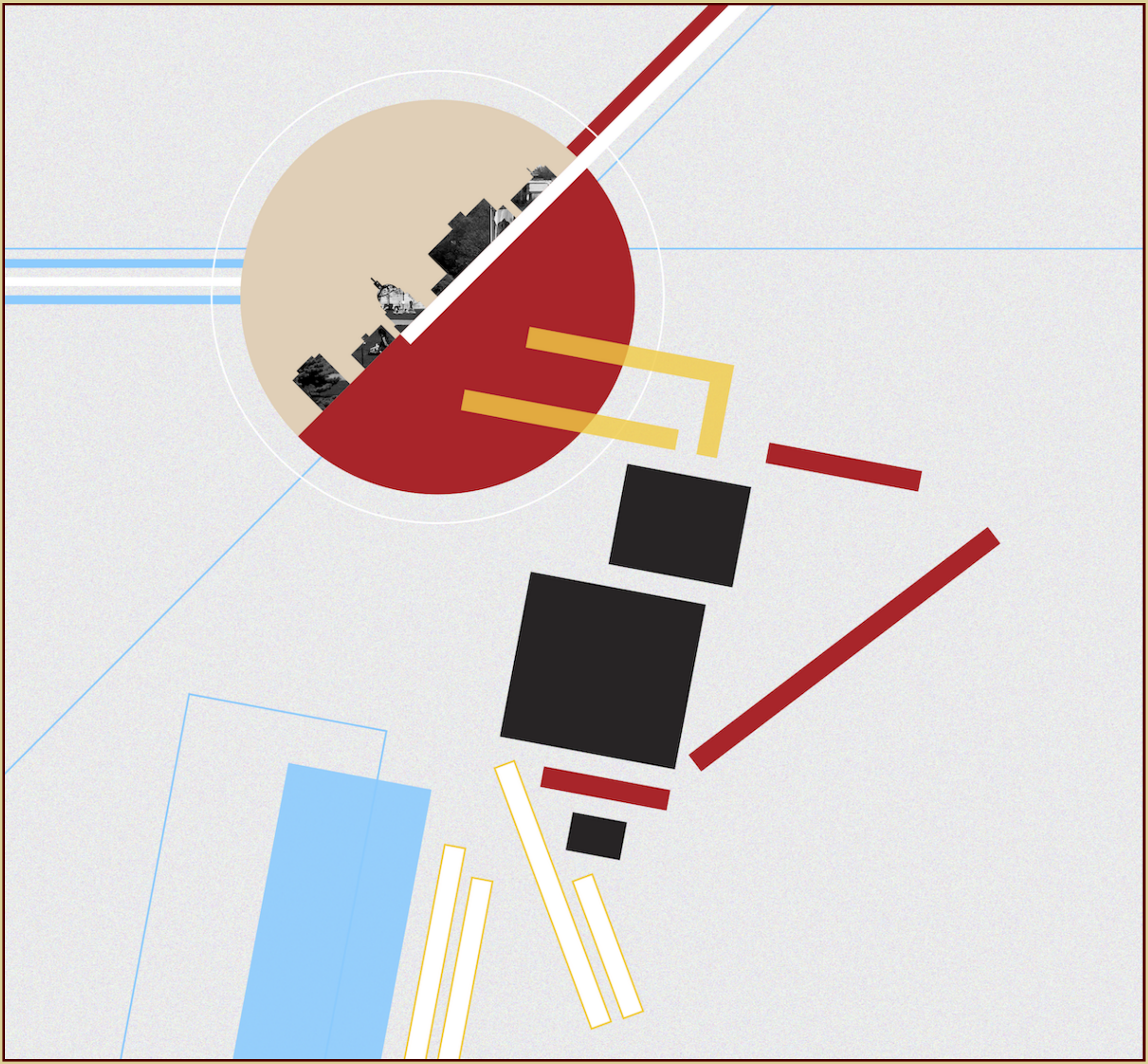
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Constructing Picard curves with complex multiplication using the Chinese remainder theorem

Sonny Arora and Kirsten Eisenträger



msp

THE OPEN BOOK SERIES 2 (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.21

Constructing Picard curves with complex multiplication using the Chinese remainder theorem

Sonny Arora and Kirsten Eisenträger

We give a new algorithm for constructing Picard curves over a finite field with a given endomorphism ring. This has important applications in cryptography since curves of genus 3 allow one to work over smaller fields than the elliptic curve case. For a sextic CM-field K containing the cube roots of unity, we define and compute certain class polynomials modulo small primes and then use the Chinese remainder theorem to construct the class polynomials over the rationals. We also give some examples.

1. Introduction

For cryptographic protocols whose security relies on the difficulty of the discrete log problem, one often wants to find a group whose order is divisible by a large prime. One option is the group of points of an elliptic curve over a finite field, or more generally, the group of points on the Jacobian of a curve over a finite field. Thus, we are interested in the problem of finding curves over finite fields whose Jacobian has a given number of points.

For elliptic curves, Atkin and Morain showed in [3] that one can use the theory of complex multiplication to solve this problem. The approach taken in [3] involves computing the Hilbert class polynomial with respect to an imaginary quadratic field by evaluating modular j-invariants at certain values. An alternative method to construct the Hilbert class polynomial, used in [9] and [1], is to compute the polynomial modulo several small primes and then reconstruct the polynomial using the Chinese remainder theorem. In the genus 2 case, analogous to the construction of the Hilbert class polynomial, one wishes to construct the so-called Igusa class polynomials. In this case, one can again use a Chinese remainder theorem approach to construct the Igusa class polynomials as shown in [11; 12].

If one wishes to construct genus 3 curves with a given number of points, less is known. Genus 3 curves fall into two classes: hyperelliptic curves and nonhyperelliptic plane quartics. One difficulty in

Arora was partially supported by National Science Foundation grants DMS-1056703 and CNS-1617802. Eisenträger was partially supported by National Science Foundation awards DMS-1056703 and CNS-1617802, and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0541.
MSC2010: primary 11G10, 11G15; secondary 14K22.
Keywords: Picard curves, Chinese remainder theorem, number theory, arithmetic geometry, constructing curves, genus 3.

the case of genus 3 curves is that there is no theory of invariants which works for all genus 3 curves. However, invariants do exist for the classes of hyperelliptic curves and nonhyperelliptic plane quartics separately. By making restrictions on the type of genus 3 curves considered, algorithms for constructing genus 3 curves with complex multiplication have been presented in [36; 23; 25; 4; 21]. All these papers take a complex analytic approach to constructing genus 3 curves similar to the method in [3]. The papers [36; 4] deal with constructing hyperelliptic genus 3 curves with complex multiplication. The paper [23] and its improvement [25] deal with constructing Picard curves with complex multiplication, while [21] deals with constructing plane quartics defined over $\mathbb{Q}$ with complex multiplication. Due to the numerous improvements to the Chinese remainder theorem approach in the elliptic curve case [5; 33], it is of interest to try to implement a Chinese remainder theorem approach for the construction of genus 3 curves. This is the aim of this paper.

As in [23], we will restrict our attention to Picard curves. These are genus 3 curves of the form $y^3 = f(x)$ where $\deg(f) = 4$ and f has no repeated roots over the algebraic closure. One advantage to using these curves is that it is very simple to generate representatives for all isomorphism classes of Picard curves over a finite field. Also, if K is a sextic CM-field that contains the cube roots of unity, then, by [23, Lemma 1], all simple, principally polarized abelian varieties of dimension 3 with complex multiplication by $\mathcal{O}_K$ arise as the Jacobians of Picard curves, so we can use Picard curves in a CRT approach.

Statement of theorem. Let K be a sextic CM-field containing the cube roots of unity. Fix a primitive CM-type Φ on the field K. Our first step will be to define suitable class polynomials for (K, Φ). For this we will require invariants for Picard curves.

We work with the set of invariants for Picard curves j_1, j_2, j_3 defined in [20]. They are discussed in more detail in Section 3.

