MATHEMATICS OF COMPUTATION
Volume 74, Number 249, Pages 499–518
S 0025-5718(04)01656-4
Article electronically published on May 21, 2004

CONSTRUCTION OF CM PICARD CURVES

KENJI KOIKE AND ANNEGRET WENG

Dedicated to the 60th birthday of Professor Rolf Peter Holzapfel

ABSTRACT. In this article we generalize the CM method for elliptic and hyperelliptic curves to Picard curves. We describe the algorithm in detail and discuss the results of our implementation.

1. INTRODUCTION

The applications of elliptic and hyperelliptic curves over finite fields to cryptography have been studied intensively [14, 20, 15]. Recently, other kinds of curves proved to be suitable for cryptosystems. The most important examples are superelliptic, or more general C_{ab}, curves [1, 7]. Since the discrete logarithm problem on a curve of genus $g \geq 4$ turned out to be easier than on a curve of lower genus [8], we are restricted to curves of genus $g \leq 3$.

A cyclic trigonal curve of genus $g = 3$ is called a **Picard curve** (see [25, 26, 12]). A Picard curve over a field κ is given by an affine equation of the form

$$y^3 = f(x), \quad f \in \kappa[x], \quad \deg(f(x)) = 4,$$

where f is a polynomial without multiple roots in $\overline{\kappa}$. If κ contains the third roots of unity, the curve is equipped with an automorphism of order 3 defined over κ.

There exists an algorithm for an efficient addition law on the degree zero divisor class group, $\mathrm{Pic}^0_C(\kappa)$, of a Picard curve defined over a finite field $\kappa = \mathbb{F}_q$ [7, 29]. Because of the Pohlig-Hellmann attack [27], the curve C defined over $\mathbb{F}_q$ should be chosen such that the order of $\mathrm{Pic}^0_C(\mathbb{F}_q)$ contains a large prime factor. To tackle this problem, we need an efficient point counting algorithm for the curve C (or $\mathrm{Pic}^0_C(\mathbb{F}_q)$). For fields of small characteristic p this problem has been solved using p-adic methods [9], but for large prime fields the question is still unanswered.

In this paper, we consider an alternative method for constructing Picard curves over large prime fields suitable for cryptography using complex multiplication. Note that the complex multiplication (CM) method is well-known for elliptic curves [2, 3]. Recently, this method has been extended to hyperelliptic curves of genus $g \leq 3$ [34, 36, 37, 38].

We now describe the CM method from an abstract point of view. Given a CM field K with $n_K = [K : \mathbb{Q}] \leq 6$, set $g = n_K/2$. In general the CM method can be described as follows:

Received by the editor February 3, 2003 and, in revised form, July 14, 2003.
2000 *Mathematics Subject Classification.* Primary 14H45, 11G15; Secondary 14G50, 14K22.
The first author was supported by the Alexander von Humboldt Stiftung. The second author was supported by the Maria Sibylla Merian program of the university of Essen.

(1) Construct the set of isomorphism classes of simple principally polarized abelian varieties of dimension g defined over $\mathbb{C}$. Represent each isomorphism class by a matrix Ω_i in the g-dimensional Siegel upper half space $\mathbb{H}_g$.
(2) For each matrix Ω_i, compute the set of absolute invariants $\{j_k^i\}$ by using values of the theta functions of Ω_i.
(3) Construct a curve with given absolute invariants.

Our paper is organized as follows. In Section 2 we recall some basic facts. In Section 3 we explain how to determine the set of isomorphism classes in step (1) of the algorithm. Section 4 deals with the theory of theta constants and invariants of a Picard curve. In Section 5 we summarize the complete algorithm and discuss subtleties of the implementation. Finally (Section 6) we give examples for Picard curves defined over $\mathbb{Q}$ and $\mathbb{F}_p$ with a Jacobian which has complex multiplication by a given CM field of degree 6.

For the computations we used the C-library Pari [5] and Magma [19]. The authors thank the referee for valuable comments for improving the paper.

2. Definitions and basic facts

2.1. **CM fields of Picard curves.** In this section we construct all CM fields which may occur as the endomorphism algebra of the Jacobian of a Picard curve.

Let K be a CM field of degree 6, i.e., a totally imaginary quadratic extension of a totally real number field of degree 3. Let J_C be the Jacobian of a Picard curve with complex multiplication by the maximal order $\mathcal{O}_K$ in K, i.e., $\mathrm{End}(J_C) \simeq \mathcal{O}_K$. Then automatically, we have $\mathbb{Q}(\zeta_3) \subseteq K$, where ζ_3 denotes a third root of unity. This means that K must be the composition of a totally real number field K_0 and the imaginary quadratic field $\mathbb{Q}(\zeta_3)$.

Conversely, we can prove the following lemma:

Lemma 1. *Let κ be an algebraically closed field of* $\mathrm{char}\,\kappa$ *different from* 3 *and let A be a principally polarized abelian variety of dimension 3 defined over κ with complex multiplication by $\mathcal{O}_K$ where K is a CM field containing the third roots of unity.*

Then A is simple and A is the Jacobian of a Picard curve.

Proof. The abelian variety A is obviously simple, since its endomorphism ring is commutative. It has an automorphism of order 3, since the roots of unity in the endomorphism ring respect the polarization (see the corollary following Proposition 3 in [31, Section 14]).

Moreover, A is isomorphic to the Jacobian variety of some curve C, since the principally polarized abelian varieties of dimension 3 are exactly the Jacobians of curves [24]. By Torelli's Theorem, the curve C is uniquely determined by the principally polarized abelian variety A and we have $\mathrm{Aut}(C)$ is isomorphic to $\mathrm{Aut}(J_C)/G$ where G is either trivial or $\{\pm 1\}$ (see, e.g., [21, Theorem 12.1] for the extended version of Torelli's theorem needed to conclude the fact about the automorphism group). Thus, A is the Jacobian of a curve C which is uniquely determined and has an automorphism of order 3.

Let $\kappa(C) = \kappa(x, y)$ be the function field of C and let $\kappa(\tilde{C})$ be the function field obtained by factoring out the automorphism α. Since J_C is simple, $\kappa(\tilde{C})$ must be the rational function field and $\kappa(C)/\kappa(\tilde{C})$ is a Kummer extension of degree three,

i.e., C can be given by an affine equation of the form $y^3 = f(x)$. By the Riemann–Hurwitz formula, $C \to \mathbb{P}_1$ is branched over five points. We may choose the point at infinity to be a ramification point. Then f has degree 4. □

For the rest of the paper we assume $K = K_0(\zeta_3)$.

2.2. **The group order over finite fields.** Let $\kappa = \mathbb{F}_p$ be a finite prime field with $p \equiv 1 \bmod 3$.

Suppose given a Picard curve defined over $\mathbb{F}_p$ whose Jacobian J_C is known to have complex multiplication by $\mathcal{O}_K$ for some CM field K of degree 6.

We claim that it is easy to determine the number of $\mathbb{F}_p$-rational points of J_C.

The p-th power Frobenius endomorphism π on the Jacobian J_C corresponds to an element $w \in \mathcal{O}_K$ with the property that w and all its conjugates have absolute value $\sqrt{p}$.

Since J_C is absolutely simple, $K = \mathbb{Q}(w)$. In this case, the minimal polynomial $f_w(t) \in \mathbb{Q}[t]$ is irreducible and coincides with the characteristic polynomial of the Frobenius on the $\mathbb{Q}_l$ vector space $V_l(J_C) = T_l(J_C) \otimes \mathbb{Q}_l$ where $T_l(J_C)$ denotes the Tate module of the Jacobian. The order of the group $J_C(\mathbb{F}_p)$ is given by the evaluation of the minimal polynomial $f_w(t)$ of w over $\mathbb{Q}$ at $t = 1$.

Let

$$S_{\mathcal{O}_K,p} = \{w \in \mathcal{O}_K : w\overline{w} = p, \mathbb{Q}(w) = K\}/\sim$$

where $w_1 \sim w_2$ if w_1 and w_2 are conjugate and let

$$N_{\mathcal{O}_K,p} := \{n \in \mathbb{N} : \#J_C(\mathbb{F}_p) = n \text{ for some } J_C \text{ with } \operatorname{End}(J_C) \simeq \mathcal{O}_K\}.$$

Then $S_{\mathcal{O}_K,p}$ has finite cardinality and $|N_{\mathcal{O}_K,p}| \le |S_{\mathcal{O}_K,p}|$. Hence, given a CM field K and a prime p we have only finitely many possible group orders. The elements in $S_{\mathcal{O}_K,p}$, resp. $N_{\mathcal{O}_K,p}$, can for example be found by factoring the ideal (p) in K. The factorization of prime ideals in number fields of low degree can efficiently be computed and it is implemented in many number theoretic libraries.

Once we have determined the set of possible group orders, we can then try to find the right order by choosing random divisor classes in the divisor class group.

3. The set of isomorphism classes

In this section, we determine all principally polarized abelian varieties over $\mathbb{C}$ with complex multiplication by the maximal order $\mathcal{O}_K$ in a CM field K. This is needed for the first step of the algorithm given in the introduction. We use the theory of complex multiplication by Shimura and Taniyama [31]. We summarize their results restricted to the case $[K : \mathbb{Q}] = 6$ (for details see [31], but also [34, 36, 38]).

Let K be a CM field of degree 6 with real subfield K_0.

