CONSTRUCTING ELLIPTIC CURVES AND CURVES OF GENUS 2 OVER FINITE FIELDS

KIRSTEN EISENTRÄGER

1. Introduction

In cryptography, the security of discrete-log-based systems depends on the the largest prime factor of the group order. Groups of points on elliptic curves and Jacobians of hyperelliptic curves of low genus can be used in these systems. Hence it is desirable to be able to construct curves over finite fields such that the resulting group order is prime. The problem of constructing elliptic curves with a given number of points has been studied extensively. The standard approach is to compute the Hilbert class polynomial for a quadratic imaginary number field. The running time of the best known algorithms is $\tilde{O}(|D|)$, where D is the discriminant of the quadratic imaginary field. In this paper we present the Chinese Remainder Theorem (CRT) algorithm by Agashe-Lauter-Venkatesan [ALV04] for constructing elliptic curves with a prescribed number of points and describe the improvements to it given in [BBEL08].

The constructions for elliptic curves can be generalized to curves of genus 2. Almost all approaches for constructing genus 2 curves rely on computing the Igusa class polynomials of quartic CM fields. In this paper we present the CRT algorithm for generating genus 2 curves defined over finite fields with a prescribed number of points on their Jacobian given in [EL10]. The algorithm in [EL10] first determines the Igusa class polynomials modulo p for certain small primes p. Then the Igusa class polynomials are computed using the Chinese Remainder Theorem and a bound on the denominators of the coefficients. We will also describe some improvements to this algorithm that were given in [BGL11] and [LR13]. As for elliptic curves, the CRT method for genus 2 curves is one of several known methods for constructing curves and we will briefly describe some of the other approaches as well.

2. Generating elliptic curves with a prescribed number of points

In this section we give an algorithm for the following problem (under certain conditions): Given a prime number ℓ and a positive integer N, construct an elliptic curve E_0 defined over $\mathbb{F}_\ell$ such that $\#E_0(\mathbb{F}_\ell) = N$.

2.1. Properties of elliptic curves over finite fields.

Let ℓ be a prime and let E be an elliptic curve defined over the finite field $\mathbb{F}_\ell$ with ℓ elements. Denote by $\mathrm{End}(E)$ its ring of endomorphisms that are defined over $\overline{\mathbb{F}}_\ell$.

For any such curve E, the number of points on the curve that are defined over $\mathbb{F}_\ell$ lie in the Hasse-Weil interval:

$$\#E(\mathbb{F}_\ell) \in [\ell + 1 - 2\sqrt{\ell}, \ell + 1 + 2\sqrt{\ell}].$$

The author was partially supported by National Science Foundation grant DMS-1056703.

The curve E has a special endomorphism π, called the *Frobenius endomorphism*, which is given by $\pi : (x, y) \mapsto (x^\ell, y^\ell)$. Its characteristic polynomial is $P(X) = X^2 - tX + \ell$; t is referred to as the trace of Frobenius. It is customary to associate the Frobenius endomorphism with a root of its characteristic polynomial. So since π satisfies the above quadratic equation, we identify it with an element of $\mathbb{Q}(\sqrt{D})$ where $D = t^2 - 4\ell$. When the trace of π is nonzero modulo ℓ, we call E ordinary and in this case $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\sqrt{D})$ and $D < 0$. The number of points on E over $\mathbb{F}_\ell$ is determined by the trace of Frobenius, $\#E(\mathbb{F}_\ell) = \ell + 1 - t$.

