Séminaires & Congrès
21, 2009, p. 161–176

A CRT ALGORITHM FOR CONSTRUCTING GENUS 2 CURVES OVER FINITE FIELDS

by

Kirsten Eisenträger & Kristin Lauter

Abstract. — We present a new method for constructing genus 2 curves over a finite field $\mathbb{F}_n$ with a given number of points on its Jacobian. This method has important applications in cryptography, where groups of prime order are used as the basis for discrete-log based cryptosystems. Our algorithm provides an alternative to the traditional CM method for constructing genus 2 curves. For a quartic CM field K with primitive CM type, we compute the Igusa class polynomials modulo p for certain small primes p and then use the Chinese remainder theorem (CRT) and a bound on the denominators to construct the class polynomials. We also provide an algorithm for determining endomorphism rings of ordinary Jacobians of genus 2 curves over finite fields, generalizing the work of Kohel for elliptic curves.

Résumé **(Un algorithme fondé sur le théorème chinois pour construire des courbes de genre 2 sur des corps finis)**

Nous présentons une nouvelle méthode pour construire des courbes de genre 2 sur un corps fini $\mathbb{F}_n$ avec un nombre donné de points sur sa jacobienne. Cette méthode a des applications importantes en cryptographie, où des groupes d'ordre premier sont employés pour former des cryptosystèmes fondés sur le logarithme discret. Notre algorithme fournit une alternative à la méthode traditionnelle de multiplication complexe pour construire des courbes de genre 2. Pour un corps quartique K à multiplication complexe de type primitif, nous calculons les polynômes de classe d'Igusa modulo p pour certains petits premiers p et employons le théorème chinois et une borne sur les dénominateurs pour construire les polynômes de classe. Nous fournissons également un algorithme pour déterminer les anneaux d'endomorphismes des jacobiennes de courbes ordinaires de genre 2 sur des corps finis, généralisant le travail de Kohel pour les courbes elliptiques.

2000 Mathematics Subject Classification. — 11G15, 11G10, 11R37, 14G50.
Key words and phrases. — Genus 2 curves, endomorphism rings, Igusa class polynomials, complex multiplication, Chinese Remainder Theorem.

The first author was partially supported by the National Science Foundation under agreement No. DMS-0111298 and by a National Science Foundation postdoctoral fellowship.

1. Introduction

In cryptography, some public key protocols for secure key exchange and digital signatures are based on the difficulty of the discrete logarithm problem in the underlying group. In that setting, groups such as the group of points on an elliptic curve or the group of points on the Jacobian of a genus 2 hyperelliptic curve over a finite field may be used. The security of the system depends on the largest prime factor of the group order, and thus it is desirable to be able to construct curves such that the resulting group order is prime. This paper presents an alternative to the CM (Complex Multiplication) algorithm for generating a genus 2 curve over a finite field with a known number of points on its Jacobian.

The CM algorithm for genus 2 is analogous to the Atkin-Morain CM algorithm for elliptic curves proposed in the context of primality testing ([**2**]). Whereas the Atkin-Morain algorithm generates the Hilbert class polynomial of an imaginary quadratic field K by evaluating the modular j-invariants of all elliptic curves with CM by K, the genus 2 algorithm generates what we will refer to as 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 K. Just as the j-invariant of an elliptic curve can be calculated in two ways, either as the value of a modular function on a lattice defining the elliptic curve as a complex torus over $\mathbb{C}$ or directly from the coefficients of the equation defining the elliptic curve, the triple of Igusa invariants ([**15, 16**]) of a genus 2 curve can also be calculated in two different ways. Using classical invariant theory over a field of characteristic zero, Clebsch defined the 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 ([**17**, p. 848], see also [**13**, Section 5.2]), and so the invariants are often referred to as Igusa or Clebsch-Bolza-Igusa invariants.

To recover the equation of a genus 2 curve given its invariants, Mestre gave an algorithm which works in most cases, and involves possibly passing to an extension of the field of definition of the invariants ([**22**]). The CM algorithm for genus 2 curves takes as input a quartic CM field K and outputs the Igusa class polynomials with coefficients in $\mathbb{Q}$ and if desired, a suitable prime p and a genus 2 curve over $\mathbb{F}_p$ whose Jacobian has CM by K. The CM algorithm has been implemented by Spallek ([**28**]), van Wamelen ([**30**]), Weng ([**31**]), Rodriguez-Villegas ([**25**]), and Cohn-Lauter ([**6**]). This method requires increasingly large amounts of precision of accuracy to obtain the theta values necessary to form the class polynomials. The running time of the CM algorithm has not yet been analyzed due to the fact that no bound on the denominators of the coefficients of the Igusa class polynomials was known prior to the work of [**13**].

The idea of the algorithm we present here is to calculate the Igusa class polynomials of a quartic CM field in a different way than the CM algorithm does. Our method

generalizes the algorithm for finding the Hilbert class polynomial given in [**1**] to the genus 2 situation. Given a quartic CM field K with primitive CM type, for each small prime p in a certain set we determine the Igusa class polynomial modulo p by finding all triples of invariants modulo p for which the corresponding genus 2 curve has CM by K. The Igusa class polynomial is then found using the Chinese Remainder Theorem (or the explicit CRT as in [**1**]) and a bound on the denominators of the coefficients.

Several difficulties arise in the genus 2 situation which are absent in the elliptic curve case. In this paper we resolve the following issues: the field of definition of a CM abelian variety, necessary conditions on the small primes for the algorithm to succeed, and the computation of the endomorphism ring of the Jacobian of a genus 2 curve in the ordinary case. Our algorithm for computing endomorphism rings of Jacobians of genus 2 curves over finite fields generalizes the work of Kohel ([**19**]) for elliptic curves.

1.1. Statement of the Theorem. — We will refer to a quartic CM field K with primitive CM type as a *primitive quartic CM 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 $(j_1(A), j_2(A), j_3(A))$ be the absolute Igusa invariants of A. Then the *Igusa class polynomials* H_i, for $i = 1, 2, 3$, are defined to be

$$H_i := \prod_{A \in \mathcal{A}} (X - j_i(A)).$$

It is known ([**27**]) that roots of these polynomials generate unramified abelian extensions of the reflex field of K. It is also known that Igusa class polynomials can be used to generate genus 2 curves with CM by K, and thus with a given zeta function over a suitable prime field (*cf.* Section 3). In this paper we prove the following theorem.

Theorem 1. — *Given a quartic CM field K with primitive CM type, the following algorithm finds the Igusa class polynomials of 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 $S \cap B = \varnothing$.

c. $\prod_{p \in S} p > c$, where c is a constant determined in Theorem 3.

