Counting points on genus 2 curves over finite fields

Chloe Martindale

November 27, 2016

These notes are from a talk given in the Algebra Seminar at Universiteit Leiden, the Netherlands on 14/11/2016 and in the Number Theory Seminar at EPFL, Lausanne, Switzerland on 24/11/2016. The contents of the talk include research from the PhD thesis of the author, which was written under the supervision of Dr Marco Streng, and research from an article which was started at the AGC2016 workshop at UCLA, as joint work together with Sean Ballentine, Aurore Guillevic, Elisa Lorenzo-Garcia, Maike Massierer, Ben Smith, and Jaap Top.

1 Motivation: elliptic curves

As cryptographic systems based on curves become more mainstream, it is important to develop fast algorithms for counting points on curves defined over finite fields $\mathbb{F}_p$, where p is a very large prime. All of this research was inspired by previous research into elliptic curves, and so we first recall definitions and results for elliptic curves as a motivation for the genus 2 case.

Definition. Suppose that E and E' are elliptic curves over a field k. An *isogeny* $\phi : E \to E'$ is a surjective morphism with finite kernel that sends the identity to the identity.

Remark. Some people consider the constant-zero morphism to be an isogeny, which is not consistent with the above definition. As this morphism will not play a role in our work, we do not include the constant-zero morphism in our definition of isogeny.

Definition. Suppose that $\phi : E \to E'$ is an isogeny of elliptic curves over a field k. This induces an injective morphism of function fields

$$\overline{k}(E') \longrightarrow \overline{k}(E).$$

We define the *degree* of ϕ to be

$$\deg(\phi) = [\overline{k}(E) : \overline{k}(E')].$$

Question 1. *A natural question to ask at this point is: given an elliptic curve over a field k, can we enumerate all the elliptic curves E' over k such that there exists an isogeny $E \to E'$ of degree ℓ?*

There is more than one way of answering this question; we give the answer that will help us eventually with point counting. Also, in this talk, we only answer this question for $k = \mathbb{F}_p$, as we are ultimately interested in counting points on curves over $\mathbb{F}_p$. We first need to define a number associated to an elliptic curve over any field, the j-invariant.

Definition. For an elliptic curve E defined over k with $\mathrm{char}(k) \neq 2, 3$, let

$$y^2 = x^3 + Ax + B$$

be a Weierstrass form for E, with $A, B \in k$. Then if $4A^3 + 27B^2 \neq 0$, we define the *j-invariant* of E to be

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

This number determines E up to isomorphism (i.e. birational transformation of x and y).

Definition. For each $\ell \in \mathbb{Z}_{\geq 2}$, the *modular polynomial of level ℓ* is a non-constant-zero polynomial

$$\Phi_\ell \in \mathbb{F}_p[X, Y]$$

such that, given any 2 elliptic curves E and E' over $\overline{\mathbb{F}_p}$, there exists an isogeny $E \to E'$ of degree ℓ if and only if $\Phi_\ell(j(E), j(E')) = 0$.

Remark. If $\ell \in \mathbb{Z}_{\geq 2}$ is prime, then the degree of $\Phi_\ell(X, Y)$ in both X and Y is given by $\ell + 1$.

For small ℓ, equations for $\Phi_\ell(X, Y)$ can be found for example at LMFDB. These equations can also be thought of as models for the modular curve $X_0(\ell)$ of level ℓ.

We can now answer Question 1: given an elliptic curve $E/\mathbb{F}_p$, compute $j(E) \in \mathbb{F}_p$, and compute the $\mathbb{F}_p$-vauled polynomial in $\Phi_\ell(j(E), Y)$ in Y. The roots of this polynomials then give us the j-invariants of each curve $E'/\overline{\mathbb{F}_p}$ for which there exists an isogeny $E \to E'$ of degree ℓ.