Possible Group Orders. Let E be an elliptic curve E defined over $\mathbb{F}_\ell$ whose endomorphism ring is an order in a quadratic imaginary number field $K = \mathbb{Q}(\sqrt{D})$, with K not equal to $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$. Then there are only two possibilities for $\#E(\mathbb{F}_\ell)$, which can be seen as follows: as before, let $P(x) = X^2 - tX + \ell$ be the characteristic polynomial of the Frobenius endomorphism of E. Let $\pi, \overline{\pi}$ be the zeros of $P(x)$. Then $\pi\overline{\pi} = \ell$, so π and $\overline{\pi}$ have norm ℓ, and (π) and $(\overline{\pi})$ are the only ideals of $\mathcal{O}_K$ of norm ℓ. Hence the only elements of norm ℓ in $\mathcal{O}_K$ are $\pi, \overline{\pi}, -\pi, -\overline{\pi}$. The characteristic polynomial of a curve E' whose Frobenius endomorphism corresponds to $-\pi$ or $-\overline{\pi}$ is then $X^2 + tX + \ell$, and for such a curve E' we have $\#E'(\mathbb{F}_\ell) = \ell + 1 + t$. So the only possible group orders for a curve whose endomorphism ring is an order in K are $\ell + 1 - t$ or $\ell + 1 + t$. The curves E and E' are quadratic twists of each other.

2.2. **Complex Multiplication (CM) Method.** Now we can give an outline of an algorithm for our problem:

Problem 2.1. Given a prime $\ell > 3$ and a positive integer N with

$$N \in [\ell + 1 - 2\sqrt{\ell}, \ell + 1 + 2\sqrt{\ell}],$$

construct an elliptic curve $E_0/\mathbb{F}_\ell$ with $\#E_0(\mathbb{F}_\ell) = N$.

Here is a sketch of the standard algorithm for finding such a curve E_0, which is called the Complex Multiplication (CM) method:

Algorithm 2.2. CM method (see [AM93])
Input: N, ℓ as above.

(1) Let π be the Frobenius endomorphism of the desired curve E_0, $t = \ell + 1 - N$ its trace, and $D = t^2 - 4\ell$. Assume $t \not\equiv 0$ modulo ℓ. Let $K := \mathbb{Q}(\sqrt{D})$.
(2) Compute the *Hilbert class polynomial* $H_D(X)$ of K.
(3) Let j_0 be a root of H_D modulo ℓ. Take the curve $E_0/\mathbb{F}_\ell$ with *j-invariant* $j(E_0) = j_0$.
(4) Compute $\#E_0(\mathbb{F}_\ell)$. If $\#E_0(\mathbb{F}_\ell) \neq N$, then a quadratic twist of E_0 has N points over $\mathbb{F}_\ell$ and is the desired curve.

Remark 2.3. In step (3) of the above algorithm we reconstruct an elliptic curve E_0 from its j-invariant j_0. The j-invariant of an elliptic curve of the form $E : y^2 = x^3 + Ax + b$ is $j(E) = \frac{256 \cdot 27 \cdot A^3}{4A^3 + 27B^2}$. Two elliptic curves E, E' defined over a field F have the same j-invariant if and only if they are isomorphic over the algebraic closure of F. Assuming $j_0 \neq 0, 1728$ and $\ell \neq 2, 3$, an elliptic curve over $\mathbb{F}_\ell$ with j-invariant j_0 is given by the Weierstrass equation $E_0 : y^2 = x^3 + 3kx + 2k$, where $k = \frac{j_0}{1728 - j_0}$.

The endomorphism ring of E_0 is an order in K. By the discussion in the previous section that means that E_0 has either $\ell + 1 - t$ or $\ell + 1 + t$ points, so either E_0 or a twist of E_0 is the desired curve.

The above algorithm shows that constructing elliptic curves with a prescribed number of points reduces to computing the Hilbert class polynomial of the imaginary quadratic number field $\mathbb{Q}(\sqrt{D})$. We will now define the Hilbert class polynomial and give an algorithm for computing it.

2.3. **Complex multiplication and Hilbert class polynomials.** Let K be a field of characteristic zero, E an elliptic curve over K, and denote by $\mathrm{End}(E)$ its ring of endomorphisms defined over $\overline{K}$. We need the notion of complex multiplication to define the Hilbert class polynomial $H_D(X)$ of K.

For most elliptic curves in characteristic zero we have $\mathrm{End}(E) = \mathbb{Z}$, and the only endomorphisms are the "multiplication-by-m" maps. The CM case is the case where $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$.

Definition 2.4. The elliptic curve E has *complex multiplication (CM) by* $\mathcal{O}$ if $\mathrm{End}(E)$ is an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{D})$ with $D < 0$.