(2) *Form the class polynomials H_1, H_2, H_3 modulo p for each $p \in S$. Let $H_{i,p}(X) := H_i(X) \mod p$. Then*

$$H_{i,p}(X) = \prod_{C \in T_p} (X - j_i(C)),$$

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 $H_i(X)$ from $\{H_{i,p}\}_{p \in S}$ $(i = 1, 2, 3)$.*

Remark 1. — *Condition 1(a) is enough to insure that p solves a relative norm equation in K/K_0, $\pi\overline{\pi} = p$, π a Weil number, and K_0 the real quadratic subfield of K (cf. Proposition 4 below).*

Remark 2. — *By* [**13**]*, the primes in the set B and in the denominators of the class polynomials are bounded effectively by a quantity related to the discriminant of K. Furthermore, it follows from* [**12**, Theorems 1 and 2] *and the discussion in* [**13**, Section 4.1] *that condition 1(b) is implied by condition 1(a).*

Remark 3. — *It follows from the Cebotarev density theorem that the density of the primes in the set S is inversely proportional to the class number of K in the case that K is Galois cyclic. In the non-Galois case, the density is inversely proportional to the degree of the normal closure of the composite of K with the Hilbert class field of the reflex of K.*

Our algorithm in the present form is not efficient, and we make no claims about the running time. A complete implementation of our algorithm is now available in [**8**], along with new efficient probabilistic algorithms for computing endomorphism rings. Our algorithm has the advantage that it does not require exponentially large amounts of precision of computation. It was recently brought to our attention that the paper [**5**] proposes a similar algorithm, but they give no proof of the validity of the approach. Indeed, they fail to impose the conditions necessary to make the algorithm correct and include many unclear statements. Also, while revising this paper, a p-adic approach to generating genus 2 curves was given in [**10**]. No comparison has yet been made between the different available approaches.

In Section 3 we show how Theorem 1 can be used to generate genus 2 curves with a given zeta function. The proof of Theorem 1 is given in Section 4. Implementation details for the algorithm are given in Section 5. In Section 6 we show how to determine the endomorphism ring of an ordinary Jacobian of a genus 2 curve. Section 7 gives an example of the computation of a class polynomial modulo a small prime.

Acknowledgments. — The authors thank E. Goren, E. Howe, K. Kedlaya, J-P. Serre, P. Stevenhagen, and T. Yang for helpful discussions. The authors also thank D. Freeman and the referee for valuable comments to improve the paper.

2. Notation

Throughout this paper, C denotes a smooth, projective, absolutely irreducible curve, and $J = J(C)$ will be its Jacobian variety with identity element $\mathbf{O}$. The field K is always assumed to be a primitive quartic CM field, $K \neq \mathbb{Q}(\zeta_5)$, with ring of integers $\mathcal{O}_K$. The real quadratic subfield of K is denoted by K_0, and a generator for the Galois group $\mathrm{Gal}(K/K_0)$ is denoted by a bar, $\omega \mapsto \bar{\omega}$. We will write K^* for the reflex of the quartic CM field K. For $i = 1, 2, 3$ we let $H_i(X)$ be the Igusa class polynomials of K, and for a prime $p \in S$ we let $H_{i,p} := H_i \mod p$. For a

field F, $\overline{F}$ will denote an algebraic closure of F. We say that C *has CM by* K if the endomorphism ring of $J(C)$ is isomorphic to the full ring of integers $\mathcal{O}_K$.

3. Generating genus 2 curves with a given zeta function

Our algorithm solves the following problem under certain conditions.

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

Given $(n,\ N_1,\ N_2)$, it is straightforward to find K, the quartic CM field such that the curve C has CM by K, by finding the quartic polynomial satisfied by Frobenius. Write $N_1 = n + 1 - s_1$, and $N_2 = n^2 + 1 + 2s_2 - s_1^2$, and solve for s_1 and s_2. Then K is generated over $\mathbb{Q}$ by the polynomial $t^4 - s_1 t^3 + s_2 t^2 - n s_1 t + n^2$.

Restrictions: If s_2 is prime to n, then the Jacobian is ordinary ([**14**, p. 2366]). Assume that $(s_2, n) = 1$. We also restrict to primitive CM fields K. If K is a quartic CM field, then K is not primitive iff $K/\mathbb{Q}$ is Galois and biquadratic ($\mathrm{Gal}(K/\mathbb{Q}) = V_4$) ([**27**, p. 64]). In the example in Section 7, K is given in the form $K = (i\sqrt{a + b\sqrt{d}})$, with $a, b, d \in \mathbb{Z}$ and d and (a, b) square free. In this form the condition is easy to check: K is primitive iff $a^2 - b^2 d \neq k^2$ for some integer k ([**18**, p. 135]). Assume further that K does not contain a cyclotomic field.

Solution: Given a triple $(n,\ N_1,\ N_2)$ satisfying the above restrictions, one can generate a curve C over $\mathbb{F}_n$ with the associated zeta function as follows. Compute K and its Igusa class polynomials H_1, H_2, H_3 using Theorem 1. From a triple of roots modulo n of H_1, H_2, H_3, construct a genus 2 curve over $\mathbb{F}_n$ using the combined algorithms of Mestre ([**22**]) and Cardona-Quer ([**4**]). To match triples of roots, in practice one can test whether the curve generated has the correct zeta function by checking the number of points on the Jacobian of the curve. A curve C with the correct zeta function will have $\#J(C)(\mathbb{F}_n) = N = (N_1^2 + N_2)/2 - n$. 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 (n, K) (*cf.* Section 5.1), a different triple of invariants may be tried until the desired group order is obtained.

4. Proof of Theorem 1

Given a primitive quartic CM field K, let $\mathcal{A}$ be a system of representatives of the isomorphism classes of simple principally polarized abelian surfaces over $\mathbb{C}$ with CM by K. Each element of $\mathcal{A}$ has a field of definition k which is a finite extension of $\mathbb{Q}$ ([**27**, Prop. 26, p. 96]). For any prime $p \in S$ satisfying the conditions of Theorem 1, the set T_p was defined in Step 2 of Theorem 1 as the collection of $\overline{\mathbb{F}}_p$-isomorphism classes of genus 2 curves over $\mathbb{F}_p$ with an isomorphism of $\mathcal{O}_K$ with $\mathrm{End}(J(C))$. We claim that we have a bijective correspondence between $\mathcal{A}$ and T_p. Moreover, we claim that reducing the Igusa invariants gives the Igusa invariants of the reduction. Taken together, these can be stated in the form of the following theorem:

Theorem 2. — *Let K be a primitive quartic CM field and let $p \in S$ be a rational prime that satisfies the conditions of Theorem 1. Then*

$$H_{i,p}(X) = \prod_{C \in T_p} (X - j_i(C)),$$

where $H_{i,p}(X)$ and T_p are defined as in Theorem 1.

