P_B(T)$ are equal.

Our first step is to understand the abelian varieties which arise from taking Weil restriction of scalars.

Proposition 3.1. *Let $A/\mathbb{F}_{q^n}$ be an abelian variety with characteristic polynomial of Frobenius equal to $P_A(T)$. Let $B/\mathbb{F}_q$ be the Weil restriction of A with respect to the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then $P_B(T) = P_A(T^n)$.*

Proof. The Frobenius endomorphism on A is just the nth power of the Frobenius endomorphism on B. $\square$

We observe the following easy corollary to the above result.

Corollary 3.2. *Let the notation be as above. If $\gcd(m,n) = 1$ then $\#A(\mathbb{F}_{q^{mn}}) = \#B(\mathbb{F}_{q^m})$. If $n|m$ then $\#B(\mathbb{F}_{q^m}) = (\#A(\mathbb{F}_{q^{m/n}}))^n$.*

Proof. Let $\zeta_n = \exp(2\pi\sqrt{-1}/n)$ and let $P_A(T) = \prod_{i=1}^{2g}(1-\alpha_i)$. Then $P_B(T) = \prod_i \prod_{j=1}^{n}(1-\zeta_n^j \alpha_i^{1/n})$ and $\#B(\mathbb{F}_{q^m}) = \prod_i \prod_j (1-\zeta_n^{mj}\alpha_i^{m/n})$. $\square$

When $\gcd(m,n) = 1$ then it is the case that the groups $A(\mathbb{F}_{q^{nm}})$ and $B(\mathbb{F}_{q^m})$ are isomorphic.

We return to the curves produced by the method of [11]. The original elliptic curve E over $\mathbb{F}_{q^g}$ has $P_E(T) = T^2 + aT + q^n$ (with $|a| < 2\sqrt{q^g}$) and so, by Proposition 3.1, the abelian variety A has char poly $P_A(T) = T^{2g} + aT^g + q^g$. If E is non-supersingular then a is coprime to q and so A is also non-supersingular (see [7]). In the construction of [11] we have $\mathrm{Jac}(C)$ isogenous to A and so it has the same polynomial $P(T)$. This proves the following result.

Proposition 3.3. *Let $g \in \{2,3\}$ and let q be a power of 2. Then constructive Weil descent as in [11] produces at most $2\sqrt{q^g}$ isogeny classes of Jacobian varieties of hyperelliptic curves of genus g over $\mathbb{F}_q$.*

A general abelian variety A of dimension n over $\mathbb{F}_q$ has characteristic polynomial of Frobenius $P_A(T)$ equal to

$$T^{2n} + a_1 T^{2n-1} + a_2 T^{2n-2} + \cdots + a_n T^n + q a_{n-1} T^{n-1} + \cdots + a_1 q^{n-1} T + q^n$$

where the coefficients $a_i \in \mathbb{Z}$ are constrained by various complicated conditions. There are $O(\binom{2g}{i} q^{i/2})$ possibilities for each a_i. Thus there are $O(q^{3/2})$ isogeny classes of abelian varieties of dimension two over $\mathbb{F}_q$ and $O(q^3)$ isogeny classes of abelian varieties of dimension three over $\mathbb{F}_q$.

For cryptography, groups whose order has a very large prime factor are the most important. Thus the abelian varieties we consider in this paper are simple, or in other words, the characteristic polynomial of Frobenius is irreducible. Of course, a simple abelian variety does not necessarily have an 'almost prime' order. In the analysis below we pay attention to simplicity but disregard the issue of whether the order has a large prime factor.

Rück [13] has shown, for abelian varieties of dimension two over prime fields $\mathbb{F}_p$, that 'most' are simple and that 'most' are isogenous over $\mathbb{F}_p$ to the Jacobian of a hyperelliptic curve $C/\mathbb{F}_p$. We expect that similar results hold for more general finite fields $\mathbb{F}_q$, but a proof of this is beyond the scope of the present work. Therefore we expect $O(q^{3/2})$ isogeny classes of simple Jacobians of genus two curves over $\mathbb{F}_q$. On the other hand, the constructive Weil descent method can only produce $O(q)$ such curves. This is an exponentially small proportion of all isogeny classes.