We now wish to introduce class polynomials for Picard curves. Recall, the Hilbert class polynomial for an imaginary quadratic field K has as roots the j-invariants of elliptic curves with complex multiplication by the full ring of integers $\mathcal{O}_K$ of K. Analogous to this situation, we would like the class polynomials we define, for a sextic CM-field K containing the cube roots of unity, to have as roots the invariants of Picard curves with complex multiplication by $\mathcal{O}_K$. A complication that does not arise in the genus 1 case is that we will need to restrict to Picard curves whose Jacobian has a given primitive CM-type on K. In genus 2, a restriction on the CM-type for class polynomials was discussed in [26].

We would like our class polynomials to be defined over $\mathbb{Q}$. This will allow us to multiply by a large enough integer to clear denominators and hence use the Chinese remainder theorem on the resulting polynomials modulo various primes. For an abelian variety A of CM-type (K, Φ) and for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, A^σ is of type $(K, \sigma\Phi)$. Thus, we define class polynomials for $i = 1, \dots, 3$ as

$$H_i^\Phi := \prod (X - j_i(C)),$$

where the product runs over all isomorphism classes of Picard curves $C/\mathbb{C}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ of type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. These polynomials will be defined over $\mathbb{Q}$.

Should one want to reconstruct a Picard curve $C/\mathbb{C}$ such that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$ from the roots of the class polynomials, it is more convenient to work with a different set of class polynomials, introduced in [14] in the genus 2 setting. This is discussed more in Section 4.

We have the following theorem:

Theorem 1.1. *The following algorithm takes as input a sextic CM-field K containing the cube roots of unity and a primitive CM-type Φ on K. Assuming the bound B in Theorem 5.4 is known, the algorithm outputs the class polynomials H_i^{Φ}, where $i = 1, \dots, 3$, corresponding to the type (K, Φ).*

(i) *Construct a set of rational primes S which satisfy*
  (a) $2 \notin S$.
  (b) *Each $p \in S$ splits completely in K.*
  (c) *Each $p \in S$ splits completely into principal ideals in K^*, the reflex field for the type (K, Φ).*
  (d) $\prod_{p \in S} p > B$ *where B is the bound in Theorem 5.4.*

(ii) *Form the class polynomials H_i^{Φ} modulo p for every $p \in S$. Let $H_{i,p} := H_i^{\Phi} \mod p$. Then*

$$H_{i,p} = \prod (X - j_i(C)),$$

where the product is over all $\overline{\mathbb{F}}_p$-isomorphism classes of Picard curves that arise as the reduction of a Picard curve over $\mathbb{C}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ of type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(iii) *Form the polynomials H_i^{Φ} from the $H_{i,p}$, $p \in S$, using the Chinese remainder theorem.*

We review background from the theory of complex multiplication in Section 2 and prove some results we will need. In Section 3 we review invariants of Picard curves. In Section 4, we discuss reducing class polynomials modulo primes. In Section 5 we show how to compute H_i^{Φ} modulo a prime p and we prove Theorem 1.1. Section 6 discusses the endomorphism ring computation, and in Section 7 we give some examples.

2. Results from complex multiplication

Definition 2.1 (CM-type). Let K be a CM-field of degree $2g$ and let Ω be an algebraically closed field of characteristic 0. Denote by $\mathrm{Hom}(K, \Omega) = \{\phi_1, \phi_2, \dots, \phi_{2g}\}$ the set of embeddings of K into Ω. Furthermore, let ρ denote the automorphism inducing complex conjugation on K. Then any subset of these embeddings Φ satisfying the disjoint union $\Phi \sqcup \rho \circ \Phi = \mathrm{Hom}(K, \Omega)$ is called a CM-type on K.

Injectivity of the reduction map.

Definition 2.2. Let A be an abelian variety over a field k with complex multiplication by the maximal order $\mathcal{O}_K$ in a CM-field K, and let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. A surjective homomorphism $\lambda_{\mathfrak{a}} : A \to A^{\mathfrak{a}}$, to an abelian variety $A^{\mathfrak{a}}$, is an $\mathfrak{a}$-multiplication if every homomorphism $a : A \to A$ with $a \in \mathfrak{a}$ factors through $\lambda_{\mathfrak{a}}$, and $\lambda_{\mathfrak{a}}$ is universal for this property, in the sense that, for every surjective homomorphism

$\lambda' : A \to A'$ with the same property, there is a homomorphism $\alpha : A' \to A^{\mathfrak{a}}$, necessarily unique, such that $\alpha \circ \lambda' = \lambda_{\mathfrak{a}}$.

For abelian varieties A and B defined over a number field and with good reduction modulo a prime $\mathfrak{P}$, the next proposition gives a condition under which A and B will be isomorphic provided that their reductions modulo $\mathfrak{P}$ are isomorphic. The fact that the conditions below are sufficient for an isomorphism to lift was given for dimension 2 in [11, Theorem 2]. Here we give a general proof of this fact.

Proposition 2.3. *Let (A, ι), (B, ι') be simple, abelian varieties of type (K, Φ) defined over a number field k. Furthermore, assume that $\mathfrak{P}$ is a prime of k such that A and B have good reduction modulo $\mathfrak{P}$ and denote by $\tilde{A}$ and $\tilde{B}$ their reductions modulo $\mathfrak{P}$, respectively. If $\tilde{A}$ and $\tilde{B}$ are simple with endomorphism ring isomorphic to $\mathcal{O}_K$ and $\gamma : \tilde{A} \to \tilde{B}$ is an isomorphism over $\overline{\mathbb{F}}_p$, then A and B are isomorphic over $\bar{k}$.*

Proof. As (A, ι), (B, ι') have the same type then, by [30, Chapter II, Proposition 16], they are isogenous via an $\mathfrak{a}$-multiplication, which we denote by $\lambda_{\mathfrak{a}}$. After possibly taking a field extension and picking a prime above $\mathfrak{P}$, we can assume that $\lambda_{\mathfrak{a}}$ and all endomorphisms are defined over k. The reduction $\tilde{\lambda}_{\mathfrak{a}}$ is also an $\mathfrak{a}$-multiplication [28, Proposition 7.30]. Define an embedding $\tilde{\iota} : \mathcal{O}_K \to \mathrm{End}(\tilde{A})$ by $\tilde{\iota}(a) = \widetilde{\iota(a)}$. This map is an isomorphism. Let $a \in \mathcal{O}_K$ be such that $\tilde{\iota}(a) = \gamma^{-1} \circ \tilde{\lambda}_{\mathfrak{a}} \in \mathrm{End}(\tilde{A})$. As $\tilde{\iota}(a)$ factors through $\tilde{\lambda}_{\mathfrak{a}}$, $a \in \mathfrak{a}$ by [28, Corollary 7.24]. Also, $\iota(a)$ must factor through the $\mathfrak{a}$-multiplication, $\lambda_{\mathfrak{a}}$, that is, $\iota(a) = \gamma_1 \circ \lambda_{\mathfrak{a}}$ for γ_1 some isogeny from B to A.

Reducing modulo $\mathfrak{P}$, $\tilde{\iota}(a) = \tilde{\gamma}_1 \circ \tilde{\lambda}_{\mathfrak{a}}$. As $\lambda_{\mathfrak{a}}$ is surjective, this implies $\gamma^{-1} = \tilde{\gamma}_1$. Similarly, we can find a γ_2 such that $\tilde{\gamma}_2 = \gamma$. Then $\tilde{\gamma}_1 \circ \tilde{\gamma}_2 = \gamma^{-1} \circ \gamma = \mathrm{id}$. As the reduction map is injective, $\gamma_1 \circ \gamma_2 = \mathrm{id}$ and $\gamma_2 \circ \gamma_1 = \mathrm{id}$, thus A and B are isomorphic. □

The congruence relation. Let $(A, \iota)/\mathbb{C}$ be of type (K, Φ) with $\mathrm{End}(A) \cong \mathcal{O}_K$. Denote by (K^*, Φ^*) the reflex of (K, Φ). Let k be a field of definition for (A, ι). As the Hilbert class field H of K^* is a field of definition for (A, ι) (see [15, Proposition 2.1]), we may assume that $k \subseteq H$. Take L to be a Galois extension of $\mathbb{Q}$ containing the field of definition k and the field K. Recall k contains K^* by [24, Chapter III, Theorem 1.1]. Let $\mathfrak{P}$ be a prime of k at which A has good reduction. Let $\mathfrak{P}_{K^*}$ be the prime of K^* below $\mathfrak{P}$. Pick a prime $\mathfrak{P}_L$ of L above $\mathfrak{P}$ and write Φ_L^{-1} for the set of elements ψ of $\mathrm{Gal}(L/\mathbb{Q})$ such that $(\psi^{-1})_{|K} \in \Phi$.