Proof. — Let $A \in \mathcal{A}$ be a principally polarized abelian surface with CM by K, defined over a number field k. Let k_0 be its field of moduli (see [**27**, p. 27] for the definition). By class field theory, p splits completely into principal ideals in K^* if and only if p splits completely in H^*, the maximal unramified abelian extension of K^* ([**7**, Corollary 5.25]). The field of moduli k_0 is contained in H^* (see [**27**, Main Theorem 1, p. 112]), but in general it is not true that $k = k_0$. By a theorem of Shimura (see [**26**, Ex. 1, p. 525], see also [**12**, Proposition 2.1]) if K is a primitive quartic CM field, then k is contained in k_0, so A is defined over k_0.

Proposition 2.1 of [**12**] also shows that A has good reduction at any prime β of $\mathcal{O}_{H^*}$. Let A_p be the reduction of A modulo a prime above p. Then because p splits completely in the Galois closure of K, A_p is ordinary ([**12**, Theorems 1 and 2]) and because p splits completely into principal ideals in K^*, A_p is defined over $\mathbb{F}_p$. By condition 1(b) of Theorem 1, A_p is the Jacobian of a genus 2 curve C over $\mathbb{F}_p$ ([**24**]). Then C is an element of T_p.

We must show that this correspondence is one-to-one and onto. To show that it is one-to-one, we can generalize the argument in [**20**, Theorem 13, p. 183]. Let $A, B \in \mathcal{A}$, and for $p \in S$ let A_p and B_p be the reductions of A and B as above. Assume that A_p and B_p are isomorphic over $\overline{\mathbb{F}}_p$, and let $\varepsilon : B_p \to A_p$ be an isomorphism. The varieties A and B both have CM by K, hence there exists an isogeny $\lambda : A \to B$ ([**27**, Corollary, p. 41]) giving rise to a reduced isogeny $\lambda_p : A_p \to B_p$. Since the endomorphism ring of A is preserved under the reduction map, there exists $\alpha \in \mathrm{End}(A)$ such that the reduction α_p satisfies $\alpha_p = \varepsilon \circ \lambda_p$. Let C be the image of the map $\lambda \times \alpha : A \times A \to B \times A$. With a similar argument as in [**20**, p. 184], one can then show that C is the graph of an isomorphism between A and B. Similarly, if there is an isomorphism of the principal polarizations on A_p and B_p then this isomorphism lifts to an isomorphism of the polarizations on A and B. This shows that the correspondence is one-to-one.

The correspondence is onto because, given a genus 2 curve C over $\mathbb{F}_p$ with CM by K representing a class of T_p, its Jacobian $J(C)$ is ordinary and so it can be lifted, along with its endomorphism ring and its polarization, to its "Serre-Tate canonical lift", A, defined over the Witt vectors $W(\mathbb{F}_p) = \mathbb{Z}_p$ ([**21**, Theorem 3.3, p. 172]). Let L be the field generated over $\mathbb{Q}$ by all the coefficients of the equations defining A. Then A is defined over L and since L has finite transcendence degree over $\mathbb{Q}$, we can embed it into $\mathbb{C}$. So we can lift $J(C)$ to an abelian variety with CM by K defined over $\mathbb{C}$.

By assumption 1(b) of Theorem 1, no prime above $p \in S$ is a prime of bad reduction for a genus 2 curve with CM by K, so by [**13**, Cor 5.1.2], $p \in S$ is coprime to the denominators of the class polynomials $H_i(X)$. We claim that reducing the coefficients

of H_i modulo p gives the same result as taking the polynomial whose roots are the absolute Igusa invariants of the curves over $\mathbb{F}_p$ with Jacobians equal to the reductions modulo a prime above p of the abelian varieties A representing the classes of $\mathcal{A}$. Since the absolute Igusa invariants are rational functions in the coefficients of the curve, the order of computation of the invariants and reduction modulo a prime can be reversed as long as the primes in the denominator are avoided and an appropriate model for the curve is chosen. □

Theorem 3. — *Suppose the factorization of the denominators of the Igusa class polynomials is known. Let ν be the largest absolute value of the coefficients of the H_i, and let λ be the least common multiple of the denominators of the coefficients of the H_i $(i = 1, 2, 3)$. Let S be a set of rational primes such that $S \cap B = \varnothing$ and $\prod_{p\in S} p > c$, where $c = 2\lambda \cdot \nu$. Then the Chinese Remainder Theorem can be used to compute the class polynomials $H_i(X) \in \mathbb{Q}[X]$ from the collection $\{H_{i,p}\}_{p\in S}$, $i = 1, 2, 3$.*

Proof. — By assumption λ is prime to all $p \in S$. The polynomials

$$F_i(X) := \lambda \cdot H_i(X) \; i = 1, 2, 3$$

have integer coefficients. For each $p \in S$ let

$$F_{i,p} := F_i \bmod p = \lambda \cdot H_{i,p} \bmod p.$$

Apply the Chinese Remainder Theorem to the collection $\{F_{i,p}\}_{p\in S}$ to obtain a polynomial which is congruent to $F_i \in \mathbb{Z}[X]$ modulo the product $\prod_{p\in S} p$. Since c was taken to be twice λ times the largest absolute value of the coefficients, we have found F_i, and so $H_i = \lambda^{-1} \cdot F_i$. □

Remark 4. — *It was proved in* [**13**] *that the primes dividing the denominators are bounded effectively in terms of the field K by a quantity related to the discriminant. The power to which each prime in the denominator appears has also been bounded in recent work of Goren, and so we can conclude that we have a bound on the denominators of the class polynomials.*

Proof of Theorem 1. — The proof of Theorem 1 now follows immediately from Theorem 2 and Theorem 3. □

5. Implementation

5.1. The possible group orders for each p. — Suppose that C is a genus 2 curve defined over $\mathbb{F}_p$ with CM by K. To find all possible group orders for $J(C)(\mathbb{F}_p)$, let $\pi \in O_K$ correspond to the Frobenius endomorphism of C. Since the Frobenius satisfies $\pi\overline{\pi} = p$, it follows that the relative norm of π is p, i.e. $\mathbf{N}_{K/K_0}(\pi) = p$, and hence $\mathbf{N}(\pi) = \mathbf{N}_{K/\mathbb{Q}}(\pi) = p^2$. So if K is fixed, primes p for which there exist genus 2 curves modulo p with CM by K are primes for which there are solutions to the relative norm equation: $\mathbf{N}_{K/K_0}(\pi) = p$. The following proposition gives the number of possible group orders in each case. It overlaps with [**32**, Thm 4.1], but our statement, assumptions, and

proof are all slightly different, and we use the details of this proof in our algorithm, so we include it here. Note that, as pointed out in [**32**], it is not known whether two of the four possible group orders could coincide in the non-Galois case.