Example 2.5. The elliptic curve $E : y^2 = x^3 - x$ defined over $\mathbb{C}$ has endomorphism ring $\mathrm{End}(E)$ which is strictly larger than $\mathbb{Z}$ since it contains the map

$$\phi : (x, y) \mapsto (-x, iy).$$

It is easy to check that $\phi \circ \phi$ is $[-1] : P \mapsto -P$. So E has CM by $\mathbb{Z}[i]$.

Now we are ready to define the Hilbert class polynomial.

Definition 2.6. Let $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$, and let $\mathcal{O}_K$ be its ring of integers. The Hilbert class polynomial $H_D(X)$ of K is the polynomial whose roots are exactly the j-invariants of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$.

$$H_D(X) = \prod_{j(E) \in \mathrm{Ell}(D)} (X - j(E)).$$

Here $\mathrm{Ell}(D) = \{j(E) : \mathrm{End}(E) \cong \mathcal{O}_K\}$ is the finite set of j-invariants of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$.

From the theory of complex multiplication we have the following theorem:

Theorem 2.7. *[Sil94, Theorem II.6.1] The polynomial $H_D(X)$ has integer coefficients.*

The approach for finding the desired curve E_0 will be to compute H_D and then reduce H_D modulo ℓ to find curves over $\mathbb{F}_\ell$ whose endomorphism ring is $\mathcal{O}_K$.

2.4. **Algorithms for computing Hilbert class polynomials.** We have seen that to construct elliptic curves with a given number of points, it is enough to compute the Hilbert class polynomial H_D. This problem has been studied extensively, and there are several methods known for computing Hilbert class polynomials: the complex analytic method by Atkin and Morain [AM93] computes $H_D(X)$ by listing all binary quadratic forms corresponding to elliptic curves with CM by $\mathcal{O}_K$. It then evaluates the j-functions as a floating-point integer with sufficient precision, takes the product, and rounds the coefficients to the nearest integer. The p-adic approach (see Couveignes-Henocq [CH02], and Bröker [Brö08]) uses p-adic lifting to approximate the roots and recognize the coefficients of the polynomial. The Chinese Remainder Theorem method by Agashe-Lauter-Venkatesan [ALV04] and the modified CRT

method by Belding-Bröker-Enge-Lauter [BBEL08] compute $H_D(X)$ modulo p for sufficiently many small primes p and then use the Chinese Remainder Theorem to compute the integer coefficients of the polynomial $H_D(X)$. The running time for all of the algorithms is exponential in $\log(|D|)$, and the complexity analysis and comparison in [BBEL08, Section 5.4] show that the fastest version of the CRT algorithm has expected run time $\tilde{O}(|D|)$, and that the run time of the complex analytic algorithm and the p-adic method is also $\tilde{O}(|D|)$.

We now give an overview of the CRT method described in [ALV04] and the improvements made in [BBEL08]. For simplicity of notation we only deal with the case where D is the discriminant of the maximal order in $\mathbb{Q}(\sqrt{D})$.

Algorithm 2.8. CRT algorithm for computing $H_D(X)$[ALV04, Section 3.1]

Input: $D < 0$, discriminant of the maximal order in the quadratic imaginary number field $\mathbb{Q}(\sqrt{D})$.

(1) Compute an upper bound B on the coefficients of $H_D(X)$.
(2) Compute $H_D(X)$ modulo small primes $p_1, \ldots, p_n$ which split completely in the Hilbert class field of K and such that $\prod_i p_i > B$.
(3) Use the Chinese Remainder Theorem to find the coefficients of $H_D(X)$.

The point of the algorithm is that we can compute $H_D(X) \bmod p$ for suitably chosen small primes p directly without knowing $H_D(X)$. To compute $H_D(X) \bmod p$ we use the following proposition.