Let $\pi \in \mathcal{O}_K$ be such that $\tilde{\iota}(\pi)$ is the $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{P})$-th power Frobenius on the reduction $\tilde{A}$. In Section 5 we will use the following proposition, which is an easy consequence of the Shimura–Taniyama congruence relation, to obtain a bijection between abelian varieties with CM by $\mathcal{O}_K$ of type Φ and abelian varieties over a finite field satisfying certain properties.

Proposition 2.4. *Assume that p splits completely in K and splits completely into principal ideals in K^*. Also, let M be the Galois closure of the compositum of K and K^* and let $\mathfrak{P}_M$ be a prime above $\mathfrak{P}_{K^*}$. Write Φ_M^{-1} for the set of elements γ of* $\mathrm{Gal}(M/\mathbb{Q})$ *such that $(\gamma^{-1})_{|K} \in \Phi$. Then $\pi \mathcal{O}_M = \prod_{\gamma \in \Phi_M^{-1}} (\mathfrak{P}_M)^{\gamma}$.*

Proof. As p splits completely into principal ideals in K^*, p splits completely in the Hilbert class field H of K^*. Thus, as mentioned above, p splits completely in the field of definition k. Therefore, $f(\mathfrak{P}_L/\mathfrak{P}) = 1$, and by [24, Chapter 3, Theorem 3.3] we obtain

$$\pi \mathcal{O}_L = \prod\nolimits_{\psi \in \Phi_L^{-1}} \mathfrak{P}_L^{\psi} \mathcal{O}_L.$$

Using the splitting conditions on p and intersecting with $\mathcal{O}_M$ on both sides, we get the desired result. □

Thus the CM-type determines the ideal generated by Frobenius. We will also need a version of this statement over $\mathbb{Q}_p$. Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Let

$$H_w = \{\phi \in \mathrm{Hom}(K, \overline{\mathbb{Q}}_p) : \ \phi \text{ factors through } K \to K_w\},$$

where K_w is the completion of K at the place w.

Proposition 2.5. *Let (A, ι) be an abelian variety with CM by the full ring of integers $\mathcal{O}_K$ and of CM-type Γ. Moreover, assume (A, ι) has a model over the p-adic integers $\mathbb{Z}_p$. If p splits completely in K, $\Gamma = \{\phi : \phi \in H_v, \ \text{where } v \mid \pi\mathcal{O}_K\}$.*

Proof. By [34, Lemme 5], $v(\pi)/v(q) = Card(\Gamma \cap H_v)/[K_v : \mathbb{Q}_p]$. If p splits completely in K, then $[K_v : \mathbb{Q}_p] = 1$ for all $v \mid p$ and $q = p$. This gives $v(\pi) = Card(\Gamma \cap H_v)$.

Also, as p splits completely in K, there is only one embedding $K \to K_v$ for every $v \mid p$. Thus $Card(H_v) = 0$ or 1, and $Card(\Gamma \cap H_v) = 1$ if and only if $v(\pi) = 1$. □

3. Invariants of Picard curves

In this section, we discuss invariants for Picard curves. Recall, if $y^3 = f(x)$ where $\deg(f) = 4$ and f has no repeated roots over the algebraic closure, then this defines a smooth curve known as a *Picard curve*. Assume L is a field of characteristic not 2 or 3, and let C be a Picard curve over L. We can express the curve C in the form $y^3 = x^4 + g_2x^2 + g_3x + g_4$. This is called the *normal form* of the curve [18, Appendix 1, Definition 7.6].

As in [20, Section 1], we define the following three invariants for a Picard curve in normal form as $j_1 := g_2^3/g_3^2, \ j_2 := g_2g_4/g_3^2, \ j_3 := g_4^3/g_3^4$.

We can write down a model for the curve with given invariants as follows:

Case 1: If $j_1 \neq 0$, then $C : y^3 = x^4 + j_1x^2 + j_1x + j_1j_2$.

Case 2: If $j_1 = 0$, $j_3 \neq 0$, then $C : y^3 = x^4 + j_3^2x + j_3^3$.

Case 3: If $j_1 = 0$, $j_2 = 0$, $j_3 = 0$, then $C : y^3 = x^4 + x$.

If $g_3 = 0$, then C is a double cover of an elliptic curve (see [20, Lemma 2.1 and Theorem 2.4]). Thus the invariants for a Picard curve C whose Jacobian is simple are always defined. This gives us the following proposition.

Proposition 3.1. *Let C be a Picard curve over a field L of characteristic not* 2 *or* 3 *with* $\mathrm{Jac}(C)$ *simple. Assume that the three invariants $j_i(C)$ are defined over a subfield k of L. Then C has a model as a Picard curve over k.*

Goren and Lauter showed that for genus 2 curves which have CM by a given primitive, quartic, CM-field K one can bound the primes occurring in the denominators of the Igusa class polynomials in terms of a value depending on K [16]. They obtain this bound by relating the primes occurring in the denominators to primes of bad reduction of the curves. For genus 3 curves with CM by a sextic CM-field K, a bound on the primes of bad reduction in terms of a value depending on K was obtained in [8; 22]. A bound on the primes occurring in the denominators of the above invariants of Picard curves was obtained in [20].

We will need the following condition for Picard curves.

Proposition 3.2. *Let $K = \mathbb{Q}(\mu)$ be a sextic CM-field, Φ be a primitive CM-type on K and p be a rational prime that splits completely in K. Let C be a genus 3 curve defined over a number field M with CM by the maximal order $\mathcal{O}_K$ of K and with type Φ. Let $\mathfrak{P}$ be a prime of M above p. Then C has potential good reduction at $\mathfrak{P}$. Moreover, if C is a Picard curve then $v_{\mathfrak{P}}(j_i(C)) \geq 0$ for all invariants j_i.*

Proof. Assume C has geometrically bad reduction modulo a prime $\mathfrak{P}$ of M above the rational prime p. After possibly extending M, we may assume that C has a stable model over M and $\mathrm{Jac}(C)$ has good reduction over M. The stable reduction $\tilde{C}$ has at least two irreducible components [8, Proposition 4.2]. $\widetilde{\mathrm{Jac}(C)}$ is isomorphic as a polarized abelian variety to the product of the Jacobians of the irreducible components of $\tilde{C}$. That is, $\widetilde{\mathrm{Jac}(C)}$ is isomorphic as a principally polarized abelian variety to $E \times A$ [8, Corollary 4.3], where E is an elliptic curve and A is a two-dimensional principally polarized abelian variety. However, as p splits completely in K, the reduction modulo $\mathfrak{P}$ of $\mathrm{Jac}(C)$ must be simple with CM by K by [30, Chapter 3, Theorem 2]. By [32, Theorem 1.2] $\widetilde{\mathrm{Jac}(C)}$ is ordinary, so $\mathrm{End}(\widetilde{\mathrm{Jac}(C)}) \otimes \mathbb{Q}$ is unchanged after base extension by [35, Theorem 7.2]. Therefore $\widetilde{\mathrm{Jac}(C)}$ is geometrically simple as the endomorphism ring tensored with $\mathbb{Q}$ is a field. This is a contradiction, so C must have potential good reduction.