Proposition 4. — *Fix a primitive quartic CM field K, and a rational prime p unramified in K. Assume that $K \neq \mathbb{Q}(\zeta_5)$, so that the only roots of unity in K are $\{\pm 1\}$. Then*

(A) There are either 0, 2 or 4 possibilities for the group order $\#J(C)(\mathbb{F}_p)$ of curves C with CM by K.

(B) Under the additional assumption that p splits completely into principal ideals in K^* and splits completely in K, there are always 2 possible group orders in the cyclic case and 4 possible group orders in the non-Galois case.

Proof. — We consider all possible decompositions of the prime p in K.

Case 1: There exists a prime ideal $\mathfrak{p}$ of K_0 above p that does not split in K. In this case there is no solution to the relative norm equation.

Case 2: The rational prime p is inert in $K_0/\mathbb{Q}$, and the prime $\mathfrak{p}$ of K_0 above p splits in K with $\mathfrak{P}_1|\mathfrak{p}$ and $\mathfrak{P}_2|\mathfrak{p}$. We have $\overline{\mathfrak{P}_1} = \mathfrak{P}_2$. In this case there are two ideals of norm p^2, $\mathfrak{P}_1$ and $\mathfrak{P}_2$. If $\mathfrak{P}_1$ is not principal, then there are no solutions to the norm equation. If $\mathfrak{P}_1$ is principal with generator π, then $\mathfrak{P}_2 = (\overline{\pi})$, and $\pi\overline{\pi} = p$. The elements π and $\overline{\pi}$ are Galois conjugates, so by Honda-Tate π and $-\pi$ give rise to all possible group orders. Let $\pi_1 := \pi$, and let $\pi_2, \ldots, \pi_4$ be its conjugates over $\mathbb{Q}$. Then $m_1 = \prod_{i=1}^{4}(1-\pi_i)$ and $m_2 = \prod_{i=1}^{4}(1-(-\pi_i))$ are the 2 possible group orders for the Jacobian.

Case 3: p splits completely in $K/\mathbb{Q}$, with $\mathfrak{P}_1, \ldots, \mathfrak{P}_4$ lying above p and with $\overline{\mathfrak{P}_1} = \mathfrak{P}_2$, and $\overline{\mathfrak{P}_3} = \mathfrak{P}_4$. Then $\mathfrak{P} := \mathfrak{P}_1\mathfrak{P}_3$, $\mathfrak{Q} := \mathfrak{P}_1\mathfrak{P}_4$, and $\overline{\mathfrak{P}}$ and $\overline{\mathfrak{Q}}$ are the only ideals with relative norm p.

Subcase (a) If $K/\mathbb{Q}$ is Galois, then the Galois group is cyclic, since we assumed that K was a primitive CM field ([**27**, p. 65]). Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Then w.l.o.g. $\mathfrak{P}_2 = \mathfrak{P}_1^{\sigma^2}, \mathfrak{P}_3 = \mathfrak{P}_1^{\sigma}$, and $\mathfrak{P}_4 = \mathfrak{P}_1^{\sigma^3}$. Thus $\mathfrak{P} = \mathfrak{P}_1\mathfrak{P}_1^{\sigma} = (\mathfrak{P}_1\mathfrak{P}_1^{\sigma^3})^{\sigma} = \mathfrak{Q}^{\sigma}$, so if $\mathfrak{P}$ is principal, so is $\mathfrak{Q}$, and their generators, ω and ω^{σ} give rise to isogenous curves. Hence if $\mathfrak{P}$ is principal, then there are two possible group orders as before, and if it is not principal, then the relative norm equation has no solution.

Subcase (b) If $K/\mathbb{Q}$ is not Galois, then the Galois group of its splitting field is the dihedral group D_4 ([**27**, p. 65]). In this case $\mathfrak{P}$ and $\mathfrak{Q}$ are not Galois conjugates. So if both $\mathfrak{P}$ and $\mathfrak{Q}$ are principal, then there are 4 possible group orders, if only one of them is principal, then there are 2 possible group orders, and otherwise there are no solutions to the relative norm equation.

Statement (A) follows from the 3 cases considered above. Statement (B) concerns Case 3. If K is Galois, then $K = K^*$ and the additional assumptions imply that $\mathfrak{P}$ is principal, and then there are 2 possible group orders. If K is not Galois, let L be the Galois closure with dihedral Galois group $\mathrm{Gal}(L/\mathbb{Q}) = \langle \tau, \sigma : \tau^2, \sigma^4, \tau\sigma\tau\sigma \rangle$ such that K is the fixed field of τ and the CM type is $\{1, \sigma\}$. Then σ^2 is complex conjugation.

According to [**12**, Theorem 2], a rational prime p that splits completely in L with $\mathcal{P} := p\mathcal{O}_L$ decomposes as follows in K and K^*:

$$p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4 = (\mathcal{P}\mathcal{P}^\tau)(\mathcal{P}^{\sigma^2}\mathcal{P}^{\tau\sigma^2})(\mathcal{P}^\sigma\mathcal{P}^{\tau\sigma})(\mathcal{P}^{\sigma^3}\mathcal{P}^{\tau\sigma^3}),$$

$$p\mathcal{O}_{K^*} = \mathfrak{P}_1^*\mathfrak{P}_2^*\mathfrak{P}_3^*\mathfrak{P}_4^* = (\mathcal{P}\mathcal{P}^{\tau\sigma^3})(\mathcal{P}^{\sigma^2}\mathcal{P}^{\tau\sigma})(\mathcal{P}^\sigma\mathcal{P}^\tau)(\mathcal{P}^{\sigma^3}\mathcal{P}^{\tau\sigma^2}).$$

By assumption, $\mathfrak{P}_1^*$, $\mathfrak{P}_2^*$, $\mathfrak{P}_3^*$, $\mathfrak{P}_4^*$ are principal. Thus both $\mathfrak{P}$ and $\mathfrak{Q}$ are principal since $\mathfrak{P} = \mathfrak{P}_1\mathfrak{P}_3 = \mathfrak{P}_3^*(\mathfrak{P}_4^*)^\sigma$, and $\mathfrak{Q} = \mathfrak{P}_1\mathfrak{P}_4 = \mathfrak{P}_1^*(\mathfrak{P}_1^*)^\tau$. Thus there are 4 possible group orders when K is not Galois. □

5.2. Generating the collection of primes S. — In practice, to generate a collection of primes belonging to S there are several alternatives. One approach is to run through small primes checking the splitting behavior in K and K^* using a computational number theory software package like PARI. A second approach is to generate solutions to the relative norm equation directly as in [**31**, Section 8], then check each solution for the splitting in K and K^* and check for the other solution to the relative norm equation in the case that K is not Galois. One advantage to this approach is that it gives direct control over the index of $\mathbb{Z}[\pi, \overline{\pi}]$ in $\mathcal{O}_K$ in terms of the coefficients c_i of π, the solution to the relative norm equation (*cf.* Proposition 5).