Question 2. *Another natural question about elliptic curves over finite fields is, given $E/\mathbb{F}_p$, what is the most efficient way of counting $\#E(\mathbb{F}_p)$ for a large prime p?*

To answer this question, we first need to know the following 2 facts for an elliptic curve $E/\mathbb{F}_p$ with trace of Frobenius t:

1. $\#E(\mathbb{F}_p) = 1 + p - t$, and
2. $|t| < 2\sqrt{p}$.

Then the beautiful theorem of Schoof, Elkies, and Atkin gives us a polynomial time algorithm for computing t, and hence $\#E(\mathbb{F}_p)$.

Theorem (Schoof, Atkin, Elkies)**.** *Let E be a non-supersingular elliptic curve over $\mathbb{F}_p$ such that $j(E) \neq 0, 1728$, and write the modular polynomial of level ℓ*

$$\Phi_\ell(j(E), Y) = f_1(Y) \cdots f_n(Y)$$

as the product of irreducible polynomials in $\mathbb{F}_p[Y]$. Then (up to ordering) the polynomials f_i satisfy one of the following:

1. *$n = 2$, $deg(f_1) = 1$, and $deg(f_2) = \ell$.*
2. *$deg(f_1) = deg(f_2) = 1$, and for every $i > 2$, $deg(f_i) = r > 1$, for some $r \in \mathbb{Z}$.*
3. *for every i, $deg(f_i) = r$, for some $r \in \mathbb{Z}$.*

Furthermore, there exists a primitive r^{th} root of unity $\zeta \in \overline{\mathbb{F}_\ell}$ such that

$$t^2 \equiv (\zeta + \zeta^{-1})^2 p \ mod\ \ell,$$

where in case (1) we set $\zeta = 1$.

We unfortunately do not have time to prove this theorem, although the proof is beautiful and elementary. Schoof has written a report on this theorem, which is referenced as [Sch].

We can now answer Question 2 in the following way: given an elliptic curve E over $\mathbb{F}_p$, we first compute t^2 modulo ℓ for many different primes ℓ (perhaps up to a root of unity). We then use the bound on $|t|$ and the Chinese Remainder Theorem to compute t^2. Lastly, we check the sign of t, for example by multiplying a non-trivial point $P \in E(\mathbb{F}_p)$ by both $1+p-t$ and $1+p+t$. For large p, this is much more efficient than any other known algorithm for counting points. Which leads us to the topic of this talk: is there a way of generalising this algorithm to higher genus curves or abelian varieties to do fast point-counting there?

2 Counting points on genus 2 curves

First, to give some intuition for those who are unfamiliar with genus 2 curves, one should have in mind that any genus 2 curve C over a field k such that $\mathrm{char}(k) \neq 2$ has a hyperelliptic model

$$C : y^2 = f(x),$$

where $f(x) \in k[x]$ has degree 5 or 6, and also that there is an abelian variety of dimension 2 associated to C, called the Jacobian of C, written as $\mathcal{J}(C)$, such that $C(k) \subseteq \mathcal{J}(C)(k)$. These properties make genus 2 curves into a natural stepping stone for generalising theory that has been developed for elliptic curves. To generalise what we have seen in this talk so far, we must answer 3 questions.

Question 3. *(a) How do we associate an isomorphism invariant to a genus 2 curve?*

(b) How do we define a modular polynomial, and can we compute it?

(c) How will these modular polynomials factor, and does the method of Schoof, Elkies, and Atkin generalise in a natural way?

2.1 Isomorphism invariants of genus 2 curves

We first (attempt to) answer Question 3(a). Perhaps the most well-known isomorphism invariant for genus 2 curves is the Igusa invariant, which can again be written in terms of the coefficients of the defining equation of the curve. That is, given a genus 2 curve C over a field k with $\mathrm{char}(k) \neq 2$, with hyperelliptic model

$$C : y^2 = f(x),$$

one can define rational functions

$$(i_1, i_2, i_3) : k[x] \longrightarrow \mathbb{A}^3_k$$

such that the tuple $(i_1(f), i_2(f), i_3(f))$ determines the curve C up to isomorphism. There is also an algorithm of Mestre which allows us to compute an equation for the curve C corresponding to a given tuple of Igusa invariants. Unfortunately, the Igusa invariants are too general for our purposes, and we need to use invariants which 'see' some extra structure on the curve.