Now assume that C is a Picard curve and that $v_{\mathfrak{P}}(j_i(C)) < 0$ for some j_i. After possibly extending M, we may assume that $\mathrm{Jac}(C)$ has good reduction modulo $\mathfrak{P}$. Then the reduction of $\mathrm{Jac}(C)$ modulo $\mathfrak{P}$ has two nontrivial abelian subvarieties by [20, Lemma 2.1]. However, as p splits completely in K, we again obtain a contradiction. □

Remark 3.3. It was pointed out to the authors by some of the anonymous referees and by Marco Streng that a condition similar to the above proposition was given in [21, Proposition 4.1] when the field $K/\mathbb{Q}$ is cyclic Galois.

Remark 3.4. To generate representatives for all distinct isomorphism classes, we use the invariants described in [23, Section 4]. To see that this enumerates all isomorphism classes of Picard curves with no repetitions, see [18, Appendix 1, Section 7.5].

4. Reduction of class polynomials

Fix a sextic CM-field K containing the cube roots of unity and a primitive CM-type Φ on K. In the introduction we defined class polynomials H_i^{Φ} for $i = 1, \ldots, 3$,

$$H_i^{\Phi} := \prod (X - j_i(C)),$$

where the product runs over all isomorphism classes of Picard curves defined over $\mathbb{C}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ and of type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Remark 4.1. If one wants to use the class polynomials above to construct Picard curves over $\mathbb{C}$ with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$, then one needs to match up the roots of the three polynomials to obtain a triple of roots (j_1, j_2, j_3) that corresponds to such a curve. In genus 2, alternate class polynomials were proposed based on Lagrange interpolation that prescribe which roots of the second and third Igusa class polynomials to choose once the first has been chosen [14, Section 3]. These polynomials only work if the first Igusa class polynomial has simple roots. For a discussion of resolving this issue in genus 2 see [31, Chapter III, Section 5].

We will show that under suitable restrictions on the prime p, the reduction modulo p of these polynomials H_i^Φ is

$$H_{i,p} := \prod (X - j_i(C)),$$

where the product runs over all $\overline{\mathbb{F}}_p$-isomorphism classes of Picard curves C which arise as the reduction of Picard curves over $\mathbb{C}$ that have complex multiplication by $\mathcal{O}_K$ and type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

First we describe when a principally polarized abelian variety is the Jacobian of a Picard curve.

In the following, whenever we assume that a field F contains the cube roots of unity, it is also implied that F does not have characteristic 3.

Lemma 4.2. *Let $(A, \mathcal{C})$ be a simple, principally polarized abelian variety of dimension 3 over a perfect field H which contains the cube roots of unity. In addition, assume $(A, \mathcal{C})$ has complex multiplication by K with $\mathbb{Q}(\zeta_3) \subset K$. Then $(A, \mathcal{C})$ is geometrically the Jacobian of a Picard curve C which has a model over H.*

Proof. By [23, Lemma 1], $(A, \mathcal{C})$ is the Jacobian of a Picard curve C after we base change to a finite extension L of H. After possibly another finite extension, we may assume L is Galois over H. Let $\sigma \in \mathrm{Gal}(L/H)$, then $\mathrm{Jac}(C^\sigma) \cong_L \mathrm{Jac}(C)^\sigma$. As $\mathrm{Jac}(C)$ has a model over H, $\mathrm{Jac}(C^\sigma) \cong_L \mathrm{Jac}(C)$.

Hence by Torelli's theorem, $C \cong_L C^\sigma$. So $j_i(C) = j_i(C^\sigma) = j_i(C)^\sigma$, $i = 1, \dots, 3$. Therefore the invariants $j_i(C)$ are defined over H. As the invariants $j_i(C)$ are defined over H, Proposition 3.1 implies that C has a model over H. □

Before we discuss reductions of our class polynomials, we need the following.

Proposition 4.3. *$H_1^\Phi, H_2^\Phi, H_3^\Phi$ are polynomials defined over $\mathbb{Q}$.*

Proof. Every abelian variety with CM by K has a model over a number field. Thus, by [29, Theorem 4], the curve C is also defined over a number field. So if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is an automorphism, then the tuple of invariants $j_i(C)^\sigma$ corresponds to the curve C^σ. But if $\mathrm{Jac}(C)$ has CM-type (K, Φ) under some embedding $\iota : K \hookrightarrow \mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q}$, then $\mathrm{Jac}(C^\sigma)$ has CM-type $(K, \sigma\Phi)$ by [24, Chapter 3, Theorem 1.2]. The number of roots of the H_i^Φ is finite as there are only finitely many principally polarized abelian varieties with endomorphism ring isomorphic to $\mathcal{O}_K$ of type $\sigma\Phi$ [24, Chapter 3, Corollary 2.7], so the H_i^Φ are polynomials defined over $\mathbb{Q}$. □

We will use the abbreviation p.p.a.v. for a principally polarized abelian variety. For a CM-field K of degree $2g$ over $\mathbb{Q}$, let

$$\mathrm{CM}_{K,\Phi} = \{\mathbb{C}\text{-isomorphism classes of simple p.p.a.v. with CM by } \mathcal{O}_K \text{ of type } \Phi\}.$$

The abelian varieties in this set are of dimension g. By [15, Proposition 2.1], every p.p.a.v. $(A, \mathcal{C})$ representing an isomorphism class in $\mathrm{CM}_{K,\Phi}$ has a model over the Hilbert class field H of the reflex field K^* which has good reduction modulo any prime $\mathfrak{P}$ of H. By [28, Chapter II, Proposition 6.7], the reduction of the polarization $\mathcal{C}$ is a polarization on the reduced variety $\tilde{A}$. If p splits completely into principal ideals in K^* then p splits completely into principal ideals in H. Thus, the reduction $(A_{\mathfrak{P}}, \mathcal{C}_{\mathfrak{P}})$ of $(A, \mathcal{C})$ modulo $\mathfrak{P}$ has a model over $\mathbb{F}_p$. Denote by $\widetilde{\mathrm{CM}}_{K,\Phi}$ the set of $\overline{\mathbb{F}}_p$-isomorphism classes occurring in this way. That is,

$$\widetilde{\mathrm{CM}}_{K,\Phi} = \{\overline{\mathbb{F}}_p\text{-isomorphism classes of p.p.a.v.'s } (A_{\mathfrak{P}}, \mathcal{C}_{\mathfrak{P}})/\mathbb{F}_p \mid (A, \mathcal{C}) \in \mathrm{CM}_{K,\Phi}\}.$$

Proposition 4.4. *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If $\Phi\gamma = \sigma\Phi$ for some $\gamma \in \mathrm{Aut}(K/\mathbb{Q})$, then $CM_{K,\Phi}$ and $CM_{K,\sigma\Phi}$ are equal. Otherwise, $CM_{K,\Phi}$ and $CM_{K,\sigma\Phi}$ are disjoint.*

Proof. For the first statement see [31, page 22]. The second statement follows from [31, Chapter I, Lemma 5.6]. □

For a sextic CM-field K containing the cube roots of unity, define

$$\mathcal{C}^{\Phi} := \{\text{Picard curves } C \text{ over } \mathbb{C} \mid \mathrm{Jac}(C) \in \mathrm{CM}_{K,\Phi}\}/\text{isomorphism over } \mathbb{C},$$

and

$$\widetilde{\mathcal{C}^{\Phi}} := \{\text{Picard curves } C \text{ over } \mathbb{F}_p \mid \mathrm{Jac}(C) \in \widetilde{\mathrm{CM}}_{K,\Phi}\}/\text{isomorphism over } \overline{\mathbb{F}}_p.$$

Let $p > 3$ be a rational prime that splits completely in K and splits completely into principal ideals in K^*.