Proposition 2.9. *[ALV04, Proposition 4.1] Let $D < 0$ be the discriminant of the maximal order $\mathcal{O}_K$ of $K := \mathbb{Q}(\sqrt{D})$. Let p be a rational prime such that $4p = t^2 - Du^2$ for some integers u and t. Let $\mathrm{Ell}'(D)$ be the set of $\overline{\mathbb{F}}_p$ isomorphism classes of elliptic curves over $\mathbb{F}_p$ with End$(E) = \mathcal{O}_K$. Then*

$$H_D(X) \pmod p = \prod_{[E'] \in \mathrm{Ell}'(D)} (X - j(E')).$$

In particular, $H_D(X) \bmod p$ splits completely into linear factors.

When D is the discriminant of the maximal order and p is a prime of the form $4p = t^2 - D$ we can compute $\mathrm{Ell}'(D)$ as follows:

Proposition 2.10. *[ALV04, Proposition 4.2] Suppose p is a prime and $t \neq 0$ is an integer such that $4p = t^2 - D$. Let E' be an elliptic curve over $\mathbb{F}_p$. Then $[E'] \in \mathrm{Ell}'(D)$ if and only if $\#E'(\mathbb{F}_p)$ is either $p + 1 - t$ or $p + 1 + t$.*

This leads us to the following algorithm for computing all factors of $H_D(X) \bmod p$:

Algorithm 2.11.
(1) For each $j \in \mathbb{F}_p$, create an elliptic curve E' over $\mathbb{F}_p$ with $j(E') = j$.
(2) If $\#E'(\mathbb{F}_p)$ is either $p + 1 - t$ or $p + 1 + t$, then $H_D(X) \pmod p$ has a factor of $(X - j(E'))$.

Remark 2.12. The first step in the above algorithm, creating an elliptic curve with a given j-invariant, is easy, as described in Remark 2.3. For the second step we can use the well known point counting algorithm by Schoof.

2.5. **Improvements.** The algorithm in [ALV04] for computing H_D mod p required an exhaustive search through all possible j-invariants to find all curves E with $\mathrm{End}(E) = \mathcal{O}_K$. The improvement by Belding-Bröker-Enge-Lauter [BBEL08] finds one curve $E/\mathbb{F}_p$ with $\mathrm{End}(E) = \mathcal{O}_K$ and then obtains the others via the action of the class group $\mathrm{Cl}(\mathcal{O}_K)$ on the set $\mathrm{Ell}'(D)$.

To compute the action of the class group, they compute ℓ_i-isogenous curves, where the ℓ_i are the norms of ideals whose classes generate the class group $\mathrm{Cl}(\mathcal{O}_K)$. One way this can be done is by computing the modular polynomials $\Phi_{\ell_i}(X, Y)$, and using the fact that if $j_0 \in \mathbb{F}_p$ is the j-invariant of some curve E with endomorphism ring $\mathcal{O}$, then the roots in $\mathbb{F}_p$ of $\Phi_{\ell_i}(X, j_0)$ correspond to curves, ℓ_i-isogenous to E, with endomorphism ring $\mathcal{O}$ (see [BBEL08, Section 3.1]). Under GRH, the algorithm in [BBEL08] has expected runtime $O(|D|(\log|D|)^{7+o(1)})$.

3. Generating genus 2 curves with a prescribed number of points

We now generalize the elliptic curve construction to generate genus 2 curves with a given number of points. The points on a curve of genus 2 do not form a group, so we use as group elements the points on the *Jacobian* of the curve.

3.1. **Background and definitions.** Let $p > 2$ be a prime, and let C be a curve of genus 2 defined over the finite field $\mathbb{F}_p$ with p elements. A genus 2 curve is hyperelliptic, so C has a model of the form $y^2 = f(x)$ with $f(x) \in \mathbb{F}_p[x]$ a polynomial of degree 5 or 6 without repeated roots (in $\overline{\mathbb{F}}_p$). By a point on C we mean a pair (x, y) with coefficients in $\overline{\mathbb{F}}_p$ that satisfies $y^2 = f(x)$, or a "point at infinity". (If f has degree 5, there is one point at infinity, if f has degree 6 there are two points at infinity.) A *divisor* D of C is a finite formal sum of the form $D = \sum m_i P_i$, where the m_i are integers and the P_i are points of C; the degree of D is $\sum m_i$. Let h be a rational function on C. We associate with h its divisor $(h) = \sum m_i P_i$, where the P_i are the zeros and poles of h (in $\overline{\mathbb{F}}_p$) with multiplicities m_i. A divisor of such a nonzero function (h) is called principal, and it is well known that a principal divisor has degree 0. The divisors of degree 0 form a group $D_0(C)$, and the principal divisors form a subgroup $\mathrm{Princ}(C)$ of $D_0(C)$. The *Jacobian* of C is the quotient group