The majority of abelian varieties of dimension three are simple. In the case of dimension three we also expect that most abelian varieties over $\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ to the Jacobian of a curve. Hence we expect $O(q^3)$ isogeny classes of Jacobians of genus three curves over $\mathbb{F}_q$. However, a genus three curve can be a plane quartic or a hyperelliptic curve. It is not clear what is the proportion of isogeny classes of hyperelliptic genus three curves. In any case, constructive Weil descent only produces $O(q^{3/2})$ isogeny classes of hyperelliptic curves, and we expect this to be an exponentially small proportion of all isogeny classes of hyperelliptic curves.

4. Experimental evidence

We now give some data for small fields $\mathbb{F}_{2^n}$ (essentially obtained by a brute-force search). Here $N_1(q)$ is the number of isogeny classes of Jacobians of genus two curves over $\mathbb{F}_q$. $N_2(q)$ is the number of classes as in N_1 for which the Jacobian is non-supersingular and simple (the abelian variety is simple if and only if the characteristic polynomial of Frobenius is irreducible). $N_3(q)$ is the number of classes as in N_2 but with the further condition that there is a curve representing the class which can be written in the form with a single point at infinity. Finally, $N_4(q)$ is the number of classes as above which can be constructed from the Weil restriction of an elliptic curve over $\mathbb{F}_{q^2}$.

q	$N_1(q)$	$N_2(q)$	$N_3(q)$	$N_4(q)$
2	20	12	6	2
4	70	46	21	4
8	≥ 160	≥ 121	56	10
16	≥ 415	≥ 366	≥ 168	24

The most important columns for the present discussion are $N_3(q)$ and $N_4(q)$, since the method of [11] produces curves which satisfy the conditions imposed in the definition of $N_3(q)$. It is seen that $N_3(q)$ is growing significantly faster than $N_4(q)$. This suggests that constructive Weil descent only produces a small proportion of the possible isogeny classes of curves.

Here is the analogous data for hyperelliptic genus three curves over $\mathbb{F}_{2^n}$. In this case $N_1(q)$ is the number of isogeny classes of Jacobians of hyperelliptic genus three curves over $\mathbb{F}_q$ and the other $N_i(q)$ are defined analogously.

q	$N_1(q)$	$N_2(q)$	$N_3(q)$	$N_4(q)$
2	59	32	24	2
4	≥ 420	≥ 200	≥ 145	6

In conclusion we see that a rather small proportion of isogeny classes of simple non-supersingular Jacobians of hyperelliptic curves with one point at infinity of genus two or three arise as the Weil restriction of an elliptic curve.

5. Generalising the construction of Hess, Seroussi and Smart

The natural strategy to overcome the problem mentioned above is the following: Rather than constructing the Weil restriction A of an elliptic curve and asking for it to be isogenous to the Jacobian of a curve C, we could ask for $\mathrm{Jac}(C)$ to be a sub-abelian-variety of A.

It is conceivable that the construction of [11] could be modified to give such a method. One key modification would be to search for elliptic curves $E/\mathbb{F}_{q^n}$ such that the characteristic polynomial of Frobenius of the Weil restriction has a factor corresponding to a g-dimensional sub-abelian-variety which has suitable order. It is then plausible that methods related to those of [9] would allow the construction of a genus g curve whose Jacobian is isogenous to that factor. One might hope that this strategy would give a much larger class of suitable curves.

For example, over $\mathbb{F}_2$ we find four new isogeny classes of two-dimensional abelian varieties. These classes correspond to the degree four factors in the following factorisations:

$$\begin{aligned}
T^6 - 5T^3 + 2^3 &= (T^4 - T^3 - T^2 - 2T + 4)(T^2 + T + 2) \\
T^6 + 5T^3 + 2^3 &= (T^4 + T^3 - T^2 + 2T + 4)(T^2 - T + 2) \\
T^{12} + 11T^6 + 2^6 &= (T^4 - 3T^3 + 5T^2 - 6T + 4)(T^4 - T^2 + 4) \\
&\quad (T^4 + 3T^3 + 5T^2 + 6T + 4).
\end{aligned}$$

We now give a small table of results for genus 2 curves over $\mathbb{F}_{2^n}$. Here, as before $N_4(q)$ is the number of non-supersingular, simple Jacobians of curves of genus two over $\mathbb{F}_q$ which can be constructed from Weil descent of an elliptic curve with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$. The quantity $N_5(q)$ is the number of isogeny classes of non-supersingular, simple abelian varieties of dimension two over $\mathbb{F}_q$ which are isogenous to a factor of the Weil descent of an elliptic curve with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$ with $n \leq 6$. We do not know if all such abelian varieties are isogenous to the Jacobian of a curve over $\mathbb{F}_q$. Experimental evidence suggests that taking $n > 6$ yields no new examples.

q	$N_4(q)$	$N_5(q)$
2	2	4
4	4	6
8	10	10
16	24	12
32	52	18

This data indicates that we do not obtain a significant number of new isogeny classes from this generalised approach. This phenomenon is also observed in the genus three case. If the generalised construction is used to produce curves which are not hyperelliptic (for instance, superelliptic curves [6] or more general curves) then it will still be true that only a small proportion of the available isogeny classes of curves will appear.