Proposition 4.5. *The reduction of the polynomials H_i^{Φ} modulo a prime satisfying the above conditions gives $H_i^{\Phi} \bmod p \equiv \prod(X - j_i(C))$, where the product is over all C such that C is in $\widetilde{\mathcal{C}^{\sigma\Phi}}$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Proof. As p splits completely into principal ideals in K^*, the reflex field for (K, Φ), it splits completely in H. Let $\mathfrak{P}$ be a prime of H above p. By [15, Proposition 2.1], $\mathrm{Jac}(C)$ is defined over H for any curve C in $\mathcal{C}^{\Phi}$. Then C itself also has a model over H by Lemma 4.2. C has potential good reduction by Proposition 3.2, so let L be a finite extension over which C obtains good reduction. Furthermore, let $\mathfrak{P}_L$ be a prime above $\mathfrak{P}$. Thus, the reduction $C_{\mathfrak{P}_L}$ of C modulo $\mathfrak{P}_L$ will be defined over a finite extension of $\mathbb{F}_p$. However, as the invariants of C belong to H, the invariants of $C_{\mathfrak{P}_L}$ belong to $\mathbb{F}_p$ so $C_{\mathfrak{P}_L}$ has a model over $\mathbb{F}_p$. Thus, we get a map from $\mathcal{C}^{\Phi}$ to $\widetilde{\mathcal{C}^{\Phi}}$. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let K_σ^* be the reflex field for the type $(K, \sigma\Phi)$. One can check that the reflex fields K^* and K_σ^* are isomorphic over $\mathbb{Q}$. Therefore, p splits completely into principal ideals in the reflex field of K_σ^*, so we also get a map from $\mathcal{C}^{\sigma\Phi}$ to $\widetilde{\mathcal{C}^{\sigma\Phi}}$ induced by reduction modulo $\mathfrak{P}_L$. It remains to show that the reduction map induces a bijection. Taking Jacobians of elements in $\mathcal{C}^{\Phi}$ and $\widetilde{\mathcal{C}^{\Phi}}$ gives bijective maps into $\mathrm{CM}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\Phi}$, respectively.

The map $\mathrm{CM}_{K,\Phi}$ to $\widetilde{\mathrm{CM}}_{K,\Phi}$ induced by reduction modulo $\mathfrak{P}$ is injective by Proposition 5.2. By definition, the map from $\mathrm{CM}_{K,\Phi}$ to $\widetilde{\mathrm{CM}}_{K,\Phi}$ is surjective, so it follows that $\mathcal{C}^{\Phi}$ is in bijection with the set $\widetilde{\mathcal{C}^{\Phi}}$ under the reduction map. The sets $\mathrm{CM}_{K,\Phi}$ and $\mathrm{CM}_{K,\sigma\Phi}$ are either equal or distinct by Proposition 4.4. The elements in $\widetilde{\mathrm{CM}}_{K,\Phi}$ are simple with CM by $\mathcal{O}_K$ by Proposition 5.1. Thus, the sets $\widetilde{\mathrm{CM}}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\sigma\Phi}$ are equal if and only if $\mathrm{CM}_{K,\Phi}$ and $\mathrm{CM}_{K,\sigma\Phi}$ are equal by Proposition 2.3. Therefore, bijectivity of the map from $\mathcal{C}^{\Phi}$ to $\widetilde{\mathcal{C}^{\Phi}}$ suffices to prove the proposition. □

5. Computing H_i^{Φ} modulo p

Let (K, Φ) be a primitive CM-type. Denote by (K^*, Φ^*) the reflex of (K, Φ). Let H be the Hilbert class field of K^* and M the normal closure of the compositum of K and K^*. Let L be the Galois closure of the compositum of H and M over $\mathbb{Q}$. Take p to be a rational prime which splits completely into principal ideals in K^* and splits completely in K. Denote by $\mathfrak{P}$ a prime of H above p, by $\mathfrak{P}_L$ a prime of L above $\mathfrak{P}$ and by $\mathfrak{P}_M$ a prime of M below $\mathfrak{P}_L$. Denote by Φ_M^{-1} the set of elements ψ_i of $\mathrm{Gal}(M/\mathbb{Q})$ such that $(\psi_i^{-1})_{|K} \in \Phi$.

An equivalent definition of $\widetilde{\mathrm{CM}}_{K,\Phi}$. In this subsection, we give an equivalent definition of $\widetilde{\mathrm{CM}}_{K,\Phi}$ in terms of a condition on the Frobenius of the abelian varieties in $\widetilde{\mathrm{CM}}_{K,\Phi}$. This new definition is more suitable for computations. In particular, we will use it in computing the set $\widetilde{\mathcal{C}^{\Phi}}$ which occurs in the description of the class polynomials H_i^{Φ} modulo p in Proposition 4.5. For a CM-field K with $[K : \mathbb{Q}] = 2g$, recall the definitions of $\mathrm{CM}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\Phi}$ from Section 4.

We will now define a set $\mathrm{CM}_{K,\Phi}^{\mathrm{Fr}}$ which we will show is equal to the set $\widetilde{\mathrm{CM}}_{K,\Phi}$. The main tool that allows us to give this equivalent description will be the Shimura–Taniyama congruence relation, specifically the statement in Proposition 2.4, which relates the CM-type of an abelian variety defined over a number field with CM to the ideal generated by Frobenius of the reduction of the abelian variety modulo $\mathfrak{P}$. In genus 2, this idea was used in [26] to describe the set we refer to as $\widetilde{\mathrm{CM}}_{K,\Phi}$.

With notation as above, denote by $\mathrm{CM}_{K,\Phi}^{\mathrm{Fr}}$ the set of all $\overline{\mathbb{F}}_p$-isomorphism classes of ordinary, simple, principally polarized abelian varieties $(A, \mathcal{C})$ of dimension g defined over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ satisfying the following condition: For $(A, \mathcal{C})$ a representative of an $\overline{\mathbb{F}}_p$ class as above, there exists an embedding ι of $K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ such that, under this embedding, the element π for which $\iota(\pi)$ is the Frobenius endomorphism on A satisfies

$$\pi \mathcal{O}_M = \prod\nolimits_{\phi \in \Phi_M^{-1}} \mathfrak{P}_M^{\phi}. \tag{5-1}$$

Recall, in the beginning of the section, we fixed a prime $\mathfrak{P}_L$ of L above the prime $\mathfrak{P}$ of H and define $\mathfrak{P}_M = \mathfrak{P}_L \cap M$. One can easily check that $\widetilde{\mathrm{CM}}_{K,\Phi}$ does not depend on the choice of $\mathfrak{P}_L$ above $\mathfrak{P}$. We now wish to show that the sets $\mathrm{CM}_{K,\Phi}^{\mathrm{Fr}}$ and $\widetilde{\mathrm{CM}}_{K,\Phi}$ are equal. First we show the following:

Proposition 5.1. *Every element in $\widetilde{\mathrm{CM}}_{K,\Phi}$ is ordinary and geometrically simple with endomorphism ring isomorphic to $\mathcal{O}_K$.*

Proof. Let $(A, \mathcal{C})$ be a representative of a class in $\mathrm{CM}_{K,\Phi}$ such that it has good reduction modulo $\mathfrak{P}$ as above. Let $A_{\mathfrak{P}}$ be the reduction of A modulo $\mathfrak{P}$. The reduction map gives an inclusion $\mathrm{End}(A) \hookrightarrow \mathrm{End}(A_{\mathfrak{P}})$ [24, Theorem 3.2], thus, $\mathcal{O}_K$ embeds into $\mathrm{End}(A_{\mathfrak{P}})$. By [30, Chapter 3, Theorem 2], the abelian variety $A_{\mathfrak{P}}$ is simple and $\mathrm{End}(A_{\mathfrak{P}}) = \mathcal{O}_K$. Also, $A_{\mathfrak{P}}$ is ordinary by [32, Theorem 1.2]. Thus, $\mathrm{End}(A_{\mathfrak{P}}) \otimes \mathbb{Q}$ is unchanged after base extension by [35, Theorem 7.2]. Hence $A_{\mathfrak{P}}$ is geometrically simple as the endomorphism ring tensored with $\mathbb{Q}$ is a field. □

The following two results are a generalization to arbitrary dimension of the dimension 2 case treated in [11, Theorem 2].