$$\mathrm{Jac}(C) = D_0(C)/\,\mathrm{Princ}(C).$$

Example 3.1. Let $f(x)$ be a monic polynomial of degree 5 over a field K of cardinality at least 5. Let $\lambda_0, \lambda_1, \lambda_2$ be distinct elements of K, not equal to 0 or 1. Then

$$C : y^2 = x(x-1)(x-\lambda_0)(x-\lambda_1)(x-\lambda_2)$$

is a curve of genus 2 that has one point at infinity ∞.

It follows from the Riemann-Roch theorem that elements of the Jacobian of a genus 2 curve C can be represented by divisors of the form

$$D = \sum_{i=1}^{r} P_i - r \cdot \infty \text{ with } P_i \in C \text{ and } r \leq 2.$$

Let C be a curve of genus 2 over $\mathbb{F}_p$. Let $P(X)$ denote the characteristic polynomial of the Frobenius endomorphism π on $\mathrm{Jac}(C)$. The polynomial $P(X)$ is monic of degree 4 and has integer coefficients. Its roots $a_1, \ldots, a_4$ have absolute value $p^{1/2}$.

Again, the characteristic polynomial $P(X)$ determines the number of points on C. It also determines the number of points on its Jacobian $\mathrm{Jac}(C)$. For any $m \geq 1$, we have $\#C(\mathbb{F}_{p^m}) = 1 - \sum_{i=1}^{4} a_i^m + p^m$, $\#\,\mathrm{Jac}(C)(\mathbb{F}_{p^m}) = \prod_{i=1}^{4}(1 - a_i^m)$, and

$$\#\,\mathrm{Jac}(C)(\mathbb{F}_p) = \frac{1}{2}\#C(\mathbb{F}_{p^2}) + \frac{1}{2}\#C(\mathbb{F}_p)^2 - p.$$

3.2. **Complex multiplication of genus 2 curves and quartic CM fields.** As in the elliptic curve case, we will work with curves whose Jacobians have endomorphism rings that are orders in CM fields. For elliptic curves the associated CM fields were quadratic imaginary fields. For genus 2 curves the associated fields have degree 4 over $\mathbb{Q}$.

Definition 3.2. A curve C of genus 2 has CM if the endomorphism ring of its Jacobian $\mathrm{End}(\mathrm{Jac}(C))$ is an order in a quartic CM field K, i.e. if $K = K_0(\sqrt{d})$ with K_0 real quadratic and $d \in K_0$ totally negative. Here $d \in K_0$ is totally negative if for both embeddings σ_1, σ_2 of K_0 into $\mathbb{R}$, we have $\sigma_i(d) < 0$ $(i = 1, 2)$.

3.3. **Outline of algorithm.** Our algorithm solves the following problem under certain conditions.

Problem: Given (ℓ, N_1, N_2) with ℓ prime, and N_1, N_2 positive integers, find a genus 2 curve C over the prime field $\mathbb{F}_\ell$ such that $\#C(\mathbb{F}_\ell) = N_1$ and $\#C(\mathbb{F}_{\ell^2}) = N_2$.

Approach: Given a triple $(\ell,\ N_1,\ N_2)$ we generate a curve as follows.