6. The curves produced by the generalised method

In this section we prove some results about the genus two curves which would arise from the generalised method outlined in Section 5. All results in this section apply only to the case of characteristic two and genus two. The main result is that the genus two curves which would be produced by the generalised method (and which would not have been produced from the original method of [11]) do not have an equation with a single point at infinity.

Lemma 6.1. *Let $q = 2^l$ and let C be a hyperelliptic curve of genus 2 over $\mathbb{F}_q$ whose Jacobian has characteristic polynomial equal to $P(T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$. If C can be given a hyperelliptic model over $\mathbb{F}_q$ with a single point at infinity then at least one of a_1 or a_2 is even. If all hyperelliptic models of C over $\mathbb{F}_q$ have two points at infinity then both a_1 and a_2 are odd.*

Proof. (Note that the method of proof of this Lemma is similar to that used in the proof of Lemma 9.1 of [7]). Let C have equation $y^2 + h(x)y = f(x)$ where $\deg h(x) \leq 3$ and $\deg f(x) \leq 6$. Then for each point (x_0, y_0) on C there is the conjugate under the hyperelliptic involution given by $(x_0, y_0 + h(x_0))$. The fixed points of the hyperelliptic involution arise from the solutions to $h(x) = 0$.

The set $C(\mathbb{F}_q)$ therefore consists of the $\mathbb{F}_q$-points at infinity, the $\mathbb{F}_q$-points fixed by the involution, and the remaining $\mathbb{F}_q$-points which all occur in pairs.

We now consider the possible equations for genus two curves over $\mathbb{F}_{2^l}$. The cases where there is one point at infinity are when $\deg(h(x)) \leq 2$ and so we can have the four subcases: $\deg(h(x)) = 0$, $\deg(h(x)) = 1$, $\deg(h(x)) = 2$ and $h(x)$ splits into linear factors, $\deg(h(x)) = 2$ and $h(x)$ has no roots in $\mathbb{F}_{2^l}$. The number of points on C over $\mathbb{F}_q$ in the first, third and fourth subcases is therefore odd, and so $a_1 = q + 1 - \#C(\mathbb{F}_q)$ is even. In the second subcase we have $\#C(\mathbb{F}_q)$ even so we must consider $\#C(\mathbb{F}_{q^2})$. Write x_0 for the root of $h(x)$. Every $x_1 \in \mathbb{F}_q \backslash \{x_0\}$ gives rise to two points $(x_1, y_1), (x_1, y_1 + h(x_1))$ in $C(\mathbb{F}_{q^2})$. Furthermore, points $(x_2, y_2) \in C(\mathbb{F}_{q^2})$ for which $x_2 \notin \mathbb{F}_q$ come in groups of four conjugates with $(x_2, y_2 + h(x_2)), (x_2^\sigma, y_2^\sigma), (x_2^\sigma, y_2^\sigma + h(x_2^\sigma))$. Thus $\#C(\mathbb{F}_{q^2}) = 1 + 1 + 2(q-1) + 4m \equiv 0 \pmod 4$ and so $a_2 = \frac{1}{2}((\#C(\mathbb{F}_{q^2}) - q^2 - 1) + a_1^2) \equiv 0 \pmod 2$.

The case with two points at infinity occurs only when $\deg(h(x)) = 3$. The equation is $\mathbb{F}_q$-isomorphic to one with a single point at infinity if and only if $h(x)$ has a root in $\mathbb{F}_q$. Thus, assume that $h(x)$ has no roots in the ground field. In this situation there can be zero or two $\mathbb{F}_q$-points at infinity and always two $\mathbb{F}_{q^2}$-points at infinity. Since the polynomial $h(x)$ has no root in $\mathbb{F}_q$ and has degree three it must in fact be irreducible over $\mathbb{F}_{q^2}$. Once again we easily see that $\#C(\mathbb{F}_q) \equiv 0 \pmod 2$ and so a_1 is odd. Now, we obtain two points of $C(\mathbb{F}_{q^2})$ for every element $x \in \mathbb{F}_q$ and we also obtain sets of 4 conjugate points for elements of $x \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. It follows that $\#C(\mathbb{F}_{q^2}) \equiv 2 \pmod 4$ and that a_2 is odd. □

We observe the following trivial but interesting corollary of the above result.