A tuple $(K, \Phi) = (K, \{\varphi_1, \varphi_2, \varphi_3\})$ consisting of the CM field K and three embeddings of K into $\mathbb{C}$ such that $\varphi_i \ne \varphi_j, \overline{\varphi}_j$, $i \ne j$, is called a **CM type**. An abelian variety of dimension 3 over $\mathbb{C}$ can be given by a complex torus $\mathbb{C}^3/\Lambda$. We suppose that there exists an isomorphism $e : \operatorname{End}(A) \to \mathcal{O}_K$. In this situation, an abelian variety is said to be **of CM type** $(K, \Phi) = (K, \{\varphi_1, \varphi_2, \varphi_3\})$ if the basis of the lattice Λ can be chosen such that the endomorphism α is given by

$$\begin{pmatrix} \varphi_1(e(\alpha)) & & \\ & \varphi_2(e(\alpha)) & \\ & & \varphi_3(e(\alpha)) \end{pmatrix}. \tag{1}$$

There is a notion of a **primitive** CM type (see, e.g., [31, Section 8.2]) and the abelian variety A is simple if and only if the CM type (K, Φ) is primitive.

Note that $K = K_0(\zeta_3)$ is either Galois or has Galois closure L where L has degree 12 over $\mathbb{Q}$ (depending on whether the subfield K_0 is normal or not). In both cases there are three different primitive CM types, up to complex conjugation ([38, Lemma 3.1]).

Suppose K is Galois and Φ_1, Φ_2 are two different primitive CM types. In this case, the set of isomorphism classes of principally polarized abelian varieties with CM type Φ_1 coincides with the set of isomorphism classes of principally polarized abelian varieties of CM type Φ_2 ([38, Lemma 3.5]). Therefore, for normal K it is enough to determine the principally polarized abelian varieties for one fixed CM type.

For every ideal $\mathfrak{B}$ of $\mathcal{O}_K$ we define a lattice

$$\Phi(\mathfrak{B}) = \left\{ \Phi(\beta) = (\varphi_1(\beta), \varphi_2(\beta), \varphi_3(\beta))^t, \beta \in \mathfrak{B} \right\}$$

in $\mathbb{C}^3$. The torus $\mathbb{C}^3/\Phi(\mathfrak{B})$ defines an abelian variety A. Obviously, the abelian variety $\mathbb{C}^3/\Phi(\mathfrak{B})$ is invariant under the action of matrices of the form (1). All abelian varieties of CM type (K, Φ) with complex multiplication by $\mathcal{O}_K$ can be constructed this way ([17, Theorem 4.1]).

Next we want to define a Riemann form on the lattice $\Phi(\mathfrak{B})$ which induces a principal polarization on the abelian variety $\mathbb{C}^3/\Phi(\mathfrak{B})$. We cite the following theorem (cf. [31, Section 14.3] or [34]):

Theorem 2. *Let K be a CM field of degree 6 and let $\delta_{K/\mathbb{Q}}$ be the different of K.*

Let $\mathfrak{B}$ be an ideal in K such that $\delta_{K/\mathbb{Q}}\mathfrak{B}\overline{\mathfrak{B}}$ is a principal ideal (b). Suppose there exists a CM type $(\varphi_1, \varphi_2, \varphi_3)$ and a unit $\varepsilon \in \mathcal{O}_{K_0}$ such that εb is totally imaginary and $\operatorname{Im} \varphi_i(\varepsilon b) < 0$ for all i. Write $\xi = (\varepsilon b)^{-1}$. The bilinear form

$$E_\xi(x, y) = \sum_{i=1}^{3} \varphi_i(\xi)(\overline{x_i} y_i - x_i \overline{y_i}) \tag{2}$$

defines a principal polarization on the lattice $\Phi(\mathfrak{B})$.

From now on the tuple $(\Phi(\mathfrak{B}), \xi)$ denotes the principally polarized abelian variety given by the torus $\mathbb{C}^3/\Phi(\mathfrak{B})$ together with the Riemann form $E_\xi(x, y)$.

Using the following two facts (see [31, Chapter 7]) it is easy to list a complete set of isomorphism classes of principally polarized abelian varieties having complex multiplication by $\mathcal{O}_K$:

- Let U (resp. U^+) be the group of units (resp. totally positive units) in $\mathcal{O}_{K_0}$, and let U_1 be the subgroup of U^+ of elements of the form $\varepsilon\overline{\varepsilon}$, $\varepsilon \in \mathcal{O}_K^*$. Choose a set of representatives $\{\varepsilon_1, \ldots, \varepsilon_d\}$ for the cosets U^+/U_1. Suppose there exists an element ξ as in Theorem 2. The set of isomorphism classes of principally polarized abelian varieties corresponding to $\Phi(\mathfrak{B})$ is given by $\{(\Phi(\mathfrak{B}), \varepsilon_i \xi), i = 1, \ldots, d\}$.
- Two principally polarized abelian varieties $(\Phi(\mathfrak{B}_1), \xi_1)$ and $(\Phi(\mathfrak{B}_2), \xi_2)$ are isomorphic if and only if there exists some $\gamma \in K$ such that $\gamma\mathfrak{B}_1 = \mathfrak{B}_2$ and $\xi_1 = \gamma\overline{\gamma}\xi_2$.

This leads to the following algorithm. Let $\delta_{K/\mathbb{Q}}$ be the different of K and let $\{\varepsilon_1, \ldots, \varepsilon_d\}$ be a set of representatives for the cosets U^+/U_1 (see Section 7.1 for

the computation of U^+/U_1). Let U_K be the set of units in K. Note that U, and therefore also U^+, has finite index in U_K. Choose representatives $u_1, \dots, u_e$ of U_K/U^+.

For every ideal class represented by an ideal $\mathfrak{B}$ with $\delta_{K/\mathbb{Q}}\mathfrak{B}\overline{\mathfrak{B}} = (b)$ principal and every CM type $(K, \Phi) = (K, \{\varphi_i\})$ we check if there exists a j such that $u_j b$ is totally imaginary and $\operatorname{Im}\varphi_i(u_j b) < 0$ for all i. If such a j exists, we define a principal polarization on $\Phi(\mathfrak{B})$ by the Riemann form E_ξ with $\xi = (u_j b)^{-1}$. We find all isomorphism classes of principally polarized abelian varieties corresponding to $\Phi(\mathfrak{B})$ by $\{(\Phi(\mathfrak{B}), \varepsilon_i\xi), i = 1, \dots, d\}$.

Given the principally polarized abelian variety $(\Phi(\mathfrak{B}), \xi)$ (resp. $(\Phi(\mathfrak{B}), \varepsilon_i\xi)$), we determine a basis $\beta_1, \dots, \beta_6$ of the lattice $\Phi(\mathfrak{B})$ such that

$$(E(\Phi(\beta_i), \Phi(\beta_j)))_{1\le i,j\le 3} = \begin{pmatrix} O & E_3 \\ -E_3 & 0 \end{pmatrix},$$

where E is the Riemann form corresponding to ξ defined by (2). Such a basis is called a Frobenius basis. It always exists and we describe an algorithm which determines a Frobenius basis for abelian varieties in arbitrary dimension in the appendix, Section 7.2.

Next we represent each isomorphism class of principally polarized abelian varieties by the matrix $\mathcal{A}_2^{-1}\mathcal{A}_1$ in the Siegel upper half space $\mathbb{H}_3 = \{\Omega \in \mathrm{Gl}_3(\mathbb{C}) : \Omega = \Omega^T, \operatorname{Im}(\Omega) \text{ is positive definite}\}$ where

$$\mathcal{A}_1 = (\Phi(\beta_1), \Phi(\beta_2), \Phi(\beta_3)) \text{ and } \mathcal{A}_2 = (\Phi(\beta_4), \Phi(\beta_5), \Phi(\beta_6)).$$

If the real subfield K_0 has a power integer basis and class number 1, the period matrices describing the lattice can be given more explicitly and the determination of the set of principally polarized abelian varieties can be simplified (see [38]).

4. Theta constants of Picard curves

4.1. **Invariants of Picard curves.** Let κ be a field of characteristic different from 2 and 3 and let C be a Picard curve defined over κ.

Without loss of generality, we may assume that C is given by

$$y^3 = x^4 + g_2x^2 + g_3x + g_4, \qquad g_i \in \kappa.$$

The coefficients g_i are invariants of the binary form $f(x, z) = x^4 + g_2x^2z^2 + g_3xz^3 + g_4z^4$ of degree i.

We describe the absolute invariants of a Picard curve over a finite prime field $\mathbb{F}_p$ (more details can be found in Section 7.5 in [12]). For that we distinguish six cases:

(1) For the majority of curves, we have $g_2g_3 \neq 0$. In this case, the isomorphism class of the Picard curve over $\overline{\kappa}$ is determined by

$$j_1 = \frac{g_3^2}{g_2^3} \quad \text{and} \quad j_2 = \frac{g_4}{g_2^2}.$$

Suppose there exists a Picard curve with $y^3 = x^4 + g_2x^2 + g_3x + g_4$ with j-invariants $j_1, j_2 \in \mathbb{F}_p$, $p \equiv 1 \bmod 3$. Then there are precisely three isomorphism classes of curves over $\mathbb{F}_p$ with invariants j_1 and j_2 given by

$$C_k : y^3 = x^4 + b^{2k}g_2x^2 + b^{3k}g_3x + b^{4k}g_4, \qquad k = 0, 1, 2,$$

where $b \in \kappa$ is a cubic non-residue. The curves C_k, $k = 0, 1, 2$, will be called **cubic twists** of each other.