5.3. Computing Igusa class polynomials modulo p. — Let $p \in S$. To compute the Igusa class polynomials mod p we must find all $\overline{\mathbb{F}}_p$-isomorphism classes of genus 2 curves over $\mathbb{F}_p$ whose Jacobian has CM by K. This can be done as follows:

(1) For each triple of Igusa invariants modulo p, generate a genus 2 curve with those Igusa invariants using an implementation of the Mestre-Cardona-Quer algorithm ([**22**], [**4**]).

(2) Let $N_p := \{(n_1, m_1), (n_2, m_2), \ldots, (n_r, m_r)\}$ be the set of possible group orders $(\#C(\mathbb{F}_p), \#J(C)(\mathbb{F}_p))$ of curves C which have CM by K as computed above in Section 5.1.

(3) Collect all curves C such that $(\#C(\mathbb{F}_p), \#J(C)(\mathbb{F}_p)) \in N_p$ as follows: for each triple of invariants and a corresponding curve C, take a random point Q on $J(C)$. Multiply Q by $m_1, \ldots, m_r$ and check if the identity element is obtained for some r. If not, then C does not belong to T_p. If a curve passes this test, then count the number of points on the curve and its Jacobian over $\mathbb{F}_p$ to check whether the Jacobian has the right isogeny type. This procedure obtains all curves in the desired isogeny class. For each curve in the desired isogeny class, the endomorphism ring of the Jacobian contains the ring $\mathbb{Z}[\pi, \overline{\pi}]$ and is contained in the ring $\mathcal{O}_K$. The curve is included in the set T_p only if $\mathrm{End}_{\mathbb{F}_p}(J(C)) = \mathcal{O}_K$. In the next section, we will show how to test this property by computing the endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(J(C))$.

6. Computing endomorphism rings of genus 2 curves

6.1. The index of $\mathbb{Z}[\pi,\overline{\pi}]$ in $\mathcal{O}_K$. — For a prime p and a Frobenius element $\pi \in \mathcal{O}_K$, the smaller the index of $\mathbb{Z}[\pi,\overline{\pi}]$ in $\mathcal{O}_K$, the less work it takes to compute the endomorphism ring. For example, if the index is 1, then we can determine whether $C \in T_p$ just from counting points on C and its Jacobian. Proposition 5 gives a bound for the index of $\mathbb{Z}[\pi,\overline{\pi}]$ in $\mathcal{O}_K$.

Proposition 5. — *Let $K := \mathbb{Q}(\eta)$ be a quartic CM field, where $\eta = i\sqrt{a+b\sqrt{d}}$ with $a,b,d \in \mathbb{Z}$ and d and (a,b) square free. Let $\mathcal{O}_K$ be its ring of integers. Assume for simplicity that the Frobenius endomorphism of C is of the form $\pi := c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})\eta$ with $c_1,\ldots,c_4 \in \mathbb{Z}$, that $a^2 - b^2 d$ is square free and that the real quadratic subfield K_0 has class number 1. If $d \equiv 2,3 \bmod 4$, then $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ divides $8c_2(c_3^2 - c_4^2 d)$. If $d \equiv 1 \bmod 4$, then $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ divides $16c_2(c_3^2 - c_4^2 d)$.*

Proof. — We have

$$\pi + \overline{\pi} - 2c_1 = 2c_2\sqrt{d}, \tag{1}$$

$$[2c_2c_3 - c_4(\pi + \overline{\pi} - 2c_1)](\pi - \overline{\pi}) = 4c_2(c_3^2 - c_4^2 d)\eta, \tag{2}$$

$$(c_3 - c_4\sqrt{d})(\pi - \overline{\pi}) = 2(c_3^2 - c_4^2 d)\eta. \tag{3}$$

So $\mathbb{Z}[2c_2\sqrt{d}, 4c_2(c_3^2 - c_4^2 d)\eta] \subseteq \mathbb{Z}[\pi,\overline{\pi}]$. Since K_0 has class number 1, we have a relative integral basis of $\mathcal{O}_K$ over $\mathcal{O}_{K_0}$. We can choose a relative basis of the form $\{1,\kappa\}$, and by [**29**], in the case that $d \equiv 2,3 \bmod 4$, κ is either

$$1.\ \eta/2 \qquad 2.\ (1+\eta)/2 \qquad 3.\ (\sqrt{d}+\eta)/2 \qquad 4.\ (1+\sqrt{d}+\eta)/2.$$

In each case the index of $\mathbb{Z}[\sqrt{d},\eta]$ in $\mathcal{O}_K$ is 2. For $d \equiv 1 \bmod 4$, κ is either

$$5.\ (1+\sqrt{d}+2\eta)/4 \qquad 6.\ (-1+\sqrt{d}+\eta)/4 \qquad 7.\ (-b+\sqrt{d}+2\eta)/4.$$

Here, in each case the index of $\mathbb{Z}[\sqrt{d},\eta]$ in $\mathcal{O}_K$ is 4. We have

$$\mathbb{Z}[\pi,\overline{\pi}] \subseteq \mathbb{Z}[\pi,\overline{\pi},\sqrt{d}] \subseteq \mathbb{Z}[\sqrt{d},\eta] \subseteq \mathcal{O}_K,$$

with $[\mathbb{Z}[\pi,\overline{\pi},\sqrt{d}] : \mathbb{Z}[\pi,\overline{\pi}]]$ dividing $2c_2$ and $[\mathbb{Z}[\sqrt{d},\eta] : \mathbb{Z}[\pi,\overline{\pi},\sqrt{d}]]$ dividing $2(c_3^2 - c_4^2 d)$. If $d \equiv 2,\ 3 \bmod 4$, then $[\mathcal{O}_K : \mathbb{Z}[\sqrt{d},\eta]] = 2$, and hence the index $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ divides $8c_2(c_3^2 - c_4^2 d)$. If $d \equiv 1 \bmod 4$, then $[\mathcal{O}_K : \mathbb{Z}[\sqrt{d},\eta]] = 4$, and hence $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ divides $16c_2(c_3^2 - c_4^2 d)$. Since the index is a positive integer, it is thus also bounded by these quantities. □

So if we want to minimize the index $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ then we have to minimize $c_2(c_3^2 - c_4^2 d)$. When $a^2 - b^2 d$ is not square free the representation of the ring of integers can become more complicated ([**29**]), but the term we need to minimize is still $c_2(c_3^2 - c_4^2 d)$. Using the relative basis of $\mathcal{O}_K$ over $\mathcal{O}_{K_0}$ we can also determine which denominators can occur in the coefficients c_i of the Frobenius endomorphism and generalize our argument to the general case.