Corollary 6.2. *Let $q = 2^l$ and let C_1 and C_2 be hyperelliptic curves of genus 2 over $\mathbb{F}_q$. Suppose that C_1 has one point at infinity and that C_2 has two points at infinity and is not isomorphic over $\mathbb{F}_q$ to a hyperelliptic model with one point at infinity. Then $\mathrm{Jac}(C_1)$ is not isogenous to $\mathrm{Jac}(C_2)$ over $\mathbb{F}_q$.*

We note that these results are not true for genus three curves, for example $y^2 + (x^3 + 1)y = x^7 + x^5 + x^4$ and $y^2 + (x^4 + x + 1)y = x^7$ have isogenous Jacobians but the first has one point at infinity while the second is not isomorphic over $\mathbb{F}_2$ to a curve with one point at infinity.

Suppose that C is a genus two curve whose Jacobian is a factor of the Weil restriction of some elliptic curve with characteristic polynomial of Frobenius equal to $T^2 + aT + q^n$. We make the assumption that a is odd (i.e., that our process starts with an ordinary elliptic curve). There are at most 5 even values for a which can arise, and so this assumption only excludes a very small number of possible isogeny classes of dimension two abelian varieties.

Write $P(T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$ for the characteristic polynomial of Frobenius for $\mathrm{Jac}(C)$ over $\mathbb{F}_q$, define $m = n - 2$ and write

$$Q(T) = T^{2m} + \alpha_1 T^{2m-1} + \alpha_2 T^{2m-2} + \cdots + \alpha_m T^m + q\alpha_{m-1}T^{m-1} + \cdots + q^m.$$

Then we must have $P(T)Q(T) = T^{2n} + aT^n + q^n$.

Proposition 6.3. *Let $q = 2^l$ and let C be a genus 2 curve over $\mathbb{F}_q$ with characteristic polynomial $P(T)$ as above such that $P(T)Q(T) = T^{2n} + aT^n + q^n$ for some integer $n \geq 3$. If a is odd then a_2 is odd and α_m is odd.*

Proof. The $n = 3$ case is trivial so we assume $n \geq 4$. With notation as above we find that the coefficient of T^n in the product $P(T)Q(T)$ has the form

$$q^2\alpha_{m-2} + qa_1\alpha_{m-1} + a_2\alpha_m + a_1q\alpha_{m-1} + q^2\alpha_{m-2} = a$$

from which we immediately deduce that $a_2 \equiv \alpha_m \equiv 1 \pmod 2$. □

The fact that $P(T)Q(T) = T^{2n} + aT^n + q^n$ imposes various conditions on the α_i as follows:

$$\begin{array}{rcl} \alpha_1 &=& -a_1 \\ \alpha_2 &=& -a_1\alpha_1 - a_2 \\ \alpha_3 &=& -a_1\alpha_2 - a_2\alpha_1 - qa_1 \\ \alpha_4 &=& -a_1\alpha_3 - a_2\alpha_2 - qa_1\alpha_1 - q^2 \end{array} \tag{1}$$

and so on. For $i \geq 5$ (and thus $n \geq 7$) the recurrence is always of the form

$$\alpha_i = -a_1\alpha_{i-1} - a_2\alpha_{i-2} - qa_1\alpha_{i-3} - q^2\alpha_{i-4}. \tag{2}$$

By substituting the earlier values of α_i we obtain

$$\begin{array}{rcl} \alpha_1 &=& -a_1 \\ \alpha_2 &=& a_1^2 - a_2 \\ \alpha_3 &=& -a_1^3 + 2a_1a_2 - a_1q \\ \alpha_4 &=& a_1^4 + a_1^2(2q - 3a_2) + (a_2^2 - q^2) \end{array} \tag{3}$$

and so on.