Recall that for any abelian variety A over a finite field $\mathbb{F}_p$, as well as the endomorphisms on A corresponding to multiplication by some integer, there exists the p-power Frobenius endomorphism

$$\begin{array}{rccc} \pi : & A & \longrightarrow & A \\ & x & \mapsto & x^p. \end{array}$$

In particular, the endomorphism ring of A satisfies

$$\mathbb{Z} \subsetneq \mathrm{End}(A).$$

In this case, we say that A has *complex multiplication*. We recall now the definition of a CM-field (CM = Complex Multiplication).

Definition. A *CM-field* K is a totally imaginary degree 2 extension of a totally real number field.

In fact, for a simple, ordinary abelian variety A over $\mathbb{F}_q$, we have much more than just $\mathbb{Z} \subsetneq \mathrm{End}(A)$, we know that there exists a CM-field of dimension $2\dim(A)$ over $\mathbb{Q}$ for which $\mathrm{End}(A) \otimes \mathbb{Q} = K$; for completeness we include here the necessary references for this fact.

Lemma. *Suppose that A is a simple abelian variety over $\mathbb{F}_q$. Then the following are equivalent:*

(a) A is ordinary,

(b) $K = \mathrm{End}(A) \otimes \mathbb{Q}$ is a CM-field of degree $2dim(A)$ over $\mathbb{Q}$,

(c) the characteristic polynomial of the q-power Frobenius endormorphism on A is irreducible.

Proof. From Notation 9.1 in Oort's article [Oor], we get (c) $\Leftrightarrow$ (b). By Dipippo and Howe, [DH], we have that A is ordinary if and only if p does not divide the middle coefficient of the minimal polynomial of the characteristic polynomial of the Frobenius. If (b) does not hold, then from Proposition 2.2 in [Oor] we have that the characteristic polynomial of Frobenius is given by

$$(x - q^{1/2})^2(x + q^{1/2})^2 = (x^2 - q)^2 = x^4 - 2qx^2 + q^2,$$

and hence by Dipippo and Howe, (a) does not hold if and only if (b) does not hold. □

Definition. Suppose that A is an abelian variety such that $\mathrm{End}(A) \otimes \mathbb{Q} = K$ is a CM-field, and denote by K_0 the maximal totally real subfield of K. We then say that *A has CM by K*, and *A has RM by K_0*. Here CM stands for complex multiplication, and RM stands for real multiplication.

So to specialise our invariants, we can fix a totally real quadratic number field K_0, and restrict to isomorphism invariants for simple, ordinary abelian varieties of dimension 2 defined over $\mathbb{F}_p$ with real multiplication by K_0. That is, given a genus 2 curve C over $\mathbb{F}_p$ with $p \neq 2$ such that $\mathcal{J}(C)$ has real multiplication by K_0, for $C : y_2 = f(x)$, we want to define rational functions

$$j_1, j_2, j_3 : \mathbb{F}_p[x]|_{\deg=5,6} \longrightarrow \mathbb{A}^3_{\mathbb{F}_p}$$

such that the tuple

$$(j_1(f), j_2(f), j_3(f))$$

determines $\mathcal{J}(C)$ up to (real-multiplication preserving) isomorphism. The only fields K_0 for which these functions are explicitly written down are $K_0 = \mathbb{Q}(\sqrt{5})$ and $K_0 = \mathbb{Q}(\sqrt{8})$, in work by Müller. The equations for j_1 and j_2 are known for all real quadratic fields, thanks to work by Lauter and Yang, but the problem of finding a general equation for j_3 is still open. The existence of such functions is proven in the thesis of the author (and perhaps has been done elsewhere, unknown to her).