Proposition 5.2. *The reduction map $CM_{K,\Phi} \to \widetilde{CM}_{K,\Phi}$ is injective.*

Proof. Every element in $\widetilde{\mathrm{CM}}_{K,\Phi}$ is simple with CM by $\mathcal{O}_K$ by Proposition 5.1. Thus, the proposition follows from applying Proposition 2.3. □

Theorem 5.3. *With notation as above, the set $\widetilde{CM}_{K,\Phi}$ is equal to the set $CM^{Fr}_{K,\Phi}$.*

Proof. We first show that $\widetilde{\mathrm{CM}}_{K,\Phi} \subset \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. Let $(A, \mathcal{C})$ be a representative of a class in $\widetilde{\mathrm{CM}}_{K,\Phi}$. By Proposition 5.1, A is ordinary and geometrically simple with $\mathrm{End}(A) \cong \mathcal{O}_K$. As we remarked above, p splits completely into principal ideals in K^*, so the Frobenius of A satisfies (5-1) by Proposition 2.4. Hence $\tilde{A} \in \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. This shows $\widetilde{\mathrm{CM}}_{K,\Phi} \subset \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. It remains to show the reverse inclusion.

To do this, we will show that the two sets have the same cardinality. Both sets are finite as there are only finitely many isomorphism classes of principally polarized abelian varieties defined over $\mathbb{F}_p$. We know from the previous proposition that $\mathrm{CM}_{K,\Phi} \to \widetilde{\mathrm{CM}}_{K,\Phi}$ is an injection. Thus, we have the inequality of cardinalities: $|\mathrm{CM}_{K,\Phi}| \le |\widetilde{\mathrm{CM}}_{K,\Phi}| \le |\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}|$.

It suffices to show $|\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}| \le |\mathrm{CM}_{K,\Phi}|$. Therefore, we will show that there is an injective map from $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ into $\mathrm{CM}_{K,\Phi}$. We define the map as follows: Let $(A_0, \mathcal{C}_0)$ be an abelian variety representing a class in $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. Since A_0 is ordinary, we can consider its Serre–Tate canonical lift [27, pages 172-173, Theorem 3.3] to $\mathbb{Z}_p$ which we will call $(A, \mathcal{C})$.

As $(A_0, \mathcal{C}_0) \in \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ we have $\pi\mathcal{O}_M = \prod_{\phi_\alpha \in \Phi_M^{-1}} (\mathfrak{P}_M)^{\phi_\alpha}$. Let $\{\psi_w\}$ be the set of all embeddings of M into $\overline{\mathbb{Q}}_p$ induced by completion at a prime $\mathfrak{P}_w$ for $\mathfrak{P}_w \mid \pi\mathcal{O}_M$. By Proposition 2.5, the embeddings induced by completion at primes occurring in the decomposition of the ideal generated by π give the CM-type of A. Under some embedding $\rho : \mathbb{Q}_p \hookrightarrow \mathbb{C}$, we can verify that $\rho(A)$ has type $(K, \sigma\Phi)$ for some $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$. By [37, Theorem 7], modifying ρ by an automorphism of $\mathbb{C}$, we can arrange that $\rho(A)$ has CM-type (K, Φ). As the choice of ρ does not depend on A, this gives us the injection from $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ to $\mathrm{CM}_{K,\Phi}$. Hence $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi} = \widetilde{\mathrm{CM}}_{K,\Phi}$. □

Correctness proof for the main algorithm. We must now show that the Chinese remainder theorem may be used to reconstruct the class polynomials from sufficiently many of the $H_{i,p}$. This is accomplished by Theorem 5.4 whose proof is identical to that of [11, Theorem 3]:

Theorem 5.4. *Let M be the least common multiple of the denominators of the class polynomials and let N be the maximum absolute value of the coefficients of the class polynomials. Let $B = 2NM$. Then if*

S is a set of primes satisfying the conditions in Theorem 1.1, we can use the Chinese remainder theorem on the polynomials $\{H_{i,p}\}_{p\in S}$, with i from 1 to 3, to reconstruct the polynomials H_i^{Φ}.

Remark 5.5. A definition of class polynomials for Picard curves and a bound on the primes occurring in the denominators are given in [22, Theorem 1.3], and the class polynomials we define divide them. In genus 2, bounds on the denominators of the Igusa class polynomials were obtained in [17].

Proof of Theorem 1.1. Using Proposition 4.5, we see that $H_{i,p} := \prod(X - j_i(C))$, where the product runs over representatives for elements in $\widetilde{\mathcal{C}^{\sigma\Phi}}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We can enumerate all $\overline{\mathbb{F}}_p$ isomorphism classes of Picard curves defined over $\mathbb{F}_p$ using the invariants discussed in Remark 3.4. We can check whether a curve is in $\widetilde{\mathcal{C}^{\Phi}}$ by checking whether $\mathrm{Jac}(C)$ is in $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ by Theorem 5.3. This involves checking that $\mathrm{Jac}(C)$ has complex multiplication by $\mathcal{O}_K$ which can be accomplished using the algorithm of Section 6. We then perform the CRT step using Theorem 5.4. □

6. Endomorphism ring computation

The algorithm of Theorem 1.1 requires us to check whether certain genus 3 curves C have complex multiplication by a sextic CM-field K. An algorithm for checking whether the Jacobian of an ordinary genus 2 curve (i.e., a curve whose Jacobian is ordinary) has complex multiplication by the full ring of integers of a primitive quartic CM-field K was presented, under certain restrictions on the field K, in [11]. Improvements to this algorithm were presented in [12] and [26]. We generalize these methods to the genus 3 case.

Theorem 6.1. *The following algorithm takes as input a sextic CM-field K and an ordinary genus 3 curve C over a field $\mathbb{F}_p$ where p splits completely in K. The algorithm outputs* **true** *if* $\mathrm{Jac}(C)$ *has endomorphism ring the full ring of integers $\mathcal{O}_K$ and* **false** *otherwise*:

(i) *Compute a list of all possible characteristic polynomials of Frobenius for ordinary, simple, abelian varieties with complex multiplication by K. Output* **false** *if the characteristic polynomial of* $\mathrm{Jac}(C)$ *is not in this list.*

(ii) *Compute a basis for $\mathcal{O}_K$.*

(iii) *For each element α of the basis in the previous step, use Proposition 6.2 to determine if it is an endomorphism. If it is not, output* **false**.

(iv) *Output* **true**.

The values for Frobenius in Step (i) satisfy $\pi\overline{\pi} = p$ with $\pi \in \mathcal{O}_K$, i.e., $N_{K/K^+}(\pi) = p$ where K^+ is the maximal totally real subfield of K. This relative norm equation can be used to find all such values of π. By the Honda–Tate theorem, every such π will arise as the Frobenius of some abelian variety A over $\mathbb{F}_p$. If the characteristic polynomial of π is irreducible, then A is simple and $\mathbb{Q}(\pi) \cong K$. If p does not divide the middle coefficient of the characteristic polynomial of Frobenius, then A is ordinary [19, Definition 3.1]. By [34, page 97, Exemple b], the endomorphism ring of A is an order in K.

Determining if an element is an endomorphism. Our approach in this subsection follows closely that of [12, Section 3] and [26, Section 4] for genus 2. We discuss some changes which are required for genus 3. To determine if $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$, we wish to check, for some $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\alpha_1, \dots, \alpha_6$, whether each α_i is an endomorphism. As $\mathbb{Z}[\pi]$ is an order in K, for every $\alpha \in \mathcal{O}_K$, we can write

$$\alpha = P_\alpha(\pi)/n := (a_0 + a_1\pi + \cdots + a_5\pi^5)/n \tag{6-1}$$

for some integer n. The next proposition lets us check if $\alpha \in \mathcal{O}_K$ is an endomorphism of $\mathrm{Jac}(C)$:

Proposition 6.2. *Let C be an ordinary curve of genus 3 over $\mathbb{F}_p$ with $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = K$, and suppose p splits completely in K. Let $\alpha = P_\alpha(\pi)/n \in \mathcal{O}_K$ with $n = \prod \ell_i^{e_i}$. Then α is an endomorphism of $\mathrm{Jac}(C)$ if and only if $P_\alpha(\pi)$ is zero on the $\ell_i^{e_i}$-torsion for $\ell_i \neq p$.*

Proof. By [12, Lemma 3.2], it suffices to check that each $P_\alpha(\pi)/\ell_i^{d_i}$ is an endomorphism. If ℓ_i is coprime to p, then by [11, Corollary 9], we can check whether $P_\alpha(\pi)/\ell_i^{d_i}$ is an endomorphism by determining if $P_\alpha(\pi)$ is zero on the $\ell_i^{d_i}$-torsion.