Lemma 6.4. *Let $q = 2^l$. The α_i can be represented as polynomials in a_1, a_2 and q. These polynomials have the following properties:*

1. *α_{2i+1} is always divisible by a_1 for $i = 0, 1, \ldots$.*
2. *The only pure power of a_1 in α_i (i.e., monomial with no a_2 or q terms) is $\pm a_1^i$.*

3. *The following congruences on* $\alpha_i \pmod 2$ *hold.*

$i \pmod 6$	$\alpha_i \pmod 2$
1	a_1
2	$a_1 + a_2$
3	a_1
4	$a_1 + a_1 a_2 + a_2$
5	$a_1 + a_1 a_2$
6	$a_1 + a_1 a_2 + a_2$

Proof. The statements are easily proved by induction using the initial cases (3) and the recurrence formula (2). For the third part we use the fact that $x^n \equiv x \pmod 2$ to simplify the expressions. $\square$

Proposition 6.5. *Let* $q = 2^l$ *and suppose* C *is a hyperelliptic curve of genus two whose Jacobian is a simple factor of the Weil restriction of an elliptic curve* E *over* $\mathbb{F}_{q^n}$ *where* $n > 2$. *Then one of the following two cases holds*

1. *A curve in the isogeny class of* C *would have already arisen from the Weil descent of an elliptic curve over the quadratic extension* $\mathbb{F}_{q^2}$. *This case can arise when* n *is even.*

2. C *has two points at infinity. This case can arise when* $n \equiv 0, 2, 3 \pmod 6$.

Proof. Consider first the case $n \equiv 3 \pmod 6$ (i.e., $m \equiv 1 \pmod 6$). Proposition 6.3 implies that $a_2 \equiv \alpha_m \equiv 1 \pmod 2$ and part 3 of Lemma 6.4 implies that $a_1 \equiv \alpha_m \pmod 2$. Lemma 6.1 implies that such a curve has two points at infinity.

For the case $n = 4$ write $P(T)(T^4 + \alpha_1 T^3 + \alpha_2 T^2 + q\alpha_1 T + q^2) = T^8 + aT^4 + q^4$ so that $a_1 = -\alpha_1$, $\alpha_2 + a_2 = \alpha_1^2$, $\alpha_1(a_2 - \alpha_2) = 0$ and $\alpha_2 \equiv a_2 \equiv 1 \pmod 2$. The case $\alpha_1 = 0$ is the case where $P(T)$ already arises from an elliptic curve over $\mathbb{F}_{q^2}$. The case $\alpha_1 \neq 0$ implies $a_2 = \alpha_2$ and so $\alpha_1^2 = 2a_2$ which implies that α_1 and a_1 are even but this in turn implies that a_2 is even which is a contradiction.

The cases $n \geq 5$ will be handled using general arguments. The basic approach is to consider the coefficient of the term T^{n+1} in $P(T)Q(T)$, which must be zero. This term is congruent modulo 2 to $a_2\alpha_{m-1} + a_1\alpha_m$. For the case $n \equiv 5 \pmod 6$ (i.e., $m \equiv 3 \pmod 6$) we argue as follows: From Lemma 6.4 and the fact that $\alpha_m \equiv a_2 \equiv 1 \pmod 2$ we have $a_1 \equiv 1 \pmod 2$ and $\alpha_{m-1} \equiv 0 \pmod 2$. But then $a_2\alpha_{m-1} + a_1\alpha_m \equiv 1 \pmod 2$ which is a contradiction. Hence when $n \equiv 5 \pmod 6$ there can be no degree 4 factors of $T^{2n} + aT^n + q^n$.

When $m \equiv 5 \pmod 6$ (i.e., $n \geq 7$ and $n \equiv 1 \pmod 6$) then the facts $a_2 \equiv \alpha_m \equiv 1 \pmod 2$ are incompatible with $\alpha_m \equiv a_1 + a_1 a_2 \pmod 2$ and so again this case cannot arise.

When m is even ($m \geq 4$) we must consider the coefficient of T^{n+1} more closely. Using part 1 of Lemma 6.4 we see that this coefficient is $a_1(q^2\alpha_{m-3}/a_1 + q\alpha_{m-2} + a_2\alpha_{m-1}/a_1 + \alpha_m + q\alpha_{m-1}/a_1)$ from which we see that either $a_1 = 0$ (and the curve would have arisen from a Weil descent over a quadratic extension) or else the second factor is zero. Now consider this factor modulo 2. Recalling that

$a_2 \equiv \alpha_m \equiv 1 \pmod 2$ it turns out that $\alpha_{m-1}/a_1 \equiv 1 \pmod 2$ must be satisfied. In the case $m \equiv 0 \pmod 6$ it follows that $a_1 \equiv 1 \pmod 2$ and so there are two points at infinity. In the case $m \equiv 2 \pmod 6$ the condition $\alpha_m \equiv 1 \pmod 2$ implies $a_1 \equiv 0 \pmod 2$ but then $\alpha_{m-1}/a_1 \equiv 0 \pmod 2$ which is a contradiction. In the case $m \equiv 4 \pmod 6$ it follows that $a_1 \equiv 1 \pmod 2$ and so the curve has two points at infinity. □

The meaning of this result is that the only way to get something 'new' results in a curve with 2 points at infinity. Experimental evidence suggests that all the new isogeny classes already appear using $n \leq 6$ in the above construction.