6.2. Determining the index of $\mathrm{End}(J)$ in $\mathcal{O}_K$. — We can summarize the necessary conditions to ensure that $[\mathcal{O}_K : \mathrm{End}(J)] = 1$ as follows:

Lemma 6. — *Under the conditions of Section 6.1, to show that the endomorphism ring of a curve is the full ring of integers $\mathcal{O}_K$, it is sufficient to test whether:*

1. *$\sqrt{d}$ is an endomorphism, where $2c_2\sqrt{d} = \pi + \overline{\pi} - 2c_1$.*
2. *η is an endomorphism, where*
$$(4c_2(c_3^2 - c_4^2 d))\eta = (2c_2c_3 - c_4(\pi + \overline{\pi} - 2c_1))(\pi - \overline{\pi}).$$
Here the c_i's are the coefficients of π written in the relative basis.
3. *κ is an endomorphism, where κ is one of the 7 possible elements listed in Section 6.1 in the case that $a^2 - b^2 d$ is square free.*

If any one of these conditions fails, we conclude that the endomorphism ring of the curve is not the full ring of integers $\mathcal{O}_K$. When $a^2 - b^2 d$ is not square free then the relative integral basis is listed in the table in [**29**, p. 186]. This algorithm can also be modified to test whether the endomorphism ring of the curve is some other subring of $\mathcal{O}_K$ or to compute the endomorphism ring exactly.

To test whether $\sqrt{d}$, η, and κ are endomorphisms, we express them as above as polynomials in π and $\overline{\pi}$ with integral denominators determined by the c_i. It will be proved in Section 6.3 below that in each case it suffices to check whether the numerator acts as zero on the s-torsion, where s is the denominator.

6.3. Action on s-torsion

Proposition 7. — *Assume that k is an algebraically closed field and that A, B, C are abelian varieties over k. Let $\beta : A \to B$, $\gamma : A \to C$ be two isogenies with β separable and $\mathrm{Ker}(\beta) \subseteq \mathrm{Ker}(\gamma)$. Then there is a homomorphism $\delta : B \to C$ such that $\delta \cdot \beta = \gamma$.*

Proof. — This proof follows the argument of Remark 7.12 in [**23**, p. 37]. Since β is separable, we can form the quotient abelian variety $A/\mathrm{Ker}(\beta)$. From the universal property of $A/\mathrm{Ker}(\beta)$ we have a regular map $A/\mathrm{Ker}\,\beta \to B$, which is again separable and bijective. Since B is nonsingular, this implies that it is an isomorphism. Thus $B \cong A/\mathrm{Ker}(\beta)$. After identifying B with $A/\mathrm{Ker}(\beta)$ and using the universal properties of quotients again we find that there is a unique regular map δ such that $\delta \cdot \beta = \gamma$. Moreover, δ is automatically a homomorphism because it maps $\mathbf{O}$ to $\mathbf{O}$. □

Proposition 8. — *Let k be an algebraically closed field and let A be an abelian variety over k. Let $R := \mathrm{End}_k A$. Let $s \in R$ be separable and let $A[s] = \{P \in A(k) : sP = \mathbf{O}\} = \mathrm{Ker}(s)$. Then $A[s]$ is a faithful R/Rs-module.*

Proof. — Clearly, $A[s]$ is an R/Rs-module. We have to show that $A[s]$ is a faithful R/Rs-module; that is, any $r \in R$ with $r \cdot A[s] = 0$ belongs to Rs. Suppose r is such that $r \cdot A[s] = 0$. Since s is separable, this implies that $r = ts$ for some endomorphism t of A by Proposition 7 above applied with $A = B = C$, $\beta = s$ and $\gamma = r$. This implies that $r \in Rs$, which proves the claim. □

We will frequently use the following

Corollary 9. — *Let A, k be as in Proposition 8. Let n be a positive integer coprime to the characteristic of k. Suppose that $\alpha : A \to A$ is an endomorphism, with $A[n] \subseteq Ker(\alpha)$, i.e. α acts as zero on the n-torsion. Then $\alpha = \beta \cdot n = n \cdot \beta$, for some endomorphism β, i.e. α is divisible by n in $R = \mathrm{End}_k(A)$.*

6.4. Computing the index using division polynomials. — In [**3**], Cantor finds recursive formulae for division polynomials for hyperelliptic curves with one point at infinity, P_∞. The rth division polynomials he defines are $(\delta_r(X), \epsilon_r(X))$ such that $(\delta_r(\frac{x-X}{4y^2}), \epsilon_r(\frac{x-X}{4y^2}))$ represents $r \cdot (x, y)$, where (x, y) is a point on the curve thought of as the point $(x, y) - P_\infty$ on the Jacobian. For a general point on the Jacobian represented as $D = P_1 + P_2 - P_\infty$, we see that $rD = 0$ iff $rP_1 = -rP_2$. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then we can write down a system of equations and an ideal, I_r, defining the solutions to the system, where I_r is an ideal in $\mathbb{F}_p[x_1, x_2, y_1, y_2]$. Various ways of finding the ideal I_r have been investigated, from Gröbner bases to resultant computations (see [**9**] and [**11**]).

The ideal I_r can be used to test the action of endomorphisms on the r-torsion. For example, to check that π^k (or any other polynomial in π) acts like a on the r-torsion, it suffices to check that in $\mathbb{F}_p[x_1, x_2, y_1, y_2]$,

$$\pi^k(D) \equiv aD \mod I_r.$$

Even if the best method for computing the I_r is not yet completely well understood in practice, in theory this is likely the most efficient way to compute the action of endomorphisms on r-torsion.