It remains to handle the case where $\ell_i = p$. For a group A, denote the p-primary part of A by A_p. Write $[\mathcal{O}_K : \mathbb{Z}[\pi]] = [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] \cdot [\mathbb{Z}[\pi, \bar{\pi}] : \mathbb{Z}[\pi]]$. It is not hard to see that $[\mathbb{Z}[\pi, \bar{\pi}] : \mathbb{Z}[\pi]]$ is a power of p (see [12, Corollary 3.6]). As p splits completely in K, one can show, $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$, thus $|(\mathcal{O}_K/\mathbb{Z}[\pi])_p| = |(\mathbb{Z}[\pi, \bar{\pi}]/\mathbb{Z}[\pi])_p|$. This follows from an argument similar to [12, Proposition 3.7].

But this implies for any $\beta \in \mathcal{O}_K$, if $p^k\beta \in \mathbb{Z}[\pi]$ then $\beta \in \mathbb{Z}[\pi, \bar{\pi}]$. Thus, any such element is an endomorphism. □

Computing the ℓ^d-torsion and arithmetic. The algorithm of Couveignes [10] shows how to compute the ℓ^d-torsion. Couveignes' method works for a very general class of curves. However, we instead use some algorithms specific to Picard curves. For a Picard curve C/k, where k is a finite field, Couveignes' method requires the ability to choose random points in $\mathrm{Jac}(C)(k)$. This is easy to do if we represent elements of $\mathrm{Jac}(C)(k)$ as formal sums of points on C. However, to do arithmetic on $\mathrm{Jac}(C)(k)$, it is easier to represent elements as ideals in the affine coordinate ring of C. Thus, we need to be able to switch between the two representations. First, we recall the following consequence of the Riemann–Roch theorem:

Proposition 6.3. *For C a Picard curve and P_∞ the point at infinity for the affine model described above, for any degree-0 divisor D there is a unique effective divisor E of minimal degree $0 \le m \le 3$ such that $E - mP_\infty$ is equivalent to D.*

Proof. As Picard curves are nonsingular with a k-rational point, the proof follows from [13, Theorem 1]. □

We will call the unique divisor above the reduced representation of D. So to find a random point in $\mathrm{Jac}(C)(k)$, we can just pick at most 3 random points on C.

A reduced divisor D for which all points in the effective part E lie in the same $\mathrm{Gal}(\bar{k}/k)$-orbit will be called an *irreducible* divisor. Every degree-0 divisor can be expressed as a sum of irreducible divisors.

We can also represent points on $\mathrm{Jac}(C)$ as elements of a particular class group. Denote the coordinate ring $k[x, y]/\langle y^3 - f(x)\rangle$ of C by R. By [13, Proposition 2], R is the integral closure of $k[x]$ in $k(C)$.

Given an irreducible divisor P we can associate to it a prime ideal $\mathfrak{P}$ of R. We can extend this to a map ρ from effective divisors to ideals of R as

$$\rho\Big(\sum n_i P_i\Big) := \prod \mathfrak{P}_i^{n_i},$$

where the P_i are irreducible divisors and the $\mathfrak{P}_i$ are the corresponding primes of R.

Proposition 6.4. *For C a Picard curve over k and R the coordinate ring of C described above, the map ρ induces an isomorphism* $\mathrm{Jac}(C)(k) \to \mathrm{Cl}(R)$, *where* $\mathrm{Cl}(R)$ *is the class group of R.*

Proof. This follows from applying [13, Proposition 3]. □

We refer to the image of a reduced divisor under the map ρ as a reduced ideal.

Proposition 6.5. *Given a reduced divisor D, there is an algorithm to find generators $u(x)$, $w(x, y)$ for the ideal $\rho(D)$. Moreover, given an ideal I of R in the form $I = \langle u(x), w(x, y)\rangle$, we can compute $\rho^{-1}(I)$.*

Proof. As a reduced divisor is a sum of irreducible divisors, it suffices to associate to an irreducible divisor Q the corresponding prime ideal. We can associate a prime ideal $\mathfrak{P}$ in R by first considering the polynomial $u = \prod(x - x_i)$, where the product is over all x-coordinates of points in Q. We then take a polynomial $w(x, y)$ such that the set of common roots of u, w is exactly the set of points of Q. If the x_i are all distinct, then we take the polynomial $w = y - v(x)$, where $v(x)$ is the polynomial interpolating the points in Q. If the roots of $u(x)$ are not distinct, then we can construct w in a way similar to the interpolation polynomial. In the case where there are two distinct x-coordinates x_1, x_2, let y_1 and y_2 be polynomials whose roots are the y-coordinates corresponding to x_1 and x_2, respectively. Then

$$w(x, y) := \frac{x - x_2}{x_1 - x_2} y_1(y) + \frac{x - x_1}{x_2 - x_1} y_2(y).$$

If there is only a single x-coordinate, then we can write $w(x, y) = \prod(y - y_i)$, where the y_i are the y-coordinates in the Galois orbit. The corresponding prime ideal in R is then the ideal generated by u and w.

We will now show how to explicitly find the inverse of ρ. Let $D = \prod \mathfrak{P}_i^{n_i}$ be the ideal decomposition of D. Write $\mathfrak{P}_i = \langle u(x), w(x, y)\rangle$. We can find the set of common zeroes of $\mathfrak{P}_i$ by finding all roots x_n of $u(x)$ and all roots $y_{n,m}$ of $w(x_n, y)$. Then the divisor $(\mathfrak{P}_i)$ equals $\sum(x_n, y_{n,m})$. Thus we have constructed the inverse of the map ρ on a prime divisor $\mathfrak{P}$. By linearity, we can explicitly find the inverse of any reduced ideal D. □

There are several algorithms which perform arithmetic on $\mathrm{Jac}(C)(k)$ using the representation of points on $\mathrm{Jac}(C)(k)$ as ideals in the class group, for example, [13; 2]. We will use the algorithm of [2] for the examples we compute. To add two elements P, Q of $\mathrm{Jac}(C)(k)$, one multiplies the corresponding ideals to get an ideal D. One then wishes to get a reduced ideal D', to have a unique representative for the point D. The algorithm of [2] gives a function g such that $D' = D + (g)$. The function g is necessary for the computation of the Weil pairing in the algorithm of Couveignes for computing torsion.

7. Examples

All examples were run on a computer with four Intel Xeon quad-core processors and 64 GB of RAM.

Let $K = K^+(\zeta_3)$, where K^+ is obtained by adjoining to $\mathbb{Q}$ a root of $x^3 - x^2 - 2x + 1$. We can verify that K is Galois with Galois group $\mathbb{Z}/6\mathbb{Z}$ and choose a primitive CM-type on K. All types on K are equivalent, so our choice does not matter. We count the expected degree of our class polynomials using [30, page 112, Note 3]. This is equivalent to counting the number of elements in the *polarized class group* (see [6]), for which there is a function in the AVIsogenies package [7]. We find that the degree of the class polynomials for K as above is 1. The first four primes satisfying the conditions of Theorem 1.1 are $13, 43, 97, 127$. For $p = 127$, our algorithm took 7 hours and 9 minutes of clock time and found one Picard curve in $\widetilde{\mathcal{C}^\Phi}$, that is, one Picard curve whose Jacobian is in $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$:

$$y^3 = x^4 + 75x^2 + 37x + 103.$$

The Picard curve $\mathbb{C}$ with CM by $\mathcal{O}_K$, for K as above, was computed in [23]. However, the authors of [23] could not verify that the curve they produce has CM by $\mathcal{O}_K$. Our output agrees with the result of their paper reduced modulo 127. Furthermore, assuming the curve they compute is correct, we get a bound as in Theorem 5.4 for the denominators and size of coefficients in the class polynomials H_i^Φ. In particular, $N = 2^{12}$ and $M = 7$ work for the values in Theorem 5.4. Using these values, we ran the CRT algorithm of Theorem 1.1 to construct the class polynomials H_i^Φ defined over $\mathbb{Q}$. The algorithm took 8 hours, 55 minutes to run. We only needed to reduce modulo the four primes $13, 43, 97, 127$. Our result agrees with the result of [23; 25]. Thus, our algorithm can compute the class polynomials H_i^Φ given that one can compute the bound in Theorem 5.4. If we compare the algorithms on the small example we computed above, the algorithm in [25] performs much faster; it was able to compute the class polynomials in seconds. However, since there are no known bounds, yet, on the denominators of the class polynomials, no complexity analysis has been done for our algorithm or the algorithms in [23; 25], so it is not clear how they would compare asymptotically.