2.2 Modular polynomials for genus 2 curves over finite fields

Having answered Question 3(a) as far as possible with the current techniques, we turn to Question 3(b): defining and computing modular polynomials in genus

2. We will use the isomorphism invariants of the previous section, and so we fix the prime p, the real quadratic number field K_0, and an isomorphism invariant (j_1, j_2, j_3) for K_0 throughout. In the elliptic curve case, the modular polynomial of level ℓ told us about isogenies of degree ℓ, otherwise known as ℓ-isogenies. We now want to look at isogenies for genus 2 curves, which we do by studying isogenies of their Jacobians. The following definition is the same as the one for elliptic curves:

Definition. A morphism of abelian varieties is an *isogeny* if it preserves the identity, is surjective, and has finite kernel.

The generalisation of an ℓ-isogeny to genus 2 that we use is quite complicated, so we do not give the details here. The interested reader can find the definition in the upcoming thesis of the author. We again associate a prime to the isogeny, but now a prime ideal in $\mathcal{O}_{K_0}$ - we study 'μ-isogenies', where μ is a totally positive element of $\mathcal{O}_{K_0}$ which generates a prime ideal in K_0. The generalisation of the modular polynomial is given by the following theorem, which is proven in the upcoming thesis of the author.

Theorem. *There exists an algorithm to compute polynomials*

$$\begin{array}{rcl} G_\mu(X_1, X_2, X_3, Z_1) & \in & \mathbb{F}_p[X_1, X_2, X_3, Z_1] \\ H_{\mu,2}(X_1, X_2, X_3, Z_1, Z_2) & \in & \mathbb{F}_p[X_1, X_2, X_3, Z_1, Z_2] \\ H_{\mu,3}(X_1, X_2, X_3, Z_1, Z_3) & \in & \mathbb{F}_p[X_1, X_2, X_3, Z_1, Z_3] \end{array}$$

with

$$\deg_{Z_1}(G_\mu) = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1, \quad \deg_{Z_2}(H_{\mu,2}) = 1, \quad \deg_{Z_3}(H_{\mu,3}) = 1,$$

such that for 'most' genus 2 curves $C/\overline{\mathbb{F}_p}$ with $C : y^2 = f(x)$, and $C'/\overline{\mathbb{F}_p}$ with $y^2 = f(x)'$, there exists a μ-isogeny $\mathcal{J}(C) \to \mathcal{J}(C')$ if and only if

$$\begin{array}{c} G_\mu(j_1(f), j_2(f), j_3(f), j_1(f')) = 0 \\ H_{\mu,2}(j_1(f), j_2(f), j_3(f), j_1(f'), j_2(f')) = 0 \\ H_{\mu,3}(J_1(f), j_2(f), j_3(f), j_1(f'), j_3(f')) = 0. \end{array}$$

For the precise definition of 'most', see the upcoming thesis of the author. The algorithm has been implemented in the cases for which j_1, j_2 and j_3 are known, and the polynomials are computed up to $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = 19$. As more polynomials are computed, they can be found at `http://pub.math.leidenuniv.nl/~martindalecr`.
This theorem tells us that given a genus 2 curve $C/\mathbb{F}_p$, we can enumerate all the (invariants of) genus 2 curves $C'/\overline{\mathbb{F}_p}$ for which there exists a μ-isogeny to $\mathcal{J}(C) \to \mathcal{J}(C')$ in the same way as we did for elliptic curves. That is, given $C/\mathbb{F}_p$, given by $C : y^2 = f(x)$, we can

1. Compute $j_1(f), j_2(f), j_3(f)$.
2. Enumerate the solutions of $G_\mu(j_1(f), j_2(f), j_3(f), Z_1) = 0$, which gives us $j_1(f')$ for every $C' : y^2 = f(x)'$ for which $\mathcal{J}(C')$ is μ-isogenous to $\mathcal{J}(C)$.

3. For each C', find the unique $j_2(f')$ and $j_3(f')$ that satisfy

$$H_{\mu,2}(j_1(f), j_2(f), j_3(f), j_1(f'), j_2(f')) = 0$$

and

$$H_{\mu,3}(J_1(f), j_2(f), j_3(f), j_1(f'), j_3(f')) = 0.$$

If one requires the equation of the curve, in the thesis of the author there are formulae to find the Igusa invariants in terms of j_1, j_2 and j_3, and we can then use Mestre's algorithm to find the curve. We now answer the remaining part of Question 3, part (c).