6.5. Computing the index through direct computation of the action of Frobenius on the torsion subgroups. — In practice, we used a computational number theory software package like MAGMA to compute the group structure of $J(C)(\mathbb{F}_{p^k})$ for small values of k. Using the generators of $J(C)(\mathbb{F}_{p^k})$ we then explicitly computed the action of Frobenius on various torsion subgroups to determine whether or not certain elements of the ring of integers are endomorphisms. An example will be given in the next section. In the example we will use the following fact repeatedly:

Fact 10. — *Let γ_k be a positive integer coprime to p. All the γ_k-torsion is defined over $\mathbb{F}_{p^k}$ if and only if $\frac{\pi^k - 1}{\gamma_k}$ is an endomorphism.*

Fact 10 follows immediately from Corollary 9. Note that it is *not* true in general that the field of definition of the r-torsion for all m is enough to determine the endomorphism ring. We found examples of curves where the field of definition of the r-torsion was the same for all r, but the endomorphism rings were different because the action of Frobenius on the torsion subgroups was different. However, there are special cases where checking the field of definition of the torsion is enough:

Remark 5. — *In the case where $\mathcal{O}_K$ is generated by elements of the form $\frac{\pi^k-1}{\gamma_k}$, for some collection of pairs of integers (k,γ_k), then equality of the endomorphism ring with $\mathcal{O}_K$ can be checked simply by checking the field of definition of the γ_k-torsion.*

7. Example

Let $K := \mathbb{Q}(i\sqrt{13-3\sqrt{13}})$. In this example we will find the Igusa class polynomials of K modulo 43 by finding all genus 2 curves C defined over $\mathbb{F}_{43}$ (up to isomorphism over the algebraic closure of $\mathbb{F}_{43}$) such that $\mathrm{End}(J(C)) \cong \mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K. Let K^* be the reflex of K. Since $a^2 - b^2 d = 2^2 \cdot 13$, the extension $K/\mathbb{Q}$ is cyclic ([**18**, p. 88]), and hence $K^* = K$ ([**27**, p. 65]). The real quadratic subfield of K is $K_0 := \mathbb{Q}(\sqrt{13})$. The prime 43 splits completely in $K = K^*$. The class number of K is 2, and so since K is Galois, we expect two classes of curves over $\mathbb{F}_{43}$ with CM by K. Let $\eta := i\sqrt{13-3\sqrt{13}}$. The ring of integers of K is

$$\mathcal{O}_K = \mathbb{Z} + \frac{\sqrt{13}+1}{2}\mathbb{Z} + (\mathbb{Z} + \frac{\sqrt{13}+1}{2}\mathbb{Z})\,\eta.$$

Let $\delta := (1+\sqrt{13})/2$. The prime 43 factors in K/K_0 as:

$$43 = \pi \cdot \overline{\pi} = (-3 + 2\cdot\delta + (-2-\delta)\,\eta)\cdot(-3+2\cdot\delta) + (2+\delta)\,\eta).$$

The characteristic polynomial of the Frobenius element corresponding to π is

$$\psi(t) = 1849t^4 + 344t^3 + 50t^2 + 8t + 1.$$

Let C be a curve over $\mathbb{F}_{43}$ whose Frobenius is $\pm\pi$. Then the possibilities for $(\#C(\mathbb{F}_{43}), \#J(C)(\mathbb{F}_{43}))$ are $(52, 2252)$ and $(36, 1548)$. Using MAGMA we found (up to isomorphism over $\overline{\mathbb{F}}_{43}$) 67 curves whose Frobenius is $\pm\pi$. However, not all 67 curves have endomorphism ring equal to the full ring of integers. To eliminate those with smaller endomorphism ring, we first observe that

$$\frac{\pi^4-1}{12} = -2 + 24\sqrt{13} + \frac{17}{2}\sqrt{13}i\sqrt{13-3\sqrt{13}} + \frac{113}{2}i\sqrt{13-3\sqrt{13}} \in \mathcal{O}_K.$$

Then Fact 10 implies that any curve whose endomorphism ring is the full ring of integers must have the full 12-torsion defined over $\mathbb{F}_{43^4}$. We can check that this eliminates all but 6 of the 67 curves. The Igusa invariants of the remaining 6 curves are:

$$(3,24,36), (4,29,28), (29,24,13), (20,21,29), (20,23,19), (36,21,6).$$

We expect only 2 curves over $\mathbb{F}_{43}$ (up to isomorphism) with CM by K. To eliminate the other 4 curves from this list, it is enough in this case to check the action of Frobenius on the 4-torsion. By Corollary 9, $\delta = \frac{\pi+\overline{\pi}+6}{4}$ is an endomorphism of $J(C)$ if and only if $\pi + \overline{\pi} + 6$ acts as zero on the 4-torsion, or equivalently, $\pi + \overline{\pi}$ acts as multiplication-by-2 on the 4-torsion.

Consider a curve C with Igusa invariants $(20,23,19)$ given by the equation $C : y^2 = 5x^6 + 21x^5 + 36x^4 + 7x^3 + 29x^2 + 32x + 10$ over $\mathbb{F}_{43}$. All the 4-torsion is defined over

a degree 4 extension, and we can use MAGMA to compute a basis for the 4-torsion by computing the abelian group structure over the degree 4 extension.

We can then compute that the action of Frobenius on the 4-torsion is given in terms of some basis by the matrix F, and the action of $\overline{\pi}$ is given given by V:

$$F = \begin{pmatrix} 1 & 0 & 1 & 3 \\ 2 & 1 & 1 & 0 \\ 0 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 0 & 3 & 1 \\ 2 & 1 & 3 & 0 \\ 0 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{pmatrix}.$$

From this it is easy to see that $\pi + \overline{\pi} = [2]$ on the 4-torsion, so δ is an endomorphism of C. Performing the identical computation on a curve C with Igusa invariants $(36, 21, 6)$, we find that δ is also an endomorphism for this curve. Doing the same calculation for the remaining 4 triples of Igusa invariants $(3, 24, 36), (4, 29, 28), (29, 24, 13), (20, 21, 29)$, we see that $\pi + \overline{\pi} = [2]$ does not hold on the 4-torsion in those cases, so $\delta \notin \mathrm{End}(J(C))$ for any of the corresponding curves.