As in the case of the elliptic curves, the first step is to find the quartic CM field K such that $\mathrm{End}(\mathrm{Jac}(C)) \subseteq K$. To do this we find quartic polynomial satisfied by Frobenius. We write

$$N_1 = \ell + 1 - s_1, \quad N_2 = \ell^2 + 1 + 2s_2 - s_1^2.$$

and solve for s_1, s_2. The quartic CM field K is then generated over $\mathbb{Q}$ by a root of $X^4 - s_1X^3 + s_2X^2 - \ell s_1 X + \ell^2$.

Restrictions: We assume that $\gcd(s_2, \ell) = 1$, which forces the Jacobian of C to be ordinary. We also restrict to *primitive* quartic CM fields. A quartic CM field is not primitive iff it is Galois over $\mathbb{Q}$ and biquadratic. We further assume that K does not contain a cyclotomic field.

This leads to the following approach for constructing genus 2 curves:

Algorithm 3.3. Constructing genus 2 curves (see [EL10, Section 3])
Given (ℓ, N_1, N_2) with restrictions as above:

(1) Compute the quartic CM field K.
(2) Compute the Igusa class polynomials H_1, H_2, H_3 of K.
(3) From a triple of roots modulo ℓ of H_1, H_2, H_3, construct a genus 2 curve over $\mathbb{F}_\ell$ using the algorithms of Mestre [Mes91] and Cardona-Quer [CQ05].
(4) Test whether the curve generated has the correct number of points on the Jacobian. A curve C with $\#C(\mathbb{F}_\ell) = N_1$ and $\#C(\mathbb{F}_{\ell^2}) = N_2$ will have $\#J(C)(\mathbb{F}_\ell) = N = (N_1^2 + N_2)/2 - \ell$. If the curve does not have the required number of points on the Jacobian, a twist of the curve may be used. In the case where 4 group orders are possible for the pair (ℓ, K), a different triple of invariants may be tried until the desired group order is obtained.

Remark 3.4. Let C be a curve of genus 2 defined over $\mathbb{F}_\ell$ with CM by the maximal order of the primitive quartic CM field K, and assume that $K \neq \mathbb{Q}(\zeta_5)$. In [EL10, Proposition 4] it is shown that there 2 or 4 possibilities for the group order $\#\operatorname{Jac}(C)(\mathbb{F}_\ell)$. If there are four possible group orders and the constructed curve C does not have the right number of points on its Jacobian, then taking a twist of C may not be sufficient to get the desired curve and a different triple of invariants may be necessary.

Next we will define the Igusa invariants and the Igusa class polynomials of a genus 2 curve. Then we will describe an algorithm for computing them.

3.4. **Igusa invariants and Igusa class polynomials.** Using classical invariant theory over a field of characteristic zero, Clebsch defined a triple of invariants of a binary sextic f defining a genus 2 curve $y^2 = f(x)$. Bolza showed how those invariants could also be expressed in terms of theta functions on the period matrix associated to the Jacobian variety and its canonical polarization over $\mathbb{C}$. Igusa showed how these invariants could be extended to work in arbitrary characteristic [Igu67, p. 848], and so the invariants are often referred to as Igusa or Clebsch-Bolza-Igusa invariants.

In [Igu60, p. 620] Igusa defined invariants I_2, I_4, I_6, I_{10} and gave a bijection between isomorphism classes of genus 2 curves over K and points $(I_2 : I_4 : I_6 : I_{10})$ in weighted projective space with $I_{10} \neq 0$.

The ring of rational functions of the coarse moduli space for hyperelliptic curves of genus 2 is generated by the absolute Igusa invariants, which can be defined as:

$$i_1 := \frac{I_2^5}{I_{10}}, \quad i_2 := \frac{I_2^3 I_4}{I_{10}}, \quad i_3 := \frac{I_2^2 I_6}{I_{10}}.$$

(See [vW99, p. 313].) This choice of generators is not unique. The absolute Igusa invariants can be viewed as a generalization of the j-invariant for elliptic curves in the following sense: if i_1 is non-zero and the characteristic is not 2 or 3, these invariants agree for two genus 2 curves exactly when the two curves are isomorphic over an algebraically closed field. The moduli space of genus 2 curves is 3-dimensional and so three invariants are needed to specify a curve up to isomorphism over an algebraically closed field.