(2) If $g_2 \neq 0$ but $g_3 = 0$, $j_1 = 0$ and the invariant j_2 determines the isomorphism class. It can easily be shown that the curve is singular if and only if $j_2 \in \{0, \frac{1}{4}\}$. For each $j_2 \notin \{0, \frac{1}{4}\}$ we get six isomorphism classes of curves over $\mathbb{F}_p$, $p \equiv 1 \bmod 3$ given by

$$y^3 = x^4 + b^k g_2 x^2 + b^{2k} g_4, \quad k = 0, \ldots, 5.$$

where b is a non-square and non-cube in κ.

(3) If $g_2 = 0$ and $g_3 g_4 \neq 0$, the isomorphism class is given by $j = \frac{g_4^3}{g_3^4}$. We have only the cubic twists described above.

(4) Over $\overline{\kappa}$ there exists only one isomorphism class with $g_2 = g_4 = 0$ (but $g_3 \neq 0$). It corresponds to the family of curves whose Jacobians have complex multiplication by $\mathbb{Z}[\zeta_9]$. We get 1, 3 or 9 isomorphism classes depending on whether $p \not\equiv 1 \bmod 3$, $p \equiv 4, 7 \bmod 9$ or $p \equiv 1 \bmod 9$. If $p \equiv 1 \bmod 9$, the 9 isomorphism classes are given by the curves

$$y^3 = x^4 + b^k x, \quad k = 0, \ldots, 8$$

where b is a non-cube in $\mathbb{F}_p$.

(5) There is only one isomorphism class over $\overline{\kappa}$ of curves with $g_4 = g_3 = 0$. We get 1, 4, 6 or 12 isomorphism classes depending on whether $p \equiv 11 \bmod 12$, $p \equiv 5 \bmod 12$, $p \equiv 7 \bmod 12$ or $p \equiv 1 \bmod 12$. If $p \equiv 1 \bmod 12$, the isomorphism classes are given by

$$y^3 = x^4 + b^k, \quad k = 0, \ldots, 11$$

where b is a non-square and non-cube in $\mathbb{F}_p$.

If $g_2 g_3 \neq 0$, the curve

$$C : y^3 = x^4 + j_1 x^2 + j_1^2 x + j_1^2 j_2 \tag{3}$$

has invariants j_1 and j_2. In a similar fashion we can deal with the other five cases. For every Picard curve it is possible to write down a model over $\kappa'(j_1, j_2)$ where κ' is the prime field of κ. Hence, every Picard curve has a model over the field where its invariants j_i are defined.

The characteristic polynomials of the Frobenius elements of the twists of C can easily be deduced from the characteristic polynomial of C.

Lemma 3. *Suppose $\kappa = \mathbb{F}_p$ with $p \equiv 1 \bmod 3$ and let C be a Picard curve with $g_2, g_3 \neq 0$ whose Jacobian has complex multiplication by the maximal order in a CM field.*

Suppose the p-th power Frobenius corresponds to an element $w \in \mathcal{O}_K$, i.e., $\#J_C(\mathbb{F}_p) = \prod_{i=1}^{6}(1 - w_i)$ by Section 2.2. The Frobenius elements of the cubic twists are given by $\zeta_3 w$ and $\zeta_3^2 w$.

Proof. The curves C_i, $i = 1, 2, 3$, are not isomorphic over $\mathbb{F}_p$ but over $\mathbb{F}_{p^3}$. Their Jacobians are also not isogenous over $\mathbb{F}_p$, since any such isogeny would already be an isomorphism.

Let w_{C_i} be the Frobenius elements of J_{C_i}, $i = 1, 2, 3$. Then

$$w_{C_1}^3 = w_{C_2}^3 = w_{C_3}^3$$

which implies that they all differ by multiplication by a third root of unity. □

Analogous statements can be made in case $g_2 g_3 = 0$. The group order of the twists can always be easily determined from a single Frobenius element w.

4.2. **Equation of Picard curves over $\mathbb{C}$.** In this section, we give an explicit formula which expresses the branch points of a Picard curve by theta functions. This formula goes back to Picard [25] and has already been worked out for a special symplectic basis in [30]. But since the period matrices constructed in Section 3 are in general not of a special form, we have to review the arguments in [25, 30] and give a more general formulation using geometric considerations.

4.2.1. *Facts on theta functions.* We first summarize some facts about theta functions. For more details see [22, 33].

Let $\delta, \varepsilon \in \mathbb{Q}^g$. The theta function with characteristic (δ, ε) is the function

$$\theta \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i (n+\delta)^t \Omega (n+\delta) + 2\pi i (n+\delta)^t (z+\varepsilon)\right)$$

of $(z, \Omega) \in \mathbb{C}^g \times \mathbb{H}_g$, where $\mathbb{H}_g = \{\Omega \in \mathrm{Gl}_g(\mathbb{C}) : \Omega = \Omega^t, \mathrm{Im}(\Omega) \text{ positive definite}\}$ is the Siegel upper half space of degree g.

The theta function with characteristic $\delta = \varepsilon = \mathbf{O}$ is called the **Riemann theta function** $\theta(z, \Omega)$. For half integral vectors $\delta, \varepsilon \in \left(\frac{1}{2}\mathbb{Z}\right)^g$, the characteristic (δ, ε) is called **even** (**odd**) if $4\delta^t\varepsilon$ is even (resp. odd). All characteristics are regarded as residue classes modulo integral vectors, as usual.

Theta functions with characteristics are related to the Riemann theta function via the formula

$$\theta \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} (z, \Omega) = \exp\left(\pi i \delta^t \Omega \delta + 2\pi i \delta^t (z+\varepsilon)\right) \theta(z + \Omega\delta + \varepsilon, \Omega). \tag{4}$$

We identify the characteristic $(\delta, \varepsilon) \in \mathbb{Q}^g \times \mathbb{Q}^g$ with $\Omega\delta + \varepsilon \in \mathbb{C}^g$.

Now let Ω be the period matrix of a smooth algebraic curve X of genus g over $\mathbb{C}$. Fix a base point $P \in X$ and consider the Abel–Jacobi map

$$\alpha : \mathrm{Sym}^k X(\mathbb{C}) \longrightarrow J_X(\mathbb{C}) = \mathbb{C}^g/(\mathbb{Z}^g + \mathbb{Z}^g\Omega), \quad Q_1 + \cdots + Q_k \mapsto \sum_{i=1}^{k} \int_P^{Q_i} w,$$

where $w = (w_1, \cdots, w_g)$ and the w_i's form a basis of $H^0(X, \Omega^1_X)$. The image of $\mathrm{Sym}^{g-1} X$ under α is equal to the zero divisor of the Riemann theta function, up to translation by some element $\Delta \in J_X(\mathbb{C})$. This element is called the **Riemann constant**. More precisely, we have the following theorem.

Theorem 4 (Riemann's Vanishing Theorem, [22, Corollary 3.6])**.** *Let $\theta(z, \Omega)$ be the Riemann theta function. We have*

$$\theta(z, \Omega) = 0 \Leftrightarrow z = \Delta - \alpha(Q_1 + \ldots + Q_{g-1}) \text{ with } Q_i \in X$$

where Δ is the Riemann constant. The Riemann constant is uniquely determined by this property if we fix the base point P.

Remark 5. It is known that $\Delta = \alpha(D_0)$ for some half canonical divisor D_0 [22]. Let us assume that the base point P is chosen such that $(2g-2)P$ is a canonical divisor. Then $D = (g-1)P$ is also a half canonical divisor. Because $2D$ and $2D_0$ are canonical divisors, we have $\alpha(2D_0) = \alpha(2D)$. By definition, $\alpha(2D) = 0 \in J_C(\mathbb{C})$, and we see that $\Delta = \alpha(D_0)$ is a 2-torsion point. So we may write $\Delta = \Omega\delta + \varepsilon$ with $(\delta, \varepsilon) \in (\frac{1}{2}\mathbb{Z})^g \times (\frac{1}{2}\mathbb{Z})^g$. The corresponding characteristics (δ, ε) depends on the choice of a symplectic basis of $H_1(X, \mathbb{Z})$. We will use this fact later.

The following theorem allows us to express the values of a function on X by theta constants.

Theorem 6 ([33, p. 177])**.** *Let f be a function on X. Write*

$$(f) = \sum_{i=1}^{m} P_i - \sum_{i=1}^{m} Q_i.$$

Choose paths from the base point P to P_i and Q_i such that

$$\sum_{i=1}^{m} \int_P^{P_i} w = \sum_{i=1}^{m} \int_P^{Q_i} w.$$

Then

$$f(D) = f(R_1) \cdots f(R_g) = E \prod_{k=1}^{m} \frac{\theta\left(\sum_{i=1}^{g} \int_P^{R_i} w - \int_P^{P_k} w - \Delta, \Omega\right)}{\theta\left(\sum_{i=1}^{g} \int_P^{R_i} w - \int_P^{Q_k} w - \Delta, \Omega\right)} \tag{5}$$

as a meromorphic function of $D = R_1 + \ldots + R_g \in \operatorname{Sym}^g X$, where E is some constant independent of D and the integral $\int_P^{R_i} w$ in the numerator and denominator are taken along the same path.