7. Odd Characteristic

It would be very useful if one could perform constructive Weil descent in odd characteristic, such as to construct a genus 2 curve over a prime field $\mathbb{F}_p$ from the Weil descent of an elliptic curve over $\mathbb{F}_{p^2}$.

Unfortunately, it seems to be rather difficult to achieve this in practice. Suppose E is an elliptic curve over $\mathbb{F}_{p^n}$ and that C is a curve of genus g on the Weil restriction of E. If $g > n$ then one only knows that $P_E(T^n) | P_{\mathrm{Jac}(C)}(T)$ and this information alone is not enough to determine the number of points on $\mathrm{Jac}(C)(\mathbb{F}_p)$. Even the knowledge that there is a large prime factor is useless in practice if one does not know the cofactor, since it is not possible to force a random element to have prime order. Thus we are forced to seek curves of genus $g \leq n$. In odd characteristic this condition is not usually satisfied for curves on the Weil restriction.

One case where this is possible has been given by Claus Diem: given an elliptic curve over $\mathbb{F}_{3^m}$ there is an explicitly given genus two curve C over $\mathbb{F}_{3^m}$ such that $\#\mathrm{Jac}(C)(\mathbb{F}_{3^m}) = \#E(\mathbb{F}_{3^{3m}})/\#E(\mathbb{F}_{3^m})$. Details of this construction are given in Section 3.2 of [4].

Of course, in odd characteristic the results of this article still apply: only a small proportion of the isogeny classes of curves can be constructed using this method.

8. Acknowledgement

I would like to thank the referees for pointing out some errors in an earlier draft of the paper. I would also like to thank Jerzy Urbanowicz and the rest of the organising committee for all their hard work in putting the conference together.

References

[1] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, *Math. Comp.*, **48**, 95–101 (1987)

[2] I. Duursma, P. Gaudry and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, in Lam et al (ed.), ASIACRYPT '99, Springer LNCS 1716, 1999.

[3] G. Frey. *How to disguise an elliptic curve*, Talk at ECC '98, Waterloo, Canada (1998)
`http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`

[4] G. Frey, *Applications of Arithmetical Geometry to Cryptographic Constructions*, Preprint (2000)
`http://www.exp-math.uni-essen.de/preprints/index00.html`

[5] S. D. Galbraith, N. P. Smart, *A Cryptographic Application of Weil Descent*, in M. Walker (ed.), Codes and Cryptography, Cirencester, Springer LNCS 1746, p. 191-200 (1999)

[6] S. D. Galbraith, S. Paulus and N. P. Smart, *Arithmetic on superelliptic curves*, To appear in *Math. Comp.*, (2001)

[7] S. D. Galbraith, *Supersingular curves in cryptography*, Preprint (2000)

[8] P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, in W. Bosma (ed.), ANTS-IV, Springer LNCS 1838, 313–332 (2000)

[9] P. Gaudry, F. Hess, N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, To appear in *J. Crypt.*, (2001)

[10] P. Gaudry, *Algorithmique des courbes hyperellipticques et applications à la cryptologie*, L'École Polytechnique thesis (2000)
`http://ultralix.polytechnique.fr/~gaudry/`

[11] F. Hess, G. Seroussi, N. P. Smart, *Two topics in hyperelliptic cryptography*, Preprint (2000)

[12] N. Koblitz, *Hyperelliptic cryptosystems*, *J. Crypt.*, **1**, no. 3 (1989) 139–150.

[13] H.-G. Rück, *Abelian surfaces and Jacobian varieties over finite fields*, *Compositio Math.*, **76**, 351–366 (1990)

[14] A.-M. Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, PhD Thesis, IEM Essen (1994)

[15] J. Tate, *Endomorphisms of abelian varieties over finite fields*, *Inv. Math.*, **2** (1966) 134–144.

[16] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup., 4th series **2**, 521–560 (1969)

[17] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Preprint (2000)
`http://www.exp-math.uni-essen.de/preprints/index00.html`