Given a primitive quartic CM field K, let $\mathcal{A}$ be a system of representatives for the set of isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$ having complex multiplication by $\mathcal{O}_K$. For each abelian variety $A \in \mathcal{A}$, let $(i_1(A), i_2(A), i_3(A))$ be the absolute Igusa invariants of A. Then the *Igusa class polynomials* H_j, for $j = 1, 2, 3$, are defined to be

$$H_j := \prod_{A \in \mathcal{A}} (X - i_j(A)).$$

Remark 3.5. The Igusa class polynomials are polynomials with coefficients in $\mathbb{Q}$. While the Hilbert class polynomial has integer coefficients, the Igusa class polynomials can have denominators. In order to run the algorithm in Theorem 3.6 below for computing them, we need to know which primes occur in the denominator and to which power. In [GL07], Goren and Lauter proved a bound on the primes which appear in the factorization of the denominators. In [GL12], they also gave a bound on the powers to which those primes appear. This bound, however, is not sharp. Independently, Bruinier and Yang formulated a conjecture that would give a way to compute the denominators of the Igusa class polynomials precisely [BY06]. Yang [Yan10, Yan13] proved this conjecture under certain assumptions on

the quartic number field K, and Lauter-Viray [LV15] proved the conjecture for all primitive quartic CM fields. Using [LV15] we can compute a bound on the denominators of the coefficients of H_1, H_2, H_3.

3.5. **Algorithm for computing Igusa class polynomials.** We have seen that in order to construct genus 2 curves with a prescribed number of points on the Jacobian, it suffices to compute the Igusa class polynomials of the quartic CM field K. As in the elliptic curve case, there are several known approaches for doing this. The complex analytic approach, which is the analogue for genus two curves of the Atkin-Morain CM method for elliptic curves, computes the Igusa class polynomials of a quartic CM field K by evaluating the modular invariants of all the abelian varieties of dimension 2 with CM by $\mathcal{O}_K$. The CM algorithm was first implemented by Spallek[Spa94], van Wamelen [vW99], and Weng [Wen03].

In this paper we present the CRT method for computing the Igusa class polynomials of a primitive quartic CM field K given in [EL10]. This approach is a generalization of the CRT method for elliptic curves [ALV04]. It first computes the Igusa class polynomials modulo p for sufficiently many small primes p. The Igusa class polynomials are then found using the Chinese Remainder Theorem and a bound on the denominators of the coefficients.

Theorem 3.6. *[EL10, Theorem 1] Given a primitive quartic CM field K, with totally real subfield K_0, the following algorithm finds the Igusa class polynomials of K:*

Algorithm 3.7. Computing Igusa class polynomials H_1, H_2, H_3 for K

(1) Produce a collection S of small rational primes $p \in S$ satisfying:
   (a) p splits completely in K and splits completely into principal ideals in K^*, the reflex of K.
   (b) Let B be the set of all primes of bad reduction for the genus 2 curves with CM by K. Then $S \cap B = \emptyset$.
   (c) $\prod_{p \in S} p > c$, where c is a constant related to the size of the coefficients and denominators of the Igusa class polynomials.

(2) Form the class polynomials H_1, H_2, H_3 modulo p for each $p \in S$. Let $H_{j,p}(X) := H_j(X) \mod p$. Then $H_{j,p}(X) = \prod_{C \in T_p}(X - i_j(C))$, where T_p is the collection of $\overline{\mathbb{F}}_p$-isomorphism classes of genus 2 curves over $\mathbb{F}_p$ whose Jacobian has endomorphism ring isomorphic to $\mathcal{O}_K$.

(3) *Chinese Remainder Step.* Form $H_j(X)$ from $\{H_{j,p}\}_{p \in S}$ $(j = 1, 2, 3)$.

To compute the Igusa class polynomials modulo p for a prime p satisfying the conditions above we do the following (see [EL10, Section 5.3]):

Algorithm 3.8. Computing Igusa class polynomials modulo p

(1) Loop through all possible triples of Igusa invariants (i_1, i_2, i_3). For each triple, construct a curve C over $\mathbb{F}_p$ with $(i_1, i_2, i_3) = (i_1(C), i_2(C), i_3(C))$ using Mestre's algorithm.