It is easy to see in this case that $\delta \in \mathrm{End}(J(C))$ and $\frac{\pi^4 - 1}{12} \in \mathrm{End}(J(C))$ is enough to conclude that $\mathrm{End}(J(C)) = \mathcal{O}_K$. Hence the two triples of invariants corresponding to curves with CM by K are $(36, 21, 6)$ and $(20, 23, 19)$. In conclusion, we have obtained the three Igusa class polynomials modulo 43 with our method:

$$H_{1,43}(X) = X^2 + 30X + 32,$$

$$H_{2,43}(X) = X^2 + 42X + 10,$$

$$H_{3,43}(X) = X^2 + 18X + 28.$$

These indeed agree modulo 43 with the class polynomials with rational coefficients computed by evaluating the quotients of Siegel modular forms with 200 digits of precision as computed by van Wamelen ([**30**]):

$$H_1(X) = X^2 - \frac{962543029253423944376809385933654662465606680133168051551192 4}{122416050313833727099273279640254521070594994 7} X + \frac{172118931035488051448159388624541408082526332130392912086861191129180767889416746834116360 04}{586706876460170625283388149341641614203283689221807467790532225 69},$$

$$H_2(X) = X^2 - \frac{323763162495966993699857124251532433502726 0}{797313250245852337928259762 9} X + \frac{101869481833026643236326057638275086345512388711354393815337676100}{387742378329008606934824201506984053723129},$$

$$H_3(X) = X^2 - \frac{251163194917077269480553186223257197507193 2}{239193975073755701378477928 87} X + \frac{836715935834575482222921425639058196291548230115404060834200617 64}{348968140496107746241341781356285648350816 1}.$$

References

[1] A. Agashe, K. E. Lauter & R. 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*, Fields Inst. Commun., vol. 41, Amer. Math. Soc., 2004, p. 1–17.

[2] A. O. L. Atkin & F. Morain – "Elliptic curves and primality proving", *Math. Comp.* **61** (1993), no. 203, p. 29–68.

[3] D. G. Cantor – "On the analogue of the division polynomials for hyperelliptic curves", *J. reine angew. Math.* **447** (1994), p. 91–145.

[4] G. Cardona & J. Quer – "Field of moduli and field of definition for curves of genus 2", in *Computational aspects of algebraic curves*, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, p. 71–83.

[5] J. Chao, K. Matsuo, H. Kawashiro & S. Tsujii – "Construction of hyperelliptic curves with CM and its application to cryptosystems", in *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, Lecture Notes in Comput. Sci., vol. 1976, Springer, 2000, p. 259–273.

[6] H. Cohn & K. E. Lauter – "Generating genus 2 curves with complex multiplication", 2001, Microsoft Research Internal Technical Report.

[7] D. A. Cox – *Primes of the form* $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley & Sons Inc., 1989.

[8] D. Freeman & K. E. Lauter – "Computing endomorphism rings of Jacobians of genus 2 curves", in *Algebraic geometry and its applications, Proceedings of the first SAGA conference, 7-11 May 2007, Papeete* (J. Hirschfeld, J. Chaumine & R. Rolland, eds.), Number Theory and Its Applications, vol. 5, 2008, p. 29–66.

[9] P. Gaudry & R. Harley – "Counting points on hyperelliptic curves over finite fields", in *Algorithmic number theory (Leiden, 2000)*, Lecture Notes in Comput. Sci., vol. 1838, Springer, 2000, p. 313–332.

[10] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler & A. Weng – "The 2-adic CM method for genus 2 curves with application to cryptography", in *Advances in cryptology—ASIACRYPT 2006*, Lecture Notes in Comput. Sci., vol. 4284, Springer, 2006, p. 114–129.

[11] P. Gaudry & É. Schost – "Modular equations for hyperelliptic curves", *Math. Comp.* **74** (2005), no. 249, p. 429–454.

[12] E. Z. Goren – "On certain reduction problems concerning abelian surfaces", *Manuscripta Math.* **94** (1997), no. 1, p. 33–43.

[13] E. Z. Goren & K. E. Lauter – "Class invariants for quartic CM fields", *Ann. Inst. Fourier (Grenoble)* **57** (2007), no. 2, p. 457–480.

[14] E. W. Howe – "Principally polarized ordinary abelian varieties over finite fields", *Trans. Amer. Math. Soc.* **347** (1995), no. 7, p. 2361–2401.

[15] J.-i. Igusa – "Arithmetic variety of moduli for genus two", *Ann. of Math.* **72** (1960), p. 612–649.

[16] _____, "On Siegel modular forms of genus two", *Amer. J. Math.* **84** (1962), p. 175–200.

[17] _____, "Modular forms and projective invariants", *Amer. J. Math.* **89** (1967), p. 817–855.

[18] L.-C. Kappe & B. Warren – "An elementary test for the Galois group of a quartic polynomial", *Amer. Math. Monthly* **96** (1989), no. 2, p. 133–137.

[19] D. Kohel – "Endomorphism rings of elliptic curves over finite fields", Ph.D. Thesis, University of California, Berkeley, 1996.

[20] S. Lang – *Elliptic functions*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Amsterdam, 1973.

[21] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Math., vol. 264, Springer, 1972.

[22] J.-F. Mestre – "Construction de courbes de genre 2 à partir de leurs modules", in *Effective methods in algebraic geometry (Castiglioncello, 1990)*, Progr. Math., vol. 94, Birkhäuser, 1991, p. 313–334.

[23] J. S. Milne – "Abelian varieties", `http://www.jmilne.org/math/CourseNotes/math731.html`.

[24] F. Oort & K. Ueno – "Principally polarized abelian varieties of dimension two or three are Jacobian varieties", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **20** (1973), p. 377–381.

[25] F. Rodriguez-Villegas – "Explicit models of genus 2 curves with split CM", in *Algorithmic number theory (Leiden, 2000)*, Lecture Notes in Comput. Sci., vol. 1838, Springer, 2000, p. 505–513.

[26] G. Shimura – "On the zeta-function of an abelian variety with complex multiplication.", *Ann. of Math.* **94** (1971), p. 504–533.

[27] ———, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton Univ. Press, 1998.

[28] A.-M. Spallek – "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen", Ph.D. Thesis, Universität Gesamthochschule Essen, 1994.

[29] B. K. Spearman & K. S. Williams – "Relative integral bases for quartic fields over quadratic subfields", *Acta Math. Hungar.* **70** (1996), no. 3, p. 185–192.

[30] P. v. Wamelen – "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68** (1999), no. 225, p. 307–320.

[31] A. Weng – "Constructing hyperelliptic curves of genus 2 suitable for cryptography", *Math. Comp.* **72** (2003), no. 241, p. 435–458.

[32] ———, "Extensions and improvements for the CM method for genus two", in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun., vol. 41, Amer. Math. Soc., 2004, p. 379–389.

Kirsten Eisenträger, Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA. • *E-mail :* `eisentra@umich.edu`

Kristin Lauter, Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA. *E-mail :* `klauter@microsoft.com`