Remark 7. By Riemann's Vanishing Theorem, the denominator and the numerator of the theta quotient in formula (5) do not vanish if the divisors $D - P_k$ and $D - Q_k$ of degree $g - 1$ are general (non-special) divisors; that is, $\ell(\kappa - D + P_k) = \ell(\kappa - D + Q_k) = 0$ where κ is a canonical divisor and $\ell(D) = \dim H^0(X, \mathcal{O}_X(D))$.

4.2.2. *Picard's Formula.* Let us return to the Picard case. We consider the following normalized form

$$C/\mathbb{C} : y^3 = x(x-1)(x-\lambda)(x-\mu). \tag{6}$$

Our goal is to express λ and μ by theta functions applying Theorem 6. Let $P_1, \ldots, P_5 \in C$ be the points lying above the branch points $0, 1, \lambda, \mu, \infty$ of the map $\pi : C \to \mathbb{P}_1,\ (x, y) \mapsto x$. We apply Theorem 6 for the function π and the divisor $D = 2P_2 + P_3$. The divisor of π is $3P_1 - 3P_5$. We get

$$\pi(D) = \pi(P_2)\pi(P_2)\pi(P_3) = \lambda = E \prod_{k=1}^{3} \frac{\theta\left(2\int_{P_5}^{P_2} w + \int_{P_5}^{P_3} w - \int_{\gamma_k} w - \Delta, \Omega\right)}{\theta\left(2\int_{P_5}^{P_2} w + \int_{P_5}^{P_3} w - \Delta, \Omega\right)}$$

where the paths γ_k from P_5 to P_1 on C are chosen such that $\sum \gamma_k = \mathbf{0}$. To see that the theta functions in the equation do not vanish, let us consider the linear system $\mathcal{L}_i = \mathcal{L}(\kappa - D + P_i)$ for $i = 1$ and 5. By the Riemann–Roch Theorem (or the residue theorem), we see that there is no rational 1-form with only one pole at P_i of order 1; moreover the canonical class of C is given by a line on $\mathbb{P}^2$. So elements in $\mathcal{L}_i$ are given by lines that pass through P_3 and are tangent to C at P_2. But such a line does not exist and we have $\ell(\kappa - D + P_i) = 0$ for $i = 1$ and 5. Hence this expression of λ as a quotient of theta constants is well defined.

By considering the divisor $D' = P_2 + 2P_3$ instead of D, we can express $\lambda^2 = \pi(D')$ by theta functions, and by taking the quotient $\pi(D')/\pi(D)$, we can eliminate the

constant E. Analogously, we can express μ by theta constants and obtain (cf. [25, 26])

$$\lambda = \prod_{k=1}^{3} \frac{\theta\left(\int_{P_5}^{P_2} w + 2\int_{P_5}^{P_3} w - \int_{\gamma_k} w - \Delta, \Omega\right)}{\theta\left(\int_{P_5}^{P_2} w + 2\int_{P_5}^{P_3} w - \Delta, \Omega\right)} \times \prod_{k=1}^{3} \frac{\theta\left(2\int_{P_5}^{P_2} w + \int_{P_5}^{P_3} w - \Delta, \Omega\right)}{\theta\left(2\int_{P_5}^{P_2} w + \int_{P_5}^{P_3} w - \int_{\gamma_k} w - \Delta, \Omega\right)}$$

and

$$\mu = \prod_{k=1}^{3} \frac{\theta\left(\int_{P_5}^{P_2} w + \int_{P_5}^{P_4} w - \int_{\gamma_k} w - \Delta, \Omega\right)}{\theta\left(\int_{P_5}^{P_2} w + 2\int_{P_5}^{P_4} w - \Delta, \Omega\right)} \times \prod_{k=1}^{3} \frac{\theta\left(2\int_{P_5}^{P_2} w + \int_{P_5}^{P_4} w - \Delta, \Omega\right)}{\theta\left(2\int_{P_5}^{P_2} w + \int_{P_5}^{P_4} w - \int_{\gamma_k} w - \Delta, \Omega\right)}.$$

4.2.3. *Vanishing properties of Picard theta functions.* To obtain a more explicit representation of λ and μ in terms of theta characteristics, we consider the 3-torsion points of $J(C)$ obtained from branch points more closely.

Choose P_5 as the base point of α. We see that $\Delta \in J_C[2]$ since $(dx/y^2) = 4P_5$ (see Remark 5), where $J_C[m]$ denotes the subgroup of m-torsion points of the Jacobian. Note that the divisor of the function

$$\pi : C \longrightarrow \mathbb{P}^1, \quad (x, y) \mapsto x$$

is given by $3P_1 - 3P_5$. Hence $\alpha(P_1)$ is a 3-torsion point of the Jacobian. Similarly we have $\alpha(P_1), \ldots, \alpha(P_4) \in J_C[3]$.

From Theorem 4 we deduce that there must be 15 torsion points of the form $\Delta + \alpha(D) \in J_C[6]$ with $D = P_1 + P_2$ and $\alpha(D) \in J_C[3]$ which lie in the zero locus of θ. These are given by

$$\begin{aligned}&\alpha(D) \in \{\alpha(2P_1), \alpha(P_1 + P_2), \alpha(P_1 + P_3), \alpha(P_1 + P_4), \alpha(P_1 + P_5), \alpha(2P_2),\\ &\alpha(P_2 + P_3), \alpha(P_2 + P_4), \alpha(P_2 + P_5), \alpha(2P_3), \alpha(P_3 + P_4), \alpha(P_3 + P_5), \alpha(2P_4),\\ &\alpha(P_4 + P_5), \alpha(2P_5) = \mathbf{0}\}.\end{aligned}$$

Because C is a smooth quartic curve, it is the canonical model of a curve of genus 3 ([11, p. 342]). It is therefore not hyperelliptic and it does not have a function of order 2. Therefore the above 15 elements are different from each other. Note that by formula (4), $\theta(\Delta + \alpha(D)) = 0$ is equivalent to $\theta[\Delta + \alpha(D)](0, \Omega) = 0$.

Remark 8. By the automorphism $\varrho : (x, y) \mapsto (x, \zeta_3 y)$, $H_1(C, \mathbb{Z})$ has the structure of a $\mathbb{Z}[\varrho]$-module (so $\mathbb{Z}[\zeta_3]$-module). In fact, it is known that $H_1(C, \mathbb{Z})$ is generated by three elements as a $\mathbb{Z}[\varrho]$-module [25]. Therefore we have $H_1(C, \mathbb{Z}) \cong \mathbb{Z}[\zeta_3]^3$. The group

$$J_C[1 - \zeta_3] = \mathrm{Ker}(1 - \varrho) \subset J_C[3]$$

is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$. Since $\varrho(P_i) = P_i$, we see that $\alpha(P_i) \in J_C[1 - \zeta_3]$. Let G be the subgroup generated by $\alpha(P_1), \ldots, \alpha(P_4)$. Then we have $G \subset J_C[1 - \zeta_3]$, and G has at least the above 15 elements. Hence we conclude that $G = J_C[1 - \zeta_3]$.

The group G is generated by $\alpha(P_1), \dots, \alpha(P_4)$. The divisor of a function

$$C \longrightarrow \mathbb{P}^1, \quad (x, y) \mapsto y$$

is $P_1 + P_2 + P_3 + P_4 - 4P_5$. We conclude that the $\alpha(P_i)$ satisfy a unique relation $\sum \alpha(P_i) = 0$.

Let A_i, B_i, $i = 1, 2, 3$, be a symplectic basis of $H_1(C, \mathbb{Z})$ such that $A_i \cdot B_j = \delta_{ij}$. The Riemann constant can be computed easily if the symplectic representation of ϱ is known. Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(6, \mathbb{Z})$ be the symplectic representation of ϱ. More precisely, M is defined by

$$\varrho(B_1, B_2, B_3, A_1, A_2, A_3) = (B_1, B_2, B_3, A_1, A_2, A_3)^t M.$$

The matrix M acts on $\mathbb{C}^3 \times \mathbb{H}_3$ via

$$(M \cdot z,\ M \cdot \Omega) = ({}^t(C\Omega + D)^{-1} z, (A\Omega + B)(C\Omega + D)^{-1}),$$

and we have $M \cdot \Omega = \Omega$ because ϱ is an automorphism of C. On characteristics, the action of M is given by

$$M \cdot \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} = \begin{bmatrix} D\delta - C\varepsilon + \frac{1}{2}(C\,{}^t D)_0 \\ -B\delta + A\varepsilon + \frac{1}{2}(A\,{}^t B)_0 \end{bmatrix}, \tag{7}$$

where $(N)_0$ is the diagonal of a matrix N.

Remark 9. We can identify characteristics $(\delta, \varepsilon) \in \mathbb{Q}^6$ with the coordinates of torsion points $H_1(C, \mathbb{Q})/H_1(C, \mathbb{Z})$. Note that δ (resp. ε) represents the coordinate for B_i (resp. A_i). The action of ϱ on torsion points is therefore represented as

$$\varrho : \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} \mapsto \begin{pmatrix} D & -C \\ -B & A \end{pmatrix} \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix}. \tag{8}$$

But we need the diagonal vector in (7) for the transformation formula of theta functions. Obviously, the fixed points of the action (8) are just the 27 elements of $J_C[1 - \zeta_3]$.