(2) For each curve C constructed, check whether $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

3.6. **Improvements for computing Igusa class polynomials.** The first improvement to the CRT method was given by Lauter and Freeman [FL08] who gave a more efficient algorithm to check whether $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. Checking this condition was needed in Step (2) of Algorithm 3.8 above for computing the Igusa class polynomials modulo p.

A further improvement to computing the Igusa class polynomials modulo p was given in [BGL11]: instead of looping through all possible triples of Igusa invariants and checking for each curve C whether $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$, as in Algorithm 3.8 above, the approach by Bröker-Gruenewald-Lauter finds *one* curve whose Jacobian has endomorphism ring equal to $\mathcal{O}_K$ (a so called *maximal curve*). The other curves in the isogeny class are then found by using computable $(3,3)$ isogenies.

Another improvement to this approach was proposed by Lauter and Robert in [LR13]. They showed that it was not necessary to find a maximal curve first. Instead they first find a curve C whose endomorphism ring is only an order in $\mathcal{O}_K$ and then give a probabilistic algorithm for "going up" to a maximal curve. Heuristically this improves the running time from p^3 per prime p to $p^{3/2}$ per prime p. Lauter-Robert give a mostly-heuristic analysis of their algorithm and state that at best their algorithm has quasiquadratic complexity in the discriminant of the quartic number field.

References

[ALV04] Amod Agashe, Kristin Lauter, and Ramarathnam Venkatesan. Constructing elliptic curves with a known number of points over a prime field. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 1–17. Amer. Math. Soc., Providence, RI, 2004.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[BBEL08] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 282–295. Springer, Berlin, 2008.

[BGL11] Reinier Bröker, David Gruenewald, and Kristin Lauter. Explicit CM theory for level 2-structures on abelian surfaces. *Algebra Number Theory*, 5(4):495–528, 2011.

[Brö08] Reinier Bröker. A p-adic algorithm to compute the Hilbert class polynomial. *Math. Comp.*, 77(264):2417–2435, 2008.

[BY06] Jan Hendrik Bruinier and Tonghai Yang. CM-values of Hilbert modular functions. *Invent. Math.*, 163(2):229–288, 2006.

[CH02] Jean-Marc Couveignes and Thierry Henocq. Action of modular correspondences around CM points. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 234–243. Springer, Berlin, 2002.

[CQ05] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Sci. Publ., Hackensack, NJ, 2005.

[EL10] Kirsten Eisenträger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 161–176. Soc. Math. France, Paris, 2010.

[FL08] David Freeman and Kristin Lauter. Computing endomorphism rings of Jacobians of genus 2 curves over finite fields. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 29–66. World Sci. Publ., Hackensack, NJ, 2008.

[GL07] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier (Grenoble)*, 57(2):457–480, 2007.

[GL12] Eyal Z. Goren and Kristin E. Lauter. Genus 2 curves with complex multiplication. *Int. Math. Res. Not. IMRN*, (5):1068–1142, 2012.

[Igu60] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[Igu67] Jun-ichi Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[LR13] Kristin E. Lauter and Damien Robert. Improved CRT algorithm for class polynomials in genus 2. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 437–461. Math. Sci. Publ., Berkeley, CA, 2013.

[LV15] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.

[Mes91] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Spa94] Anne-Monika Spallek. Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen. Ph.D. Thesis. Universität Gesamthochschule Essen, 1994.

[vW99] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.

[Wen03] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72(241):435–458 (electronic), 2003.

[Yan10] Tonghai Yang. An arithmetic intersection formula on Hilbert modular surfaces. *Amer. J. Math.*, 132(5):1275–1309, 2010.

[Yan13] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. *Asian J. Math.*, 17(2):335–381, 2013.

Current address: The Pennsylvania State University, University Park, PA 16802, USA
E-mail address: `eisentra@math.psu.edu`
URL: `http://www.personal.psu.edu/kxe8/`