2.3 Schoof's algorithm in genus 2

This section is joint work with Ballentine, Guillevic, Lorenzo-Garcia, Massierer, Smith, and Top. As before, we fix p, K_0, j_1, j_2, and j_3. We again need to recall how the number of $\mathbb{F}_p$-points on a genus 2 curves relates to the Frobenius polynomial:
Let C be a genus 2 curve over $\mathbb{F}_p$; then there exist integers s and t such that the characteristic polynomial of the p-power Frobenius on $\mathcal{J}(C)$ is given by

$$X^4 - tX^3 + (2p + s)X^2 - tpX + p^2.$$

Then in particular, we have the following facts:

1. $\#C(\mathbb{F}_p) = 1 + p - t$,
2. $\#\mathcal{J}(C)(\mathbb{F}_p) = 1 - t + 2p + s - tp + p^2$,
3. $|s| < 4p$, and
4. $|t| < 4\sqrt{p}$.

Given these facts, we hope for a Schoof-style algorithm to compute s and t, and the following theorem gives us just that.

Theorem. *Let $C/\mathbb{F}_p$ be a genus 2 curve, $C : y^2 = f(x)$, such that $\mathcal{J}(C)$ is simple and ordinary, $(\mathrm{End}(\mathcal{J}(C)) \otimes \mathbb{Q}) \cap \mathbb{R} = K_0$, and $\mathrm{Aut}(\mathcal{J}(C)) = \{\pm 1\}$. Then for a totally positive element $\mu \in \mathcal{O}_{K_0}$ such that $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$ is prime, the factorisation of*

$$G_\mu(j_1(f), j_2(f), j_3(f), Z_1) = f_1 \cdots f_n$$

into irreducible polynomials in $\mathbb{F}_p[Z_1]$ satisfies one of

1. $\deg(f_1) = 1$, *and for* $i > 1$, $\deg(f_i) = r$,
2. $\deg(f_1) = \deg(f_2) = 1$, *and for* $i > 2$, $\deg(f_i) = r$, *or*
3. *for every* i, $\deg(f_i) = r$.

Furthermore, there exist primitive $2r^{th}$-roots of unity ζ_{2r} and ζ'_{2r} in $\overline{\mathbb{F}_\ell}$ such that for $\eta_{2r} = \zeta_{2r} + \zeta_{2r}^{-1}$ and $\eta'_{2r} = \zeta'_{2r} + \zeta_{2r}^{'-1}$, we have

$$t_2 \equiv (\eta_{2r} + \eta'_{2r})^2 p \bmod \ell,$$

and

$$s \equiv \pm \eta_{2r} \eta'_{2r} p \bmod \ell.$$

Here we define a 'primitive ℓ^{th} root of unity' to be 1.

Hence, our point counting algorithm now becomes, given a curve $C/\mathbb{F}_p$ with real multiplication by K_0 such that $\mathrm{Aut}(\mathcal{J}(C)) = \{\pm 1\}$, with $C : y^2 = f(x)$,

1. Compute $j_1(f), j_2(f), j_3(f)$.
2. Compute t^2 and s mod ℓ for many small ℓ using the theorem above.
3. Find t^2 and s using the Chinese Remainder Theorem, and the bounds on s and t.
4. Check the sign of t with your favourite method (eg. multiplying a random $\mathbb{F}_p$ point in $\mathcal{J}(C)$ by the 2 options for $\#\mathcal{J}(\mathbb{F}_p)$).

References

[DH] Dipippo, Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory 73 (1998), 426450; Corrig., J. Number Theory 83 (2000), 182.

[Oor] Oort, *Abelian Varieties over Finite Fields*, `http://www.math.nyu.edu/~tschinke/books/finite-fields/final/05_oort.pdf` (2007).

[Sch] Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux 7 (1995), 219-254.