Lemma 10. *The Riemann constant Δ is the unique odd characteristic such that $M \cdot \Delta = \Delta$.*

Proof. Since C is not hyperelliptic, the Riemann constant Δ must be odd. If we apply the theta transformation formula [18, p. 231] for M, we get

$$\theta[M \cdot \Delta]({}^t(C\Omega + D)^{-1} z, \Omega) = (\text{automorphic factor}) \times \theta[\Delta](z, \Omega).$$

The right-hand side vanishes exactly on $\alpha(\mathrm{Sym}^2 C)$, so the function $\theta[M \cdot \Delta](z, \Omega)$ vanishes on the divisor ${}^t(C\Omega + D)^{-1}\alpha(\mathrm{Sym}^2 C)$. Note that ${}^t(C\Omega + D) \in GL_3(\mathbb{C})$ is the analytic representation of ϱ with respect to the normalized basis of $H^0(C, \Omega^1_C)$. Hence, for $Q_i \in C$ we have

$$\begin{aligned} {}^t(C\Omega + D)^{-1}\alpha(Q_1 + Q_2) &= \sum_{k=1}^{2} \int_{P_5}^{Q_k} {}^t(C\Omega + D)^{-1} w \\ &= \sum_{k=1}^{2} \int_{P_5}^{Q_k} (\varrho^{-1})^* w = \sum_{k=1}^{2} \int_{\varrho^{-1}(P_5)}^{\varrho^{-1}(Q_k)} w = \sum_{k=1}^{2} \int_{P_5}^{\varrho^{-1}(Q_k)} w, \end{aligned}$$

and this is equal to $\alpha(\varrho^{-1}(Q_1) + \varrho^{-1}(Q_2))$. Therefore the function $\theta[M \cdot \Delta](z, \Omega)$ vanishes exactly on $\alpha(\varrho^{-1}(\mathrm{Sym}^2 C)) = \alpha(\mathrm{Sym}^2 C)$, and we have $M \cdot \Delta = \Delta$.

Let us recall that every smooth quartic curve has 28 bitangent lines $l_1, \cdots, l_{28}$ and that they define odd characteristics (see [6]). More precisely, odd characteristics of $J(C)$ are given by

$$\alpha(Q_i + Q_i') - \Delta = \Omega\delta_i + \varepsilon_i, \quad (\delta_i, \varepsilon_i) \in (\frac{1}{2}\mathbb{Z})^3 \times (\frac{1}{2}\mathbb{Z})^3,$$

where Q_i and Q_i' are tangent points of l_i. It is obvious that invariant odd characteristics are obtained from bitangent lines invariant under the action of ϱ. The projective equation of C is

$$ZY^3 = X(X - \lambda_1 Z)(X - \lambda_2 Z)(X - \lambda_3 Z).$$

The action of ϱ is given by $[X : Y : Z] \mapsto [X : \zeta_3 Y : Z]$. One checks that $l = \{Z = 0\}$ is the unique invariant bitangent line. For this line we have $l \cap C = 4P_5$ and $\alpha(P_5 + P_5) = 0$. □

We summarize the results of our discussion:

Corollary 11. *Let Ω be the period matrix of the Jacobian of a Picard curve, and let $M \in Sp(6, \mathbb{Z})$ be the symplectic representation of ϱ. The Riemann constant Δ is the unique odd theta characteristic such that $M \cdot \Delta = \Delta$.*

There is a set S_1 of 15 theta characteristics $\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right]$ in $\left(\frac{1}{3}\mathbb{Z}/\mathbb{Z}\right)^6$ (including $\left[\begin{smallmatrix}\mathbf{0}\\ \mathbf{0}\end{smallmatrix}\right]$) fixed by M (as a linear transformation) with

$$\theta\left[\begin{pmatrix}\delta\\ \varepsilon\end{pmatrix} + \Delta\right](0, \Omega) = 0.$$

There is a subset $S_2 = \{D_1, \ldots, D_4\} \subset S_1$ with the property that each three characteristics in S_2 are linearly independent, but $\sum_{i=1}^4 D_i = \mathbf{0}$.

In terms of theta functions with characteristics, the formulas for λ and μ in the last paragraph become (using (4))

$$\lambda = \left(\frac{\theta[D_2 + 2D_3 - D_1 - \Delta](0,\Omega) \cdot \theta[2D_2 + D_3 - \Delta](0,\Omega)}{\theta[D_2 + 2D_3 - \Delta](0,\Omega) \cdot \theta[2D_2 + D_3 - D_1 - \Delta](0,\Omega)}\right)^3,$$

$$\mu = \left(\frac{\theta[D_2 + 2D_4 - D_1 - \Delta](0,\Omega) \cdot \theta[2D_2 + D_4 - \Delta](0,\Omega)}{\theta[D_2 + 2D_4 - \Delta](0,\Omega) \cdot \theta[2D_2 + D_4 - D_1 - \Delta](0,\Omega)}\right)^3.$$

Since $D_1 + D_2 + D_3 + D_4 = 0$ and $\theta[D](0,\Omega) = \theta[-D](0,\Omega)$, we conclude $2D_2 + D_3 - D_1 = D_2 + 2D_4 - 2D_1$ and

$$\theta[2D_2 + D_3 - D_1 - \Delta](0,\Omega) = \theta[2D_2 + D_4 - D_1 - \Delta](0,\Omega).$$

The computation of the equation of the curve over $\mathbb{C}$ reduces to the evaluation of three theta constants, i.e.,

(9)

$$\lambda = \left(\frac{\theta[D_2 + 2D_3 - D_1 - \Delta](0,\Omega)}{\theta[2D_2 + D_3 - D_1 - \Delta](0,\Omega)}\right)^3 \text{ and } \mu = \left(\frac{\theta[D_2 + 2D_4 - D_1 - \Delta](0,\Omega)}{\theta[2D_2 + D_3 - D_1 - \Delta](0,\Omega)}\right)^3.$$

5. The complete algorithm

We now describe the algorithm to construct Picard curves over finite fields $\mathbb{F}_p$, where p is a large prime.

5.1. **Precomputation.** We first perform a precomputation step.

Given a CM field $K = K_0(\zeta_3)$, we compute different primes $p = w\overline{w}$, $w \in \mathcal{O}_K$, the corresponding sets $S_{\mathcal{O}_K,p}$ described in Section 2.2 and the sets of possible group orders

$$\{f_w(1) : w \in S_{\mathcal{O}_K,p}\}. \tag{10}$$

If the set (10) contains an order which is prime up to a small cofactor, we try to construct the corresponding curve.

Note that for every Frobenius element $w \in S_{\mathcal{O}_K,p}$ we find five more Frobenius elements $-w, \pm\zeta_3 w, \pm\zeta_3^2$. In contrast to elliptic or hyperelliptic curves, not every such element can necessarily be realized as the Frobenius of a curve. Given a Picard curve with $g_2 g_3 \neq 0$, j-invariants j_1, j_2 and Frobenius corresponding to $w \in \mathcal{O}_K$, there exist only two more isomorphism classes of curves over $\mathbb{F}_p$ with the same j-invariant and Frobenius elements $\zeta_3^k w$, $k = 1, 2$ (see Section 4.1).

By the theorem of Honda-Tate [13, 35], every element in $S_{\mathcal{O}_K,p}$ can be realized as the Frobenius of a principally polarized abelian variety over $\mathbb{F}_p$. If C is a Picard curve defined over $\mathbb{F}_p$ with $g_2 g_3 \neq 0$ and w the Frobenius of J_C, we can construct a principally polarized abelian variety with Frobenius $-w$ as follows. The Weil restriction of the Jacobian over $\mathbb{F}_{p^2}$ factors into two principally polarized abelian varieties defined over $\mathbb{F}_p$, one being the principally polarized abelian variety A which is $\mathbb{F}_p$-isomorphic to J_C with Frobenius corresponding to w and the quadratic twist A' with Frobenius element equal to $-w$. Suppose C' were a curve with Jacobian A'. Then C and C' would be isomorphic over $\mathbb{F}_{p^2}$ but not over $\mathbb{F}_p$. They had the same j-invariants, which leads to a contradiction.

Hence, for a given CM field $K \supset \mathbb{Q}(\zeta_3)$, a given prime p and a group order $f_w(1)$ we find a Picard curve C with $\#J_C(\mathbb{F}_p) = f_w(1)$ with probability $\frac{1}{2}$. In any case, we can find a principally polarized abelian variety A defined over $\mathbb{F}_p$ with $\#A(\mathbb{F}_p) = f_w(1)$. There exists a Picard curve C defined over $\mathbb{F}_p$ such that A is either $\mathbb{F}_p$-isomorphic to J_C or the $\mathbb{F}_p$-rational points of A are in 1-1 correspondence to the $\mathbb{F}_{p^2}$-rational points $R \in J_C$ which satisfy $\pi_p(R) + \pi_p^2(R) = 0$ where π_p is the p-th power Frobenius on J_C.

5.2. **The construction algorithm.** We present the algorithm for constructing a Picard curve over $\mathbb{F}_p$ with given group order $n = n(\mathcal{O}_K, p)$.

Input: CM field $K = K_0(\zeta_3)$, $p = w\overline{w}$, $w \in \mathcal{O}_K$, a group order $n(p, \mathcal{O}_K)$ with a large prime factor
Output: Picard curve over $\mathbb{F}_p$

(1) Determine a complete set of isomorphism classes of all principally polarized abelian varieties having complex multiplication by $\mathcal{O}_K$. Represent each isomorphism class by a matrix $\Omega_i \in \mathbb{H}_3$ (see Section 3).

Parallel to this computation we find for each Ω_i the rational representation $M_i \in \mathrm{Sp}(6, \mathbb{Z})$ of the automorphism ζ_3 of order 3.

Let s be the number of isomorphism classes.

(2) The next steps have to be done for each isomorphism class Ω_i, $1 \leq i \leq s$:
   (a) Compute the unique odd theta characteristic Δ, $\Delta \in (\mathbb{Z}/2\mathbb{Z})^{2g}$, fixed by M_i (where the operation of $\mathrm{Sp}(6, \mathbb{Z})$ on $(\mathbb{Z}/2\mathbb{Z})^{2g}$ is given as in (7)).
   (b) Determine the set $S = \{\tau = (\delta, \varepsilon), \delta, \varepsilon \in (\mathbb{Z}/3\mathbb{Z})^g\}$ of 27 theta characteristics fixed by M_i (where the action of $\mathrm{Sp}(6, \mathbb{Z})$ is now given by (8))

and compute the theta function $\theta[\tau+\Delta](0,\Omega)$ of characteristic $1/6$. Determine the subset of elements τ_σ of S for which $\theta[\tau_\sigma+\Delta](0,\Omega)$ vanish at Ω_i. The cardinality of this subset is 14, we denote its element by $\tau_1,\dots,\tau_{14}$.

(c) Find four characteristics D_1, D_2, D_3, D_4 in $\{\tau_1,\dots,\tau_{14}\}$ such that three of them are linearly independent but $\sum_{i=1}^{4} D_i = \mathbf{0}$.

(d) Compute λ and μ using (9). This gives the curve

$$C^{(k)} : y^3 = x(x-1)(x-\lambda)(x-\mu)$$

over $\mathbb{C}$ corresponding to $\Omega^{(k)}$.

(e) Compute the absolute invariants $j_1^{(k)}$, $j_2^{(k)}$ over $\mathbb{C}$ (cf. Section 4.1).

(3) Determine the two class polynomials

$$H_{j_i}(X) = \prod_{k=1}^{s} (X - j_i^k), \qquad i = 1, 2.$$

They are defined over $\mathbb{Q}$ and we find its denominator using the continued fraction algorithm.

(4) For each tuple $(\overline{j_1}, \overline{j_2})$ with $H_{j_i}(\overline{j}_i) \equiv 0 \bmod p$:

(a) Write down a curve $\overline{C}$ over $\mathbb{F}_p$ using, e.g., equation (3) with invariants $\overline{j_1}$, $\overline{j_2}$.

(b) Test if $J_{\overline{C}}(\mathbb{F}_p) = n_t$ for some t by choosing random divisors in the divisor class group.

Remark 12. (1) As explained in the previous subsection, the algorithm succeeds with probability $\frac{1}{2}$.

(2) The complexity of the construction method depends on the invariants of K (the class number, the embeddings of the units, the size of the Galois closure), since these invariants determine the number of isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$.

(3) The computation of theta constants is very time consuming. However, in step (2)(b) we need the theta constants only up to a low precision, because we only want to know if they vanish.

(4) It would be helpful to first apply Siegel reduction to the period matrix. Unfortunately, unlike in the case of dimension $g = 2$ [10], no Siegel reduction algorithm for dimension 3 matrices is known. At least we should try to get a good approximation to a Siegel reduced matrix. This would speed up the computation.

(5) For step (4)(b) we really need the arithmetic in the function field (resp. the divisor class group of degree zero) of the curve. Such algorithms can for example be found in [4, 7, 29].

(6) Note that all computations are only done up to some fixed precision. Hence, we do not have a rigorous mathematical proof for the claim that the resulting curve does really have complex multiplication by the given CM field. Our algorithm works under the assumption that the height of the coefficients of $H_{j_i}(X)$ are small if the discriminant of the CM field is small. In the examples given below a precision of 60 digits was sufficient.

6. Examples

In this section we present some examples.

6.1. **Curves defined over the rationals.** We first give examples of CM Picard curves which are defined over the rationals. This is not the main theme of our paper but might be of theoretical interest (cf. [36] for hyperelliptic CM curves of genus 2 defined over $\mathbb{Q}$).

If the curve is defined over the rationals, the CM field has to be a Galois extension of $\mathbb{Q}$ ([32, Proposition 5.17 (5)]). There are precisely five sextic normal CM fields with class number one containing $\mathbb{Q}(\zeta_3)$ (see [39]). For all fields we get a Picard curve defined over $\mathbb{Q}$. For each example we give one model of the curve representing the isomorphism class over $\mathbb{C}$.

(1) Let $K = K_0^1(\zeta_3)$ where K_0^1 is given by $y^3 - 3y - 1$. Note that $K = \mathbb{Q}(\zeta_9)$. This CM field leads to the curve
$$C_1 : y^3 = x^4 - x$$
whose Jacobian has CM by $\mathbb{Z}[\zeta_9]$.

(2) Let $K = K_0^2(\zeta_3)$ where K_0^2 is given by $y^3 - y^2 - 2y + 1$. We find the invariants
$$j_1 = \frac{g_3^2}{g_2^3} = \frac{-2^3}{7^2} \quad \text{and} \quad j_2 = \frac{g_4}{g_2^2} = \frac{-1}{7 \cdot 2^2}.$$
The curve is given by
$$C_2 : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 x - 7^3.$$

(3) Let $K_0^3(\zeta_3)$ where K_0^3 is given by $y^3 - y^2 - 4y - 1$. The invariants are
$$j_1 = \frac{-2^3 47^2 5^2}{7^6 \cdot 13} \quad \text{and} \quad j_2 = \frac{-31 \cdot 5^2}{2^2 7^4}$$
and we get the curve
$$C_3 : y^3 = x^4 - 13 \cdot 2 \cdot 7^2 x^2 + 2^3 \cdot 13 \cdot 5 \cdot 47x - 5^2 \cdot 31 \cdot 13^2.$$

(4) Let $K = K_0^4(\zeta_3)$ where K_0 is given by $y^3 + y^2 - 10y - 8$. The invariants are
$$j_1 = \frac{-2^{19} \cdot 47^2}{7^3 \cdot 31 \cdot 73^3} \quad \text{and} \quad j_2 = \frac{-11593}{73^2 \cdot 7 \cdot 2^2}.$$
The curve is given by
$$C_4 : y^3 = x^4 - 73 \cdot 7 \cdot 2 \cdot 31x^2 + 2^{11} \cdot 47 \cdot 31x - 7 \cdot 31^2 \cdot 11593.$$

(5) Let $K = K_0^5(\zeta_3)$ where K_0 is given by $y^3 - y^2 - 14y - 8$. The invariants are
$$j_1 = \frac{-2^{11} 11^2 \cdot 41^2 \cdot 59^2}{7^3 43^2 223^3} \quad \text{and} \quad j_2 = \frac{-11^2 \cdot 419 \cdot 431}{2^2 \cdot 7^2 \cdot 43 \cdot 223^2}.$$
We find the curve
$$C_5 : y^3 = x^4 - 2 \cdot 7 \cdot 223 \cdot 43^2 x^2 + 2^7 \cdot 11 \cdot 41 \cdot 43^2 \cdot 59x - 11^2 \cdot 43^3 \cdot 419 \cdot 431.$$

Note that all three curves given in (2)–(4) are of the form $y^3 = f(x)$ where $f(x) = (x - \lambda)g(x)$ with g a polynomial of degree three whose roots lie in the real subfield K_0. We have the following lemma:

Lemma 13. *Let $K = K_0(\zeta_3)$ be a Galois CM field of degree 6 whose class number is equal to one and such that $|U^+/U_1| = 1$. Then there exists a Picard curve $C : y^3 = f(x)$ over $\mathbb{Q}$ such that $\mathrm{End}(J_C) \simeq \mathcal{O}_K$ and all roots of f lie in K.*

Proof. First, by the discussion following Theorem 2 we can easily check that up to isomorphism there is only one principally polarized abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Hence, the field of moduli of A is equal to $\mathbb{Q}$. The j-invariants of the corresponding Picard curve lie in $\mathbb{Q}$ and the curve itself can be defined over $\mathbb{Q}$.

The roots of f correspond to the fixed points $P_1, \ldots, P_4$ of C under the automorphism $\varrho : (x, y) \mapsto (x, \zeta_3 y)$. The images $\alpha(P_i)$ under the embedding α of C into its Jacobian J_C span the subgroup $J_C[1 - \zeta_3]$.

Let $V = J_C/\mathrm{Aut(J_C)}$ be the Kummer variety and let $h : J_C \to V$ be the Kummer map. Both are defined over $\mathbb{Q}$ ([31, Section I.4.4]). Let (K, Φ) be the CM type of A. Then Φ is primitive and $K = K^*$, since K abelian.

The field extension $K(h(J_C[1 - \zeta_3]))$ is a class field of K. It corresponds to the class group

$$\{\mathfrak{B} \in I_K : \mathfrak{B}^{\psi_1}\mathfrak{B}^{\psi_2}\mathfrak{B}^{\psi_3} = (\beta), \beta\overline{\beta} = N_{K/\mathbb{Q}}(\mathfrak{B}), \beta \equiv 1 \bmod (1 - \zeta_3)\}. \tag{11}$$

where $(K, \Psi) = (K, \{\psi_1, \psi_2, \psi_3\})$ is the reflex type ([31, Chapter IV, Section 17]).

Let $\mathfrak{B}$ be an ideal in K. Since the class number h_K of K is equal to 1, $\mathfrak{B} = (\pi)$ for some $\pi \in K$. Write $\pi = \pi_1\pi_2$ where $\pi_1 \in K_0$ and $\pi_2 \in \mathbb{Q}(\zeta_3)$. Set $\beta = \pi^{\psi_1}\pi^{\psi_2}\pi^{\psi_3}$. Then $\beta = N_{K_0/\mathbb{Q}}(\pi_1)N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\pi_2)\pi_2 \in \mathbb{Q}(\zeta_3)$ and after multiplying β by a root of unity, we may assume $\beta \equiv 1 \bmod (1 - \zeta_3)$ and $\beta\overline{\beta} = N_{K/\mathbb{Q}}(\pi)$. Thus $K(h(J_C[1 - \zeta_3])) = K$.

Assume now that P_i is defined over some number field M. We may assume M/K Galois by replacing M by its Galois closure and set $G = \mathrm{Gal}(M/K)$. For $\sigma \in G$, $\sigma(P_i)$ is also a ramification point of C.

Now consider $\beta(P_i)$, $\beta(\sigma(P_i)) \in J_C$. Since h and $h(\beta(P_i))$ are defined over K,

$$h(\sigma(\beta(P_i))) = \sigma(h(\beta(P_i))) = h(\beta(P_i)).$$

By the property of the Kummer map, there exists an automorphism $\mu \in \mathrm{Aut}(J_C)$ such that $\sigma(\beta(P_i)) = \mu\beta(P_i)$ but this implies $\sigma = \mathrm{id}$. Hence, P_i is defined over K. □

Suppose J_C is a Jacobian defined over $\mathbb{F}_p$ with complex multiplication by the maximal order in a CM field as described in Lemma 13. Then, p splits completely in K and the group order $\#J_C(\mathbb{F}_p)$ is divisible by 27.

6.2. **Curves over finite field.** There are two possibilities to get a curve over $\mathbb{F}_p$.

6.2.1. *Reduction of the global model.* Choose a curve C defined over $\mathbb{Q}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ for some given CM field K and reduce it modulo a suitable prime p.

(1) Take the prime number $p = 1152921504606861907 = w\overline{w}$, $w \in \mathcal{O}_K$, and the curve $C_2/\mathbb{Q}$ from the previous section. It has group order

$$153249553857085525822048394493236312246944134161854448 1=3^3 \cdot q_{\mathrm{prime}}$$

modulo p.

(2) Take the prime $p = 1152921504606848023$ and the curve $C_3/\mathbb{Q}$. We obtain the group order

$$153249554398685759762676919128449446817842260239324563 3=3^3 \cdot q_{\text{prime}}.$$

Both curves are suitable for cryptographic applications, since q_{prime} has 52, resp. 54, decimal digits.

6.2.2. *Computation of the curve from its invariants.* We now present some example for the algorithm given in Section 5.

(1) We take the CM field $K = K_0(\zeta_3)$ where K_0 is given by $y^3 - y^2 - 3y + 1$. The prime $p = 1152921504606850963$ splits completely in $K/\mathbb{Q}$. One of the group orders corresponding to $\mathcal{O}_K$ and p is equal to

$$n=n(p,\mathcal{O}_K)=153249554324503588785833863803355280361284479904691594 9$$

which is of the form $27 \cdot q_{\text{prime}}$ where q_{prime} has 53 decimal digits.

We now apply the construction algorithm with input K, p and n.

The CM field K has class number one and is non-normal. We get three isomorphism classes of principally polarized abelian varieties defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$.

The class polynomials for j_1 and j_2 are given by

$$\begin{aligned} H_1(x) = \;& 12136871902141x^3 + 7414575044352x^2 \\ & +1237453206528x + 31310028800, \\ H_2(x) = \;& 33800087104x^3 + 1389314640x^2 - 439574100x - 26755625. \end{aligned}$$

For $H_1(x) \bmod p$, resp. $H_2(x) \bmod p$, we find the roots

$$\overline{j_1} = 1047392199222542445 \quad \text{and} \quad \overline{j_2} = 421995974217783139.$$

The corresponding curve over $\mathbb{F}_p$ is given by the equation

$$y^3 = z^4 + z^2 - 949958165379570266z - 730925530389067824.$$

(2) We choose the CM field $K = K_0(\zeta_3)$ where K_0 is given by $y^3 - y^2 - 4y + 1$. The prime $p = 1152921504606848077$ splits completely in $K/\mathbb{Q}$. One of the group orders corresponding to $\mathcal{O}_K$ is equal to

$$n=n(p,\mathcal{O}_K)=153249554349395443457383034391618067616796421331749166 1$$

which is of the form $9 \cdot q_{\text{prime}}$ where q_{prime} has 53 decimal digits.

We have $h_K = 1$ and K is non-normal. Again we get three isomorphism classes over $\mathbb{C}$. The class polynomials are given by

$$H_1(x) = 943427331x^3 + 2809491048x^2 + 641981504x - 34877952$$

and

$$H_2(x) = 167340096x^3 + 50179920x^2 - 20073524x - 1971081.$$

The polynomials $H_1(X)$, resp. $H_2(X)$, have roots

$$\overline{j_1} = 712939366860039460 \quad \text{and} \quad \overline{j_2} = 913313516550283314$$

in $\mathbb{F}_p$. The corresponding curve over $\mathbb{F}_p$ is given by the equation

$$y^3 = z^4 + 2z^2 - 696757215341552432z - 607007046380386391.$$

It has the desired group order n.

7. Appendix

7.1. **The computation of U^+/U_1.** Fix an embedding σ_1 of K_0 into $\mathbb{C}$ and denote by σ_2, σ_3 the two other embeddings. For $\alpha \in \mathcal{O}_{K_0}$ with $\sigma_1(\alpha) > 0$ we define the **embedding type** equal to

1. if α is totally positive,
2. if $\sigma_2(\alpha) < 0$ and $\sigma_3(\alpha) > 0$,
3. if $\sigma_2(\alpha) > 0$ and $\sigma_3(\alpha) < 0$,
4. if $\sigma_2(\alpha) < 0$ and $\sigma_3(\alpha) < 0$.

Let U_K be the set of units in $\mathcal{O}_K$ generated by a root of unity μ and the two fundamental units ν_1 and ν_2 and let U_{K_0} be the set of units in $\mathcal{O}_{K_0}$ with fundamental units δ_1, δ_2 chosen such that $\sigma_1(\delta_1) > 0$ and $\sigma_1(\delta_2) > 0$.

As before, the subgroup U^+ denotes the totally positive units and the subgroup of U^+ of elements of the form $\varepsilon\overline{\varepsilon}$ for some $\varepsilon \in U_K$ is denoted by U_1.

We first compute the free generators u_1, u_2 of U^+.

Case 1. Both generators of U_{K_0} are totally positive. Set $u_1 := \delta_1$ and $u_2 := \delta_2$.

Case 2. If δ_1 is totally positive but δ_2 is not, set $u_1 := \delta_1$ and $u_2 := \delta_2^2$ (and vice versa).

Case 3. If δ_1, δ_2 are both not totally positive but have the same embedding type, set $u_1 := \delta_1\delta_2$ and $u_2 := \delta_2^2$.

Case 4. If δ_1, δ_2 are both not totally positive and have different embedding type, set $u_1 := \delta_1^2$ and $u_2 := \delta_2^2$.

We next want to determine U^+/U_1. Suppose the complex conjugates of v_1 and v_2 are given by $\overline{v_1} = v_1^{e_{11}} v_2^{e_{12}}$ and $\overline{v_2} = v_1^{e_{21}} v_2^{e_{22}}$. To test whether an element $\varepsilon \in U_{K_0}$ is a unit in K, we search for $k_1, k_2 \in \mathbb{Z}$ such that $\varepsilon = v_1^{k_1}\overline{v_1}^{k_1} v_2^{k_2}\overline{v_2}^{k_2} = v_1^{k_1(1+e_{11})} v_2^{k_1 e_{12}} v_1^{k_2 e_{21}} v_2^{k_2(1+e_{22})}$. This is just linear algebra.

In Case 4, $U^+/U_1 = \{1\}$. In the second and third case, we get $U^+/U_1 = \{1\}$, resp. $\{1, u_1\}$, depending on whether $u_1 \in U_1$ or not. In the first case,

$$|U^+/U_1| = \begin{cases} 1 & \text{if } u_1, u_2 \in U_1, \\ 2 & \text{if precisely one of the elements } u_1,\ u_2 \text{ or } u_1u_2 \text{ is in } U_1, \\ 4 & \text{if } u_1,\ u_2 \text{ and } u_1u_2 \text{ are not in } U_1. \end{cases}$$

7.2. **Skew-symmetric matrices and Riemann forms.** We show how to compute Frobenius bases for Riemann forms using an algorithm described in [23].

A **skew-symmetric** matrix of dimension $2n$ is a $2n \times 2n$ matrix $(a_{ij})_{i,j}$ with $a_{ij} = -a_{ji}$. In particular, $a_{ii} = 0$ for all i.

Let V be a complex vector space of dimension n and let D be a lattice of full dimension. A **Riemann form** E on V with respect to D is a $\mathbb{R}$-valued form $E : V \times V \to \mathbb{R}$ satisfying the following conditions:

(1) The form E is alternating.
(2) It takes integral values on $D \times D$.
(3) The form $(x, y) \mapsto E(ix, y)$ is positive definite.

Suppose we have given a basis $e_1, \ldots, e_{2n}$ of D. The corresponding $2n$-dimensional matrix $(E(e_i, e_j))_{i,j}$ has integer entries and is skew-symmetric.

It is a well-known fact (see, e.g., [16, p. 90]) that there exists a basis $e'_1, \ldots, e'_{2n}$ of D such that $(E(e'_i, e'_j))_{i,j}$ is of the form

$$\begin{pmatrix} & & & & d_1 & 0 & \ldots & 0 \\ & & & & 0 & d_2 & \ldots & 0 \\ & & \mathbf{0}_n & & \ldots & & & \\ & & & & 0 & \ldots & 0 & d_n \\ -d_1 & 0 & \ldots & 0 & & & & \\ 0 & -d_2 & \ldots & 0 & & & & \\ \ldots & & & & & \mathbf{0}_n & & \\ 0 & \ldots & 0 & -d_n & & & & \end{pmatrix}.$$

Such a basis is called a **Frobenius basis** for D.

We now describe an algorithm which, given a basis $e_1, \ldots, e_{2n}$ for D and the matrix $(E(e_i, e_j))_{i,j}$, computes a Frobenius basis $e'_1, \ldots, e'_{2n}$ for D.

For simplicity we now denote $(E(e_i, e_j))_{i,j}$ by A.

For the algorithm we mainly have to add multiples of a row (column) to another row (column) and we have to be able to exchange rows (columns).

Suppose we would like to interchange the column (row) a_i with a_j where $i < j$. The operation on the basis is given by the n-dimensional matrix B, which is up to interchanging the i-th and j-th column the identity matrix. We have $A_{\text{new}} = B^T A_{\text{alt}} B$.

Suppose now we would like to add a k-th multiple of the i-th row (column) to the j-th row (column). The operation on the basis is given by $B = E_n + kI_{ij}$ where I_{ij} denotes the corresponding elementary matrix and E_n is the n-dimensional identity matrix..

The transformation matrix at the end of the algorithm is just the product of the transformation matrices of the single steps.

Algorithm for computing a Frobenius basis

Input: A basis $\{e_1, \ldots, e_{2n}\}$ and the alternating matrix $A = (a_{i,j})_{i,j} := (E(e_i, e_j))_{i,j}$ of the non-degenerate Riemann form E

Output: A Frobenius basis for E

(1) $n :=$ Rank(A); $T := E_n$;
(2) $m := 1$;
(3) WHILE $m \leq n - 2$
  (a) FOR $i := m$ to $n - 1$
    (i) IF $a_{i,i+1} = 0$
    Exchange columns such that $a_{i,i+1} \neq 0$.
    ENDIF;
    (ii) $d := \gcd(a_{i,i+1}, \ldots, a_{i,n}) = r_{i+1}a_{i,i+1} + \ldots + r_n a_{i,n}$
    with $\gcd(r_{i+1}, \ldots, r_n) = 1$;
    (iii) Find a transformation matrix T' of dimension n such that T' is equal to the identity for the first i columns and rows and that the $(n - i)$ times $(n - i)$ submatrix given by the entries $t'_{s,t}$, $i + 1 \leq s, t \leq n$, has determinant 1 and $t'_{i+1,t} = r_t$ (see [28, p. 178]).
    (iv) Compute $A_{\text{new}} = (T')^t A_{\text{alt}} T'$ and set $T := T' \cdot T$.
    (v) FOR $j := i + 2$ to n
    $A[j] := A[j] - a_{i,j}/a_{i,i+1} A[i + 1]$;

Compute the corresponding transformation matrix T' and set $T := T' \cdot T$.
ENDFOR
ENDFOR
(b) IF $a_{m,m+1}$ does not divide all elements in A
(i) $A[m] := \sum_{k=m+1}^{n} A[k]$;
(ii) Compute the corresponding transformation matrix T' and set $T := T' \cdot T$.
ELSE
(i) $A[m+2] := A[m+2] + a_{m+1,m+2}/a_{m,m+1}A[m]$; $m := m+2$;
(ii) Compute the corresponding transformation matrix T' and set $T := T' \cdot T$.
ENDIF
ENDWHILE
(4) Apply suitable permutation to the set of rows and adjust T.
(5) return T;

References

[1] S. Arita. Construction of secure C_{ab} curves using modular curves. *Algorithmic number theory (Leiden, 2000), LNCS 1838*, pages 113–126, 2000. MR2002f:11067
[2] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. *Unpublished manuscript*, 1991.
[3] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993. MR93m:11136
[4] M. Bauer. The arithmetic of certain cubic function fields. *Math. Comp.*, 73:387–413, 2003.
[5] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. User's guide to pari-gp. 2000.
[6] I. Dolgachev and D. Ortland. Point sets in projective spaces and theta functions. *Asterisque*, 165, 1985. MR90i:14009
[7] S. Galbraith, S.M. Paulus, and N. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71(237):393–405, 2002. MR2002h:14102
[8] P. Gaudry. An algorithm for solving the discrete logarithm problem on hyperelliptic curves. *Eurocrypt 2000, LNCS 1807*, Springer, pages 19–34, 2000.
[9] P. Gaudry and N. Gurel. An extension of Kedlaya's algorithm to superelliptic curves. *Asiacrypt 2001, LNCS 2248,* Springer, pages 480–494, 2001. MR2003h:11159
[10] E. Gottschling. Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades. *Math. Ann.*, 138:103–124, 1959. MR21:5748
[11] R. Hartshorne. Algebraic geometry. *Springer*, 1977. MR57:3116
[12] R.-P. Holzapfel. The ball and some Hilbert problems. *Birkhäuser*, 1995. MR97g:11059
[13] T. Honda. Isogeny classes of abelian varieties over finite fields. J. *Math. Soc. Japan*, 20:83–95, 1968. MR37:5216
[14] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987. MR88b:94017
[15] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989. MR90k:11165
[16] S. Lang. *Introduction to Algebraic and Abelian Functions*. Springer, 1982. MR84m:14032
[17] S. Lang. *Complex Multiplication*. Springer, 1983. MR85f:11042
[18] H. Lange and Ch. Birkenhake. *Complex Abelian varieties*. Springer, 1982.
[19] MAGMA. http://magma.maths.usyd.edu.au/magma/. *University of Sydney*, 2002.
[20] V. S. Miller. The use of elliptic curves in cryptography. *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985), Springer, Berlin LNCS*, 218:417–426, 1986. MR88b:68040
[21] J.-S. Milne. Jacobian varieties. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer, 1986.
[22] D. Mumford. *Tata Lectures on Theta I*. Birkhäuser, 1983. MR85h:14026
[23] M. Newman. *Integral matrices*. Pure and applied mathematics, Vol. 45, Academic Press, New York-London, 1972. MR49:5038

[24] F. Oort and K. Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math*, 20:377-381, 1973. MR51:520
[25] E. Picard. Sur les fonctions de deux variables indépendantes analogues aux fonctions modulaires. *Acta math.*, 2:114-135, 1883.
[26] E. Picard. Sur les formes quadratiques ternaire indéfinies et sur les fonctions hyperfuchsiennes, *Acta math.*, 5:121-182, 1884.
[27] S. Pohlig and M. Hellmann. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inform. Theory*, IT-24:106–110, 1978. MR58:4617
[28] E. Pohst and H. Zassenhaus. *Algorithmic Number Theory*. Cambridge University Press, 1989. MR92b:11074
[29] E. Reinaldo-Barreiro, J. Estrada-Sarlabois, and J.P. Cherdieu. Efficient reduction on the Jacobian variety of Picard curves. *Coding theory, cryptography and related areas (Guanajuato, 1998)*, Springer, pages 13–28, 2000. MR2001f:14057
[30] H. Shiga. On the representation of the Picard modular function by θ constants i-ii. *Publ. RIMS, Kyoto Univ.*, 24(3):311–360, 1988. MR89k:11036
[31] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Princeton University Press, revised edition, 1998. MR99e:11076
[32] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971. MR47:3318
[33] C.L. Siegel. *Topics in Complex Function Theory. Vol. II*. John Wiley and Sons, 1972
[34] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
[35] J. Tate. Classes d'isogénie des variétès abéliennes sur un corps fini (d'après T. Honda). *Seminaire Bourbaki, Soc. Math. France.*, 352, 95-110. 1968
[36] P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68, 1999. MR99c:11079
[37] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72:435–458, 2003. MR2003i:14029
[38] A. Weng. A class of hyperelliptic CM-curves of genus three. *Journal of the Ramanujan Mathematical Society* 16, 4:339–372, 2001. MR2002k:11099
[39] K. Yamamura. On unramified Galois extensions of real quadratic number fields. *Osaka J. Math.* 23, 471–486, 1986. MR88a:11112

Institut für Algebra und Geometrie, Johann Wolfgang Goethe-Universität Frankfurt, Robert-Mayer-Str. 10, D-60054 Frankfurt am Main, Germany
E-mail address: kkoike@math.uni-frankfurt.de

Johannes Gutenberg Universität, Fachbereich Mathematik, Staudinger Weg 9, D-55128 Mainz, Germany
E-mail address: weng@mathematik.uni-mainz.de