Now let $K = K^+(\zeta_3)$, where K^+ is the field obtained by adjoining to $\mathbb{Q}$ a root of $x^3 + x^2 - 3x - 1$. This field is non-Galois, and the Galois group of the normal closure over $\mathbb{Q}$ is $S_3 \times \mathbb{Z}/2\mathbb{Z}$. We also pick a CM-type Φ on K. Our computations predicted that our class polynomials would have degree 3 using the polarized class group. We picked $p = 67$, which satisfies the conditions of Theorem 1.1. Our algorithm ran in 2 hours and 23 minutes, and we got 3 Picard curves over $\mathbb{F}_p$ whose Jacobians lie in $\mathrm{CM}^{\mathrm{Fr}}_{K,\sigma\Phi}$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\begin{aligned} y^3 &= x^4 + 8x^2 + 64x + 61, \\ y^3 &= x^4 + 62x^2 + 25x + 6, \\ y^3 &= x^4 + 54x + 54. \end{aligned}$$

Acknowledgements

The authors would like to thank Yuri Zarhin for helpful discussions. We thank the anonymous referees for several helpful suggestions. We thank Marco Streng for valuable feedback on an earlier version of this paper and for pointing out additional references.

References

[1] Amod Agashe, Kristin Lauter, and Ramarathnam Venkatesan, *Constructing elliptic curves with a known number of points over a prime field*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., no. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 1–17. MR 2075643

[2] Seigo Arita, *An addition algorithm in Jacobian of C_{ab} curves*, Discrete Appl. Math. **130** (2003), no. 1, 13–31. MR 2008402

[3] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), no. 203, 29–68. MR 1199989

[4] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent, *Constructing genus-3 hyperelliptic Jacobians with CM*, LMS J. Comput. Math. **19** (2016), suppl. A, 283–300. MR 3540961

[5] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter, *Computing Hilbert class polynomials*, Algorithmic number theory, Lecture Notes in Comput. Sci., no. 5011, Springer, 2008, pp. 282–295. MR 2467854

[6] Gaetan Bisson, *Computing endomorphism rings of abelian varieties of dimension two*, Math. Comp. **84** (2015), no. 294, 1977–1989. MR 3335900

[7] Gaetan Bisson, Robert Cosset, and Damien Robert, *AVIsogenies (abelian varieties and isogenies)*, Magma package for explicit isogenies between abelian varieties, 2010.

[8] Irene Bouw, Jenny Cooley, Kristin Lauter, Elisa Lorenzo García, Michelle Manes, Rachel Newton, and Ekin Ozman, *Bad reduction of genus three curves with complex multiplication*, Women in numbers Europe, Assoc. Women Math. Ser., no. 2, Springer, 2015, pp. 109–151. MR 3596603

[9] Jinhui Chao, Osamu Nakamura, Kohji Sobataka, and Shigeo Tsujii, *Construction of secure elliptic cryptosystems using CM tests and liftings*, Advances in cryptology—ASIACRYPT 1998, Lecture Notes in Comput. Sci., no. 1514, Springer, 1998, pp. 95–109. MR 1727916

[10] J.-M. Couveignes, *Linearizing torsion classes in the Picard group of algebraic curves over finite fields*, J. Algebra **321** (2009), no. 8, 2085–2118. MR 2501511

[11] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, Arithmetics, geometry, and coding theory, Sémin. Congr., no. 21, Soc. Math. France, Paris, 2010, pp. 161–176. MR 2856565

[12] David Freeman and Kristin Lauter, *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*, Algebraic geometry and its applications, Ser. Number Theory Appl., no. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 29–66. MR 2484047

[13] S. D. Galbraith, S. M. Paulus, and N. P. Smart, *Arithmetic on superelliptic curves*, Math. Comp. **71** (2002), no. 237, 393–405. MR 1863009

[14] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., no. 4284, Springer, 2006, pp. 114–129. MR 2444631

[15] Eyal Z. Goren, *On certain reduction problems concerning abelian surfaces*, Manuscripta Math. **94** (1997), no. 1, 33–43. MR 1468933

[16] Eyal Z. Goren and Kristin E. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 2, 457–480. MR 2310947

[17] ———, *Genus 2 curves with complex multiplication*, Int. Math. Res. Not. **2012** (2012), no. 5, 1068–1142. MR 2899960

[18] Rolf-Peter Holzapfel, *The ball and some Hilbert problems*, Birkhäuser Verlag, Basel, 1995. MR 1350073

[19] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401. MR 1297531

[20] Pinar Kiliçer, Elisa Lorenzo García, and Marco Streng, *Primes dividing invariants of CM Picard curves*, preprint, 2018. arXiv 1801.04682

[21] Pinar Kiliçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng, *Plane quartics over Q with complex multiplication*, preprint, 2017. arXiv 1701.06489

[22] Pinar Kiliçer, Kristin Lauter, Elisa Lorenzo García, Rachel Newton, Ekin Ozman, and Marco Streng, *A bound on the primes of bad reduction for CM curves of genus 3*, preprint, 2016. arXiv 1609.05826

[23] K. Koike and A. Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518. MR 2085904

[24] Serge Lang, *Complex multiplication*, Grundl. Math. Wissen., no. 255, Springer, 1983. MR 713612

[25] Joan-C. Lario and Anna Somoza, *A note on Picard curves of CM-type*, preprint, 2016. arXiv 1611.02582

[26] Kristin E. Lauter and Damien Robert, *Improved CRT algorithm for class polynomials in genus 2*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., no. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 437–461. MR 3207426

[27] William Messing, *The crystals associated to Barsotti–Tate groups: with applications to abelian schemes*, Springer, 1972. MR 0347836

[28] J. S. Milne, *Complex multiplication*, course notes, 2006.

[29] Frans Oort and Kenji Ueno, *Principally polarized abelian varieties of dimension two or three are Jacobian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 377–381. MR 0364265

[30] Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, no. 46, Princeton University Press, 1998. MR 1492449

[31] M. Streng, *Complex multiplication of abelian surfaces*, thesis, Universiteit Leiden, 2010.

[32] Ken-ichi Sugiyama, *On a generalization of Deuring's results*, Finite Fields Appl. **26** (2014), 69–85. MR 3151358

[33] Andrew V. Sutherland, *Accelerating the CM method*, LMS J. Comput. Math. **15** (2012), 172–204. MR 2970725

[34] John Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki 1968/69, Lecture Notes in Math., no. 175, Springer, Berlin, 1971, exposé no. 352, 95–110. MR 3077121

[35] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560. MR 0265369

[36] A. Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372. MR 1877806

[37] Paul B. Yale, *Automorphisms of the Complex Numbers*, Math. Mag. **39** (1966), no. 3, 135–141. MR 1581614

Received 22 Feb 2018. Revised 4 Jun 2018.

SONNY ARORA: sza149@psu.edu
Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, United States

KIRSTEN EISENTRÄGER: eisentra@math.psu.edu
Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

The cover image is based on a design by Linh Chi Bui.

Electronic copies can be obtained free of charge from http://msp.org/obs/2 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine