Canad. J. Math. Vol. 72 (2), 2020 pp. 480–504
http://dx.doi.org/10.4153/S0008414X18000111

Primes Dividing Invariants of CM Picard Curves

Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng

Abstract. We give a bound on the primes dividing the denominators of invariants of Picard curves of genus 3 with complex multiplication. Unlike earlier bounds in genus 2 and 3, our bound is based, not on bad reduction of curves, but on a very explicit type of good reduction. This approach simultaneously yields a simplification of the proof and much sharper bounds. In fact, unlike all previous bounds for genus 3, our bound is sharp enough for use in explicit constructions of Picard curves.

1 Introduction

The *Hilbert class polynomial* of an imaginary quadratic field K is the polynomial whose roots are the j-invariants of the elliptic curves E with endomorphism ring isomorphic to the maximal order $\mathcal{O}_K$. Its roots generate the Hilbert class field and are used for constructing elliptic curves with prescribed order, which are used in cryptography.

The Hilbert class polynomial has integer coefficients, so in order to compute it, it suffices to numerically approximate its coefficients up to the decimal point. These ideas can be generalized to curves of genus g as long as their Jacobians have *complex multiplication* (CM). The imaginary quadratic field needs to be replaced by a *CM field* K of degree $2g$, that is, a totally imaginary quadratic extension of a totally real number field of degree g, and we consider curves whose Jacobian has endomorphism ring isomorphic to $\mathcal{O}_K$.

Using suitable invariants for curves of genus g, this gives rise to *class polynomials*, whose coefficients are rational, but not necessarily integral. Computational methods for numerically approximating these polynomials are known for $g \leq 3$ [1–3, 8, 9, 13, 16, 18, 25, 27, 28].

For the efficiency of the methods, as well as a proof of their output, and a theoretical understanding of the types of S-integers created with such constructions, we need to know the denominators of the coefficients of these polynomials.

For the case $g = 2$, these denominators are now understood, thanks to the work of Bruinier, Goren, Lauter, Viray, and Yang [7, 10, 11, 19]. The denominators in that case are effectively computable products of powers of small primes, which have been used for computing and proving correctness of CM curves of genus two [6].

Received by the editors February 4, 2018; revised September 15, 2018.
Published online on Cambridge Core May 7, 2019.
Author E. L. G. was partially supported by a project PEPS-Jeunes Chercheur-e-s - 2017. Author P. K. was partially supported by DFG priority project SPP 1489.
AMS subject classification: **14H45,** 14K22, 11H06, 14G50, 14H40, 14Q05.
Keywords: Picard curve, curve invariant, complex multiplciation, Hilbert class polynomial, bad reduction.

In general for $g = 3$, it is expected [13, §4] that such a result does not hold. However, for the specific case of hyperelliptic curves ($y^2 = x^8 + \cdots$), a bound on the primes dividing the denominators of invariants is given in [14]. Its proof also works for Picard curves ($y^3 = x^4 + \cdots$), except for a technical conjecture in [14], which is a work in progress. The bound in [14] is unfortunately too large to be practical.

All bounds mentioned so far are based on the fact that primes dividing the denominators of invariants are primes of bad reduction. The difficulty that makes the bound of [14] so large is that just knowing bad reduction of the curve does not give much information on the endomorphism structure of the reduction of the Jacobian.

In this paper we propose an alternative set of invariants for Picard curves. With that set of invariants, the primes dividing the denominators are primes of a certain very explicit type of reduction (Lemma 3.1).

We use the embedding of $\mathcal{O}_K$ into the endomorphism ring of the reduction of the Jacobian ($\mathrm{Jac}(C)$ modulo $\mathfrak{p}$) to get a contradiction for large p. We get matrices whose entries are quaternion algebra elements. These quaternion algebra elements are forced to commute when p gets very large [10, 14]. Our explicit type of reduction allows us to prove commutativity directly, so we do not need to assume that p is very large in our proofs.

This drastically reduces the final bound on p (Theorem 2.2). In fact, we get a formula for a small set S of small primes such that the denominators are S-units (Theorem 9.1). We also conjecture a bound on the exponents, yielding a formula for a denominator that is small enough for practical computation (Conjecture 9.2). We made a SageMath implementation of our bounds (available online [15]) and give numerical examples in Section 10.

2 Picard Curve, Invariants, and Statement of the Main Theorem

In this section we introduce Picard curves, a new set of invariants of Picard curves, and the basic concepts of complex multiplication. We also state the main theorem and give an overview of the proof.

2.1 Picard Curves

Let L be a field of characteristic not 2 or 3. A *Picard curve* of genus 3 over L is a smooth, projective, plane curve given by an equation of the form

$$C : y^3 = x^4 + ax^2 + bx + c, \tag{2.1}$$

where $a, b, c \in L$. Suppose that L contains a primitive third root of unity ζ_3. The automorphism group of C then contains $\rho\colon (x, y) \mapsto (x, \zeta_3 y)$ of order 3. The push-forward ρ_* of this automorphism is an automorphism of the Jacobian $J = \mathrm{Jac}(C)$, and hence is a primitive third root of unity in the endomorphism ring. By abuse of notation, we denote $\rho_* \in \mathrm{End}(J)$ also by ζ_3.

Two Picard curves $C : y^3 = x^4 + ax^2 + bx + c$ and $C' : y^3 = x^4 + a'x^2 + b'x + c'$ over a field L of characteristic not dividing 6 are isomorphic over L if and only if there

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

exists a $\lambda \in L^*$ with

$$\lambda^6 a = a', \qquad \lambda^9 b = b', \qquad \lambda^{12} c = c'. \tag{2.2}$$

2.2 Complex Multiplication

Let C be a Picard curve. We say that C or its Jacobian $J = \mathrm{Jac}(C)$ has *complex multiplication* (CM) if there is a number field K of degree 6 and an embedding $\iota\colon K \to \mathrm{End}(J) \otimes \mathbb{Q}$. Henceforth, assume that this is the case, and let K and ι be as above. We say that C and J have *CM by the order* $\mathcal{O} = \iota^{-1}(\mathrm{End}(J)) \subset K$.

We say that J has *primitive CM* if the embedding ι gives an isomorphism from K to the endomorphism algebra $\mathrm{End}(J_{\overline{L}}) \otimes \mathbb{Q}$ of J over the algebraic closure of L. If $\mathrm{char}(L) = 0$ and J has CM, then after extending L, the induced representation on the tangent space is isomorphic to a product of embeddings of K into L. The set Φ of such embeddings is called the *CM type* of the map $K \to \mathrm{End}(J) \otimes \mathbb{Q}$. It is known that if J has primitive CM if and only if K is a CM field and the CM type is *primitive*, that is, if and only if for every CM subfield $K_1 \subsetneq K$, the restriction of Φ to K_1 is not a CM type [17, §1.3.5].

Note that if J has primitive CM by $\mathcal{O}$, then the endomorphism ζ_3 of Section 2.1 is (via ι) a primitive third root of unity in $\mathcal{O}$. Conversely, if a smooth curve of genus 3 has primitive CM by an order containing a primitive third root of unity, then the curve is a Picard curve (this is stated in the case of maximal orders [16, Lemma 1], though the final sentence of the proof is wrong and needs to be replaced by [12, Lemma 7.3 and the paragraph above it]; the proof does not use that the order is maximal, only that the third root of unity is in the order).

This allowed Koike and Weng [16] to construct genus-three Picard curves with CM by orders in fields of the form $F(\zeta_3)$ for a totally real cubic field F and a third root of unity ζ_3, just as one can construct elliptic curves with CM by orders in imaginary quadratic fields.

2.3 Invariants of Picard Curves

A *homogeneous Picard curve invariant* is a weighted homogeneous polynomial $I \in \mathbb{Z}[a, b, c]$ where a, b, c are formal polynomial variables of weights 2, 3, 4, respectively. For a model as in (2.1) of a Picard curve C over a field L, we get the value $I(C) \in L$ by evaluating I in the coefficients of (2.1).

For example, we have the invariant

$$\Delta = -4a^3b^2 + 16a^4c - 27b^4 + 144ab^2c - 128a^2c^2 + 256c^3 \tag{2.3}$$

of weight 12, and $\Delta(C)$ is non-zero for all Picard curves C, as it is the discriminant of the right-hand side of (2.1). An *absolute Picard curve invariant* is a quotient $j = u/b^\ell$, where $u \in \mathbb{Z}[a, b, c]$ has weight 3ℓ. For example, the three rational functions $j_1 = a^3/b^2$, $j_2 = ac/b^2$, and $j_3 = c^3/b^4 = j_1^{-1} j_2^3$ are absolute Picard curve invariants.

All Picard curves C with $a(C) \neq 0$ can be reconstructed up to twists from the values $j_1(C)$ and $j_2(C)$ of the invariants j_1 and j_2 as follows. Given a Picard curve C over a field L, the curve $D : y^3 = x^4 + j_1(C)x^2 + j_1(C)x + j_1(C)j_2(C)$ is isomorphic to C over the algebraic closure $\overline{L}$.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Moreover, the three invariants j_1, j_2, and j_3 generate the ring of all absolute Picard curve invariants. Indeed, an absolute Picard curve invariant is a linear combination of monomials $a^A c^C / b^B$ with $2A + 4C = 3B$, and each such monomial is a non-negative power of j_2 times a monomial with $A = 0$ or $C = 0$, which in turn is a power of j_3 or j_1.

Instead of the quotients $b^2/a^3 = 1/j_1$ and $c/a^2 = j_2/j_1$ used by Koike and Weng [16], we consider j_1, j_2, j_3 because the primes dividing the denominators of our invariants have nice properties that we can use to find good bounds for them (Lemma 3.1 and Proposition 3.3).

Remark 2.1 If C is a Picard curve of genus 3 over a number field L with primitive CM and $j = u/b^l$ is an absolute Picard curve invariant, then $b(C) \neq 0$ and $j(C) \in L$. This is because if $b(C) = 0$, then the curve C admits a non-constant morphism to an elliptic curve (formula in (3.1)) and hence its Jacobian is not simple, which gives a contradiction with having a primitive CM-type.

In particular, for every sextic CM of order $\mathcal{O}$ with $\zeta_3 \in \mathcal{O}$, the class polynomials

$$H_{\mathcal{O},1}(X) = \prod_C (X - j_1(C)), \tag{2.4}$$

$$\widehat{H}_{\mathcal{O},2}(X) = \sum_C j_2(C) \prod_{D \not\cong C} (X - j_1(D)), \tag{2.5}$$

(with sums and products ranging over the isomorphism classes of curves over $\mathbb{C}$ with primitive CM by $\mathcal{O}$; see [9]) are well defined.

2.4 Statement of the Main Result and Overview of the Proof

A weak version of our main theorem is as follows.

Theorem 2.2 *Let C be a Picard curve of genus 3 over a number field L with* $\mathrm{End}\left(\mathrm{Jac}(C)_{\bar{L}}\right)$ *isomorphic to an order $\mathcal{O}$ of a number field K of degree 6. Let K_+ be the real cubic subfield of K. Let $\mu \in \mathbb{Z} + 2\mathcal{O}$ be such that $K_+ = \mathbb{Q}(\mu)$.*

Let $j = u/b^\ell$ be an absolute Picard curve invariant. Let $\mathfrak{p}$ be a prime of L lying over a rational prime p. If $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$, *then*

$$p \leq \mathrm{tr}_{K_+/\mathbb{Q}}(\mu^2)^3 \quad \textit{and} \quad p \leq \left(1 + \frac{16}{\pi}|\Delta(\mathcal{O}_+)|^{1/2}\right)^3 < 196|\Delta(\mathcal{O}_+)|^{3/2}.$$

In Sections 3–8 we prove Theorem 2.2. We give a stronger version in Section 9. The stronger version gives an algorithm for computing a set of primes, instead of just a bound on the primes. In Section 9 we also give a conjecture about the powers to which such primes appear in the denominators of the invariants. A SageMath implementation is available online [15]. In Section 10 we give examples that show that the resulting denominator bounds are small enough for practical class polynomial computations.

The first step of the proof of Theorem 2.2 is the explicit type of reduction that is implied by the appearance of a prime $\mathfrak{p}$ in the invariant b. This type of reduction is given in Lemma 3.1. Proposition 3.3 then shows how this type of reduction

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

makes the reduction of the Jacobian decompose into a product of an elliptic curve A_1 and a principally polarized abelian surface A_2. The rest of Section 3 is the proof of Proposition 3.3.

Once we know this decomposition of the reduction $\bar{J}$ of the Jacobian $J = \mathrm{Jac}(C)$, the endomorphisms of J give rise to matrices consisting of homomorphisms between the components A_1 and A_2 of $\bar{J}$. This will make A_2 decompose further and give our endomorphisms as matrices over the endomorphism ring $\mathcal{R}$ of A_1 (see Section 4).

An important part of the earlier proofs in genus 2 and 3 [10, 14] is to force these matrices to have entries in a *field* instead of in the quaternion ring $\mathcal{R}$. This was always done by an argument from [10] that uses the fact that elements of small norm of quaternion algebras of large discriminant commute. In order to be able to use this fact, the prime p needs to be very large, which is why bounds based on that type of argument typically are very large (see [19] for an exception that is more complicated and has not yet been generalized to genus 3). In Section 5 we use the explicit endomorphism $\zeta_3 = \rho_*$ and the fact that this induces an endomorphism of A_1 and A_2 to get commutativity. This greatly simplifies our proof and drastically reduces the resulting bounds.

In Section 6 we use primitivity of the CM type, via the tangent space, to show that primes with our type of reduction divide the exponent n of the kernel of the isogeny $\bar{J} \to A_1^3$. This argument is exactly the same as in [14], hence that section is very short and is basically a reference to [14]. In genus 2 [10] such an argument is not needed; see [14, § 5] for details.

In Section 7 we bound the exponent n mentioned in the previous paragraph. For this, we need to have a well-chosen isogeny in Section 4 on which to base the exponent n, and we need to look at what happens with the polarizations (which give rise to positive definite matrices) under our isogenies. This completes the proof of the first inequality of Theorem 2.2.

Section 8 uses geometry of numbers to derive the second inequality from the first.

3 Reduction of Picard Curves

In this section we give the explicit type of reduction that follows from a prime dividing the invariant b of a Picard curve. Lemma 3.1 gives the three possible reduction types of the curve, and Proposition 3.3 shows what this implies for the decomposition of the reduction of the Jacobian.

Lemma 3.1 *Let C be a Picard curve of genus 3 over a number field L and let $\mathfrak{p} \nmid 6$ be a prime of $\mathcal{O}_L$. Let $j = u/b^\ell$ be an absolute Picard curve invariant.*

If $\mathrm{ord}_\mathfrak{p}(j(C)) < 0$, then after replacing L with an extension and C with an isomorphic curve, we are in one of the following cases.

(1) *$C : y^3 = x^4 + ax^2 + bx + 1$ with $a, b \in \mathcal{O}_L$ such that $b \equiv 0$ and $a \equiv \pm 2$ modulo $\mathfrak{p}$. The reduction of this equation (from $\mathcal{O}_L$ to $\mathcal{O}_L/\mathfrak{p}$) is the singular curve $y^3 = (x^2 \pm 1)^2$ of geometric genus 1.*

(2) *$C : y^3 = x^4 + x^2 + bx + c$ with $b, c \in \mathfrak{p}$. The reduction of this equation is the singular curve $y^3 = (x^2 + 1)x^2$ of geometric genus 2.*

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

(3) $C : y^3 = x^4 + ax^2 + bx + 1$ *with* $a, b \in \mathcal{O}_L$ *such that* $b \equiv 0$ *and* $a \not\equiv \pm 2$ *modulo* $\mathfrak{p}$. *The reduction of this equation is the smooth curve* $y^3 = x^4 + \overline{a}x^2 + 1$ *of genus* 3, *where* $\overline{a} = (a \bmod \mathfrak{p})$.

Proof Let $m_0 = \min\left\{\frac{1}{2}v(a), \frac{1}{3}v(b), \frac{1}{4}v(c)\right\}$, where $v = \mathrm{ord}_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation. By our assumption that $\mathfrak{p}$ divides the denominator of $j(C)$, this minimum is not attained by $\frac{1}{3}v(b)$.

If it is attained by $\frac{1}{4}v(c)$, then we scale the curve over $\overline{L}$ as in (2.2) so that $c = 1$. As the minimum is not attained by $\frac{1}{3}v(b)$, we get that the reduction is $y^3 = x^4 + \overline{a}x^2 + 1$, where the right-hand side has discriminant $16(\overline{a}-2)^2(\overline{a}+2)^2$. In particular, if $\overline{a} \neq \pm 2$, then we are in case (3).

If $\overline{a} = \pm 2$, then the reduction is $y^3 = (x^2 \pm 1)^2$. Let $Y = (x^2 \pm 1)/y$. Then we get $Y^3 = (x^2 \pm 1)$, that is, the curve $\overline{C}$ is birational to the elliptic curve $x^2 = Y^3 \mp 1$ with j-invariant 0.

The only remaining case is the case where the minimum is not attained by $\frac{1}{4}v(c)$. As the minimum is not attained by $\frac{1}{3}v(b)$, we find that it is only attained by $\frac{1}{2}v(a)$. Now we scale the curve so that $a = 1$. We get that the reduction is $y^3 = x^4 + x^2 = (x^2+1)x^2$. Let $Y = y/x$. Then we get $xY^3 = x^2 + 1$, which is the hyperelliptic curve $x^2 - Y^3x = -1$ of genus 2. In fact, taking $X = 2x - Y^3$, we get the hyperelliptic curve $X^2 = Y^6 - 4$. ∎

Example 1 Let $K = K_+(\zeta_3)$, where $K_+ = \mathbb{Q}[y]/(y^3 - y^2 - 4y - 1) = \mathbb{Q}(\zeta_{13})_+$ is totally real abelian of discriminant 13^2 and conductor 13. Let

$$C : y^3 = x^4 - 2 \cdot 7^2 \cdot 13x^2 + 2^3 \cdot 5 \cdot 13 \cdot 47x - 5^2 \cdot 13^2 \cdot 31.$$

The curve C was computed by Koike and Weng [16, §6.1(3)], who conjectured that its Jacobian has CM by $\mathcal{O}_K$ of primitive CM type. This curve and its reductions also appear in [5, §5.2].

We compute

$$j_1 = -\frac{7^6 \cdot 13}{2^3 \cdot 5^2 \cdot 47^2}, \quad j_2 = \frac{7^2 \cdot 13 \cdot 31}{2^5 \cdot 47^2}, \quad j_3 = -\frac{5^2 \cdot 13^2 \cdot 31^3}{2^{12} \cdot 47^4}.$$

We find that the primes in the denominators of j_1, j_2, and j_3 are 2, 5, and 47. Lemma 3.1 does not apply to the prime 2 as it divides 6. The prime 5 is of case (2) in Lemma 3.1.

The prime 47 is of case (3) in Lemma 3.1 as follows. Take an integer $r \equiv 11$ modulo 47, let $\alpha = \sqrt{r}$ and $L = \mathbb{Q}(\alpha)$. Then C is isomorphic over L to the curve given by

$$y^3 = x^4 - \alpha^6 \cdot 2 \cdot 7^2 \cdot 13x^2 + \alpha^9 \cdot 2^3 \cdot 5 \cdot 13 \cdot 47x - \alpha^{12} \cdot 5^2 \cdot 13^2 \cdot 31,$$

which modulo 47 is $C : y^3 = x^4 + 19x^2 + 1$.

Remark 3.2 We know of no examples of Picard curves with primitive CM by a sextic field that have a reduction as in Lemma 3.1 (1).

Proposition 3.3 *Let* C *be a Picard curve of genus* 3 *over a number field* L *containing a primitive third root of unity* ζ_3. *Let* $\mathfrak{p} \nmid 6$ *be a prime of* L. *Suppose that* C *is given (over* L*) by an equation as in one of the three cases of Lemma* 3.1.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Let $J = \mathrm{Jac}(C)$ be the Jacobian of C, let $\mathcal{J}$ be its Néron model over $\mathbb{Z}_{\mathfrak{p}}$ and let $\overline{J}$ be its reduction modulo $\mathfrak{p}$. Assume that J has CM or that we are in case 3 of Lemma 3.1. Recall that $\zeta_3 = \rho_*$ is a third root of unity in $\mathrm{End}(J)$; it induces endomorphisms of $\mathcal{J}$ and $\overline{J}$ that we also denote by ζ_3.

Then there are abelian subvarieties A_i (with inclusion maps $I_i\colon A_i \hookrightarrow \overline{J}$), surjective homomorphisms $s_i\colon \overline{J} \to A_i$ and endomorphisms $e_i \in \mathrm{End}(\overline{J})$ for $i \in \{1,2\}$, and an integer $d \in \{1,2\}$ such that the following hold for all $i, j \in \{1,2\}$.

(i)

$$\begin{aligned} e_1 + e_2 &= [d] \in \mathrm{End}(\overline{J}),\\ e_i^2 &= [d]e_i \in \mathrm{End}(\overline{J}),\\ e_1e_2 &= e_2e_1 = 0 \in \mathrm{End}(\overline{J}),\\ e_i^\dagger &= e_i \in \mathrm{End}(\overline{J}), \quad \text{where } {}^\dagger \text{ denotes the Rosati involution,}\\ e_i &= I_is_i \in \mathrm{End}(\overline{J}),\\ s_iI_i &= [d] \in \mathrm{End}(A_i),\\ \text{if } i \neq j, \text{ then } s_iI_j &= 0 \in \mathrm{Hom}(A_j, A_i). \end{aligned}$$

Here and later, we write simply fg for $f \circ g$ in order to keep the notation clean and concise.

(ii) *The abelian variety A_i has dimension i and we have a commutative diagram*

$$\begin{array}{ccccccc} \overline{J} & \xrightarrow{\binom{s_1}{s_2}} & A_1 \times A_2 & \xrightarrow{(I_1\ I_2)} & \overline{J} & \xrightarrow{\binom{s_1}{s_2}} & A_1 \times A_2. \\ & \searrow^{[d]} & & \searrow^{[d]} & & & \end{array}$$

(iii) *if $i \neq j$, then we have $s_i\zeta_3I_j = 0 \in \mathrm{Hom}(A_j, A_i)$.*

We prove Proposition 3.3 separately in the smooth case (Lemma 3.1 (3) and in the singular cases (Lemma 3.1 (1) and (2)). The smooth case is the main case and the proof is in Section 3.1. The proofs of the singular cases are in Section 3.2.

3.1 The Smooth Case: $y^3 = x^4 + \overline{a}x^2 + 1$

We now prove Proposition 3.3 in the smooth case (3) of Lemma 3.1, where we will see that it holds with $d = 2$. We consider the Picard curve

$$\overline{C}\colon y^3 = x^4 + \overline{a}x^2 + 1.$$

The automorphism group $\mathrm{Aut}(\overline{C})$ contains the elements $\sigma\colon (x, y) \mapsto (-x, y)$ of order 2 and $\rho = \rho_{\overline{C}}\colon (x, y) \mapsto (x, \zeta_3 y)$ of order 3.

As C has good reduction at $\mathfrak{p}$, we have $\overline{J} = \mathrm{Jac}(\overline{C})$; we associate the $\mathcal{O}_{K,\mathfrak{p}}$-scheme $\mathrm{Pic}^0(\mathcal{C})$ with C. By [4, Theorem 9.3.7], the special fiber of $\mathrm{Pic}^0(\mathcal{C})$ is $\mathrm{Jac}(\overline{C})$ and it is smooth. Finally, by [4, Theorem 9.5.1], we have that $\mathrm{Pic}^0(\mathcal{C})$ is a Néron model $\mathcal{J}$ of the Jacobian of $\mathcal{C}$. In particular, the special fiber of $\mathrm{Pic}^0(\mathcal{C})$, *i.e.*, $\mathrm{Jac}(\overline{C})$, is isomorphic to the special fiber of $\mathcal{J}$, that is, $\overline{J}$.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

The curve $\overline{C}$ is a 2-cover of the elliptic curve $E: v^2 + av = u^3 - 1$ with CM by $\mathbb{Z}[\zeta_3]$. Indeed, we have

$$\phi: \overline{C} \longrightarrow E \tag{3.1}$$
$$(x, y) \longmapsto (u, v) = (y, x^2).$$

The curve E also has an automorphism $\rho = \rho_E: (u, v) \mapsto (\zeta_3 u, v)$ of order 3, and we have $\rho_E \circ \phi = \phi \circ \rho_{\overline{C}}$, or simply

$$\rho\phi = \phi\rho. \tag{3.2}$$

For every curve morphism $f: D_1 \to D_2$, we get a push-forward morphism $f_*: \mathrm{Jac}(D_1) \to \mathrm{Jac}(D_2)$ and a pullback morphism $f^*: \mathrm{Jac}(D_2) \to \mathrm{Jac}(D_1)$. With this notation, let

$$e_1 = \phi^*\phi_*, \quad e_2 = [2] - e_1 \quad \in \mathrm{End}(\bar{J}).$$

Let A_i be the image of e_i and let s_i be defined by the commutative diagram

$$\begin{array}{ccccc} \bar{J} & \xrightarrow{s_i} & A_i & \xhookrightarrow{I_i} & \bar{J} \\ & \searrow^{e_i} & & \nearrow & \end{array}.$$

Let $d = 2$. The equality $e_1 + e_2 = 2$ is the definition of e_2. As ϕ is a 2-cover, we get $\phi_*\phi^* = [2] \in \mathrm{End}(E)$. In particular, we get $e_1^2 = \phi^*\phi_*\phi^*\phi_* = \phi^*[2]\phi_* = 2e_1$ and $e_2^2 = 4 - 4e_1 + e_1^2 = 2e_2$. We also get $e_1e_2 = e_1([2] - e_1) = 2e_1 - 2e_1 = 0$ and similarly $e_2e_1 = 0$.

By Mumford [21, pp. 327–328], if $f: D_1 \to D_2$ is a non-constant curve morphism and $(\mathrm{Jac}(D_i), \lambda_i)$ is the Jacobian of D_i with its polarization, then

$$(f_*)^\vee = \lambda_1 f^* \lambda_2^{-1} \quad \text{and} \quad \lambda_i^\vee = \lambda_i.$$

Taking duals, we also have $(f^*)^\vee = \lambda_2 f_* \lambda_1^{-1}$. In particular, we get

$$e_1^\dagger = \lambda_{\overline{C}}^{-1}(\phi^*\phi_*)^\vee \lambda_{\overline{C}} = \lambda_{\overline{C}}^{-1}(\phi_*)^\vee(\phi^*)^\vee\lambda_{\overline{C}} = \phi^*\phi_* = e_1,$$
$$e_2^\dagger = [2]^\dagger - e_1^\dagger = [2] - e_1 = e_2.$$

The identities $e_i = I_i s_i$ are the definition of s_i. To compute $s_i I_j$, we compose with the surjective map s_j and the injective map I_i. If $i = j$, then we get $I_i(s_i I_i)s_i = e_i^2 = 2e_i = I_i[2]s_i$. By surjectivity of s_j and injectivity of I_i, this gives $s_i I_i = [2]$. If $i \neq j$, then we get $I_i(s_i I_j)s_j = e_i e_j = 0 = I_i[0]s_j$, hence again by surjectivity and injectivity we get $s_i I_j = 0$. This proves (i).

Commutativity of the diagram follows from $I_1 s_1 + I_2 s_2 = e_1 + e_2 = 2$ and the formulas for $s_i I_j$. The dimension of A_1 is the dimension of E, which is 1. The commutativity of the diagram shows that $A_1 \times A_2$ has the same dimension as J, hence A_2 has dimension 2, which proves (ii).

Finally, we prove (iii). Since I_i is injective and s_j is surjective, it suffices to prove $I_i s_i \zeta_3 I_j s_j = 0$, that is, $e_i \zeta_3 e_j = 0$.

Recall $\zeta_3 = \rho_*$, and by (3.2), we have $\phi_*\rho_* = \rho_*\phi_*$. Hence we get

$$\begin{aligned} e_1\zeta_3 e_1 &= \phi^*\phi_*\rho_*\phi^*\phi_* = \phi^*\rho_*\phi_*\phi^*\phi_* = \phi^*\rho_*[2]\phi_* \\ &= \phi^*\phi_*\rho_*[2] = 2e_1\zeta_3. \end{aligned}$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

In particular, we get $e_1\zeta_3 e_2 = 2e_1\zeta_3 - 2e_1\zeta_3 = 0$.

We also have $\rho^*\rho_* = 1$, so $\zeta_3 = (\rho^*)^{-1}$. Therefore, we also have

$$\begin{aligned} e_1\zeta_3 e_1 &= \phi^*\phi_*(\rho^*)^{-1}\phi^*\phi_* = \phi^*\phi_*\phi^*(\rho^*)^{-1}\phi_* = \phi^*[2](\rho^*)^{-1}\phi_* \\ &= [2](\rho^*)^{-1}\phi^*\phi_* = 2\zeta_3 e_1. \end{aligned}$$

In particular, we get $e_2\zeta_3 e_1 = 2\zeta_3 e_1 - 2\zeta_3 e_1 = 0$. This proves Proposition 3.3 with $d = 2$ in Lemma 3.1 (3). ∎

Remark 3.4 We did not need to write A_2 as the Jacobian of an explicit curve for our work. However, for those who are interested, if $\overline{C} : y^3 = x^4 + ax^2 + 1$ with $a \neq 0, -2, 2$ in a field of characteristic not 2 or 3, then a special case by Ritzenthaler and Romagny [23, Theorem 1.1] gives $\overline{J} \sim E \times \mathrm{Jac}(H)$ with E as in Section 3.1 and

$$H : -ay^2 = (x^2 + 2x - 2) \cdot (x^4 + 4x^3 + (2a^2 - 8)x - a^2 + 4).$$

3.2 The Singular Cases

In the singular cases, by [14, Theorem 1.1], we already have a bound $p < \frac{1}{8}B^{10}$ under the hypotheses of Theorem 2.2. However, we will see that we can do better.

In this section, we prove Proposition 3.3 in the singular cases of Lemma 3.1 (1) and (2), where we will see that it holds with $d = 1$. In case (g) for $g \in \{1, 2\}$, let A_g be the Jacobian of the *smooth* model C_g of the curve of geometric genus g listed in Lemma 3.1 (g).

Since the curve C has CM, Proposition 4.2 in [5] applies, so the reduction $\overline{\mathcal{C}}$ of a stable model $\mathcal{C}$ of C is tree-like and the reduction $\overline{J}$ of its Jacobian $J = \mathrm{Jac}(C)$ is the polarized product of the Jacobians of the irreducible components of $\overline{\mathcal{C}}$.

Then by [5, Corollary 4.3], the reduction of the stable model is a union of either three smooth curves of genus 1 or a smooth curve of genus 1 and a smooth curve of genus 2. By Lemma A.1 (see also Corollary A.2), one of these curves is isomorphic to the curve C_g. We conclude that the reduction of the stable model is the union of a copy of C_g and up to two additional smooth curves of total genus $3 - g$. Let A_g be the Jacobian of C_g and let A_{3-g} be the polarized product of the Jacobians of those additional curves, so

$$\overline{J} = A_1 \times A_2 \tag{3.3}$$

as principally polarized abelian varieties.

For $i \in \{1, 2\}$, let I_i be the inclusion map of A_i into $\overline{J}$ and let s_i be the projection map of $\overline{J}$ onto A_i. Let $e_i = I_i s_i$. Then we get $s_i I_j = 0$ if $i \neq j$ and $s_i I_i = [d]$ with $d = 1$. As (3.3) is an identity of principally polarized abelian varieties, we get $e_1^\dagger = e_1$, $e_2^\dagger = e_2$, and $e_1 + e_2 = [1]$. The identities $e_i^2 = e_i$ and $e_1 e_2 = e_2 e_1 = 0$ now follow from the identities in terms of I_i and s_i, and the commutativity of the diagram follows from all the given identities. This proves (i) and (ii).

Next we prove (iii). As I_i is an injective map and s_j is a surjective one, it suffices to prove $I_i s_i \zeta_3 I_j s_j = 0$, that is, $e_i\zeta_3 e_j = 0$. By the Néron mapping property, the automorphism ρ of C uniquely extends to an automorphism of the stable model. And by the explicit equations in Lemma 3.1, it also extends to an automorphism of order 3 of

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

C_g. Let ζ_3 denote not only ρ_* on $\bar{J}$, but also ρ_* on A_g. Then we get $s_g\zeta_3 = \zeta_3 s_g$ and $\zeta_3 I_g = I_g\zeta_3$. So we get

$$e_g\zeta_3 e_g = I_g s_g \zeta_3 I_g s_g = I_g s_g I_g s_g \zeta_3 = I_g s_g \zeta_3 = \zeta_3 I_g s_g = e_g\zeta_3 = \zeta_3 e_g.$$

In particular, we get

$$e_g\zeta_3 e_{3-g} = e_g\zeta_3 - e_g\zeta_3 = 0, \quad \text{and} \quad e_{g-3}\zeta_3 e_g = \zeta_3 e_g - e_g\zeta_3 e_g = 0.$$

This proves Proposition 3.3 in cases of Lemma 3.1 (1) and (2). Case (3) was done in the previous section. ∎

4 Decomposition and Matrices

If a prime $\mathfrak{p}$ does not divide 6 and does appear in the denominator of $j(C)$, then Section 3 shows that $\bar{J}$ is isogenous (via the isogeny F_0) to a product of abelian varieties A_1 and A_2 of lower dimension. We also got much information about the isogeny F_0, and how it behaves with respect to the third root of unity $\zeta_3 = \rho_* \in \mathrm{End}(\bar{J})$ (see Proposition 3.3).

In this section we show that if J has complex multiplication, then we can use an element μ of the endomorphism ring of J to decompose A_2 further.

Just the fact that A_2 is decomposable is not enough. In order to have small and explicit bounds in the end, it is crucial that we can compute the degree of the isogeny $A_2 \to A_1 \times A_1$ in terms of elements of $\mathcal{O}$.

Suppose henceforth that we are in the situation of the hypotheses of the main theorem (Theorem 2.2). In other words, we have $\mathrm{End}(J_{\bar{L}}) = \mathcal{O}$ for an order $\mathcal{O}$ in a sextic CM field K, we have a totally real element $\mu \in \mathbb{Z} + 2\mathcal{O}\backslash\mathbb{Z}$, an absolute Picard curve invariant j, and a prime $\mathfrak{p}$ of L lying over a rational prime p such that $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$.

Suppose for now that $p \neq 2, 3$.

We get $\zeta_3 \in \mathcal{O}$ (see Section 2.2) and hence $K = K_+(\zeta_3)$ for the totally real cubic field K_+ of K.

Our goal is only to bound p, so without loss of generality we assume that all elements of $\mathrm{End}(J_{\bar{L}})$ and the isomorphisms and models of Lemma 3.1 are defined over L.

Remark 4.1 In [14], a μ is taken with $\mu^2 \in K_+$ totally negative. In our situation, we can switch between totally negative and totally positive μ^2 by replacing μ by $(2\zeta_3+1)\mu$, and the proof remains roughly the same. To make the proof as simple as possible, we will work with totally positive μ^2, that is, totally real μ.

Let $F_0 = (I_1\ I_2) \colon A_1 \times A_2 \to \bar{J}$ be the isogeny from Proposition 3.3 (ii), and let s_i and d also be as in that proposition. We get an embedding

$$\iota_0 \colon \mathrm{End}(\bar{J}) \otimes \mathbb{Q} \longrightarrow \mathrm{End}(A_1 \times A_2) \otimes \mathbb{Q},$$
$$\alpha \longmapsto F_0^{-1}\alpha F_0 = \frac{1}{d}\begin{pmatrix} s_1 & \\ & s_2 \end{pmatrix} \circ \alpha \circ (I_1\ I_2) = \frac{1}{d}\begin{pmatrix} s_1\alpha I_1 & s_1\alpha I_2 \\ s_2\alpha I_1 & s_2\alpha I_2 \end{pmatrix}$$

sending

$$\mathbb{Z} + 2\mathcal{O} \subset \mathbb{Z} + d\,\mathrm{End}(\bar{J}) \longrightarrow \mathrm{End}(A_1 \times A_2). \tag{4.1}$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Write

$$\iota_0(\mu) = \left(\begin{array}{c|c} x & y \\ \hline z & w \end{array}\right),$$

where the size of a box reflects the dimension of the domain and codomain of the homomorphism. As $\mu \in \mathbb{Z} + 2\mathcal{O}$, by (4.1) we get

$$x = \frac{1}{d} s_1 \mu I_1 \in \mathrm{End}(A_1), \qquad y = \frac{1}{d} s_1 \mu I_2 \in \mathrm{Hom}(A_2, A_1),$$
$$z = \frac{1}{d} s_2 \mu I_1 \in \mathrm{Hom}(A_1, A_2), \qquad w = \frac{1}{d} s_2 \mu I_2 \in \mathrm{End}(A_2).$$

Lemma 4.2 *We have*

$$\iota_0(2\zeta_3 + 1) = \left(\begin{array}{c|c} r_1 & 0 \\ \hline 0 & r_2 \end{array}\right),$$

where $r_i \in \mathrm{End}(A_i)$ *satisfy* $r_i^2 = -3$.

Proof The off-diagonal boxes are zero by the equalities $s_i \zeta_3 I_j = s_i I_j = 0$ of Proposition 3.3 (i, iii). This gives the shape of the matrix. As its square is -3, we get $r_i^2 = -3$. ∎

Lemma 4.3 *The homomorphism*

$$F_1 = \left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & z & wz \end{array}\right) \colon A_1 \times A_1 \times A_1 \longrightarrow A_1 \times A_2$$
$$(P, Q, R) \longmapsto (P, z(Q) + wz(R))$$

is an isogeny.

Proof It is necessary and sufficient to prove that the map $A_1 \times A_1 \to A_2$ given by $(Q, R) \mapsto z(Q) + zw(R)$ is an isogeny. But this is analogous to [14, Lemma 3.1], and the proof is identical. We only use that μ does not have degree 1 or 2 over $\mathbb{Q}$. ∎

Remark 4.4 An alternative choice of isogeny $F_1 \colon A_1^3 \to A_1 \times A_2$ is obtained by replacing wz by $z' = \frac{1}{2}(zx + wz)$. Indeed, write $\mu = i + 2j$ with $i \in \{0, 1\}$ and $j \in \mathcal{O}$. Then we get $\frac{1}{2}(\mu^2 - i) = 2(j^2 - ij) \in 2\mathcal{O}$. As z' is the lower left entry of $\iota_0(\frac{1}{2}(\mu^2 - i))$, it is in $\mathrm{Hom}(A_1, A_2)$. Then instead of F_1 use

$$\left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & z & z' \end{array}\right) \colon A_1 \times A_1 \times A_1 \longrightarrow A_1 \times A_2$$
$$(P, Q, R) \longmapsto (P, z(Q) + z'(R)).$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

This gives a bound in the end whose valuation at 2 is better, but still non-optimal. As it makes the formulas more complicated, we will not consider it further in this article, but we give this choice as an option in our SageMath implementation.

Let $\mathcal{R} = \mathrm{End}(A_1)$ and $\mathcal{B} = \mathcal{R} \otimes \mathbb{Q}$. We get an isogeny $F = F_0F_1$ and ring homomorphisms

$$\begin{aligned} \iota_1 \colon \mathrm{End}(A_1 \times A_2) &\longrightarrow \mathrm{M}_{3\times 3}(\mathcal{B}) \\ f &\longmapsto F_1^{-1} f F_1, \end{aligned}$$

and

$$\begin{aligned} \iota = \iota_1 \circ \iota_0 \colon \mathrm{End}(\bar{J}) &\longrightarrow \mathrm{M}_{3\times 3}(\mathcal{B}), \\ \alpha &\longmapsto F^{-1} \alpha F. \end{aligned}$$

Take $n \in \mathbb{Z}_{>0}$ such that

$$[n] \ker(F_1) = 0. \tag{4.2}$$

In (7.2) below, we will take a specific n.

5 Using Commutativity to Get Matrices Over a Field

In this section we use the fact that we have an explicit ζ_3 that commutes with μ in order to find that the entries of the 3×3 matrix $\iota(\mu)$ from Section 4 all lie in the same quadratic field. In the proof of the previous bounds ([10] for $g = 2$ and [5, 14] for $g = 3$), we had no such ζ_3; the proof that the entries were in a quadratic field was based instead on the fact that "small" elements of large-discriminant quaternion algebras commute, hence that argument worked only for very large primes. Because of our explicit decomposition, our proof is much simpler and our results are much sharper.

We also get various relations between the entries, which we use in Section 7 to bound the entries.

Lemma 5.1 *Let μ and ι be as in Section 4, let $\mathcal{R} = \mathrm{End}(A_1)$, and let n be as in (4.2).*

(i) *For every $\alpha \in \mathbb{Z} + 2\mathcal{O}$, the entries of the 3×3 matrix $\iota(\alpha)$ are in $\frac{1}{n}\mathcal{R}$, and the entries of the top row are in $\mathcal{R}$.*

(ii) *We have*

$$\iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & e \\ 0 & 1 & f \end{pmatrix}$$

with $x, a, b, ne, nf \in \mathcal{R}$.

(iii) *We have*

$$\iota(2\zeta_3 + 1) = \begin{pmatrix} r_1 & 0 & 0 \\ 0 & s & t \\ 0 & u & v \end{pmatrix}$$

with $r_1, ns, nt, nu, nv \in \mathcal{R}$, and $r_1^3 = -3$.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Proof Let $G\colon A_1 \times A_2 \to A_1 \times A_1 \times A_1$ be the isogeny satisfying $GF_1 = [n]$ that exists because of (4.2). Then we have

$$F_1 = \begin{pmatrix} 1 & 0 & 0 \\ \boxed{0} & \boxed{z} & \boxed{wz} \end{pmatrix} \quad \text{and} \quad F_1^{-1} = \frac{1}{n}G = \frac{1}{n}\begin{pmatrix} n & \boxed{0} \\ 0 & \boxed{g_1} \\ 0 & \boxed{g_2} \end{pmatrix}$$

for some $g_i\colon A_2 \to A_1$ satisfying $\frac{1}{n}\left(\begin{smallmatrix} g_1 \\ g_2 \end{smallmatrix}\right)(z, wz) = \left(\begin{smallmatrix} \frac{1}{0} & \frac{0}{1} \end{smallmatrix}\right)$.

For $i, j \in \{1, 2\}$, the (i, j)-entry of $\iota_0(\alpha)$ is in $\mathrm{Hom}(A_j, A_i)$. Now because of the shape of F_1 and F_1^{-1}, the matrix $\iota(\alpha) = F_1^{-1}\iota_0(\alpha)F_1$ has entries in $\frac{1}{n}\mathcal{R}$ with the entries of the top row in $\mathcal{R}$. This proves (i).

For (ii), we now only need to compute the lower left 2×2 block, so

$$\iota(\mu) = F_1^{-1}\iota_0(\mu)F_1 = \frac{1}{n}\begin{pmatrix} * & \boxed{*} \\ 0 & \boxed{g_1} \\ 0 & \boxed{g_2} \end{pmatrix}\begin{pmatrix} * & \boxed{*} \\ \boxed{z} & \boxed{w} \end{pmatrix}\begin{pmatrix} 1 & 0 & * \\ \boxed{0} & \boxed{z} & \boxed{*} \end{pmatrix}$$

$$= \begin{pmatrix} * & * & * \\ 1 & 0 & * \\ 0 & 1 & * \end{pmatrix}.$$

For (iii), we note that by Lemma 4.2 we are multiplying block-diagonal matrices as follows:

$$\iota(2\zeta_3 + 1) = F_1^{-1}\iota_0(2\zeta_3 + 1)F_1 = \begin{pmatrix} 1 & \boxed{0} \\ 0 & \boxed{*} \\ 0 & \boxed{*} \end{pmatrix}\begin{pmatrix} r_1 & \boxed{0} \\ \boxed{0} & \boxed{*} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ \boxed{0} & \boxed{*} & \boxed{*} \end{pmatrix}$$

$$= \begin{pmatrix} r_1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

■

Remark 5.2 Lemma 5.1 (ii) and its proof are analogous to Lemma 3.2 of [14] and its proof.

The following lemma is one of the things that distinguishes our proof from the proofs of earlier denominator bounds. It shows that all entries of the matrices in Lemma 5.1 commute. Contrary to the previous bounds, it shows this without assuming that small elements in large-discriminant quaternion rings commute, and hence without assuming that p is large.

Lemma 5.3 *In the notation of Lemma 5.1, we have $v = s = r_1$ and $u = t = 0$. Moreover, all of x, a, b, e, f, and all entries of $\iota(\alpha)$ for all $\alpha \in K$ are in $\mathbb{Q}(r_1)$.*

Proof As the matrices $\iota(\mu)$ and $\iota(2\zeta_3 + 1)$ commute, we have

$$\begin{pmatrix} r_1x & r_1a & r_1b \\ s & t & se + tf \\ u & v & ue + vf \end{pmatrix} = \begin{pmatrix} xr_1 & as + bu & at + bv \\ r_1 & eu & ev \\ 0 & s + fu & t + fv \end{pmatrix}.$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

We immediately read off $s = r_1$ and $u = 0$, and once we use $u = 0$, we also get $t = 0$ and $v = s$. Now $\iota(2\zeta_3 + 1)$ is r_1 times the identity matrix, hence the fact that the two matrices commute implies that all entries of the matrices commute with r_1. As r_1 is not in $\mathbb{Q}$, this implies that these entries are in the quadratic field $\mathbb{Q}(r_1)$. Finally, as μ and $2\zeta_3 + 1$ generate the field K, we get that all entries of $\iota(\alpha)$ are in $\mathbb{Q}(r_1)$. ∎

In the rest of this section, we express b, e, and f in terms of x, a, and the coefficients of the minimal polynomial of μ.

As μ is a cubic integral over $\mathbb{Z}$, we have $\mu^3 - t_1\mu^2 + a_1\mu - N = 0$, where $t_1 = \mathrm{tr}_{K_+/\mathbb{Q}}(\mu)$, $N = N_{K_+/\mathbb{Q}}(\mu)$, and a_1 are in $\mathbb{Z}$ and depend only on μ.

Lemma 5.4 *We have*

$$f = t_1 - x, \qquad e = -(a_1 + x^2 + a - t_1 x),$$
$$b = N - (x^3 - t_1 x^2 + 2xa + a_1 x - t_1 a).$$

Proof As ι is a ring homomorphism, we find that the matrix

$$M = \iota(\mu)^3 - t_1\iota(\mu)^2 + a_1\iota(\mu) - N\mathrm{Id}_{3\times 3}$$

is the zero matrix, where $\mathrm{Id}_{3\times 3}$ is the 3×3 identity matrix.

As the entries of $\iota(\mu)$ are given explicitly in terms of x, a, b, e, f in a *field* $\mathbb{Q}(r_1)$, we can easily compute M in terms of these quantities and t_1, a_1, N. The leftmost column is exactly

$$\begin{pmatrix} x^3 - t_1 x^2 + (2a + a_1)\, x - t_1 a + b - N \\ x^2 - t_1 x + a + e + a_1 \\ x + f - t_1 \end{pmatrix},$$

which proves the result. ∎

6 Tangent Spaces and Primitive CM Types

As in (4.2), let $n \in \mathbb{Z}_{>0}$ be such that $[n]\ker(F_1) = 0$. In this section, we prove the following proposition implying that in order to bound p, it suffices to find a small n. In (7.2) below, we choose a specific n.

Proposition 6.1 *For C and p as in the hypotheses of Theorem 2.2, let $n \in \mathbb{Z}_{>0}$ be such that $[n]\ker(F_1) = 0$. Then $p \le 3$ or $p \mid n$.*

Proof Suppose $p \nmid 6n$. We claim that primitivity of the CM type implies that the matrix $\iota(2\zeta_3 + 1)$ has two distinct eigenvalues.

Note that having two distinct eigenvalues contradicts the first statement of Lemma 5.3, which was the equality $\iota(2\zeta_3+1) = r_1\mathrm{Id}_{3\times 3}$. In particular, the result follows once we prove the claim.

The idea behind the claim is as follows. Note that primitivity of the CM type implies that the action of $2\zeta_3+1$ on the tangent space of J has two distinct eigenvalues. If p does not divide $6n$, then these two eigenvalues induce distinct eigenvalues for the action on the tangent space of $\bar{J}$ via F and $[2n]F^{-1}$. This proves the claim.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

In more detail, the proof of the claim is the same as the proof of [14, Proposition 5] with $\delta = 3$ and $\sqrt{-\delta} = 2\zeta_3 + 1$, except for the following changes.

- We use F as above and we use A_1 instead of E, and $2n$ instead of n. Let $G = [2n]F^{-1}$.
- Instead of [14, Proposition 4.1], use Lemma 5.3; so in particular the condition $p > \frac{1}{8}B^{10}$ is not needed.
- The reductions of $\pm\sqrt{-\delta}$ are distinct as we have $p \nmid 2\delta = 6$. This also does not need any additional bounds on p.
- The invertibility of $2n$ modulo p follows from our assumption $p \nmid 6n$ and also does not need additional bounds on p. ∎

7 Using the Polarization to Get Bounds

By Proposition 6.1, it now suffices to find a sufficiently well-bounded $n \in \mathbb{Z}_{>0}$ with $[n]\ker(F_1) = 0$. In this section, we do exactly this, using the polarization that C induces on A_1^3 via F_1. The key here is that we constructed F_1 very explicitly, and that polarizations give rise to positive definite matrices. Compared to [14], our matrices are a bit simpler, since in our situation we are able to prove that the entries are in a field, where [14] needs the bounds in order to prove exactly that.

Let $\lambda = F^\vee \lambda_C F$ be the polarization induced on A_1^3 by the polarization λ_C of $\bar{J}$. We identify A_1 with its dual via the natural polarization λ_{A_1}, which we sometimes leave out from the notation. Then λ can be viewed as an endomorphism of A_1^3, and the following result gives it as a matrix.

Lemma 7.1 ([14, Lemma 4.3]) *We have*

$$\lambda = \begin{pmatrix} m & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \beta^\vee & \gamma \end{pmatrix}.$$

with $m, \alpha, \gamma \in \mathbb{Z}_{>0}$, and $\beta \in \mathcal{R}$ with $\alpha\gamma - \beta\beta^\vee > 0$. Moreover, we have $m \mid 2$.

Proof Recall from just above the statement of the lemma that λ is defined as a homomorphism $A_1^3 \to (A_1^\vee)^3$ by $\lambda = F^\vee \lambda_C F$, and as an endomorphism of A_1^3 by $\lambda = (\lambda_{A_1}^{-1} \times \lambda_{A_1}^{-1} \times \lambda_{A_1}^{-1}) F^\vee \lambda_C F$. The symmetry of λ now follows from the symmetry of λ_C [22, (3), p. 190].

We now prove that the off-diagonal entries of the first row and column of λ are zero. Since $F = F_0 F_1$, we write

$$\lambda = \operatorname{diag}(\lambda_{A_1}^{-1}, \lambda_{A_1}^{-1}, \lambda_{A_1}^{-1}) F_1^\vee (I_1\ I_2)^\vee \lambda_C (I_1\ I_2) F_1, \quad \text{where } F_1^\vee = \begin{pmatrix} 1 & 0 \\ 0 & z^\vee \\ 0 & z^\vee w^\vee \end{pmatrix}.$$

To see that four entries are zero, we only look at the off-diagonal entries of the first row. This suffices by symmetry. By Proposition 3.3 (i), we get $e_1^\vee \lambda_C e_2 = \lambda_C e_1^\dagger e_2 =$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

$\lambda_C e_1 e_2 = 0$. As $e_i = I_i s_i$ and s_i is surjective, we get $I_1^\vee \lambda_C I_2 = 0$. Therefore we have

$$(I_1\, I_2)^\vee \lambda_C (I_1\, I_2) = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix},$$

and hence the off-diagonal entries of the first row of λ are zero.

From the final paragraph of Mumford [22, Application III, p. 210], we get that λ is positive definite, hence $m, \alpha, \gamma, \alpha\gamma - \beta\beta^\vee > 0$.

It remains only to prove $m \mid 2$. We have $m = I_1^\vee \lambda_C I_1$ since we defined m to be the first diagonal entry of $(I_1\, I_2)^\vee \lambda_C (I_1\, I_2)$.

Recall that by Proposition 3.3 (i) we have $e_1 = e_1^\dagger$. This implies $e_1 = \lambda_C^{-1} e_1^\vee \lambda_C$ and by $e_1 = I_1 s_1$, we get $I_1 s_1 = \lambda_C^{-1} s_1^\vee I_1^\vee \lambda_C$. Therefore, we have $\lambda_C I_1 s_1 I_1 = s_1^\vee I_1^\vee \lambda_C I_1$, hence $\lambda_C I_1[d] = s_1^\vee I_1^\vee \lambda_C I_1$. Since λ_C is an isomorphism and I_1 is injective, we get that $\ker(s_1^\vee I_1^\vee \lambda_C I_1) = A_1[d]$. Hence, $\ker(I_1^\vee \lambda_C I_1) \subseteq A_1[d]$, and we know that $m = I_1^\vee \lambda_C I_1$ is a positive integer. So we finally get $m = 1$ or 2. ∎

Since $\mu \in K_+$, it equals its complex conjugate $\overline{\mu}$. Moreover, (analogously to [5, Proposition 4.8]), we have for every $\eta \in K$,

$$\begin{aligned} \lambda^{-1} \iota(\eta)^\vee \lambda &= (F^\vee \lambda_C F)^{-1} (F^{-1} \eta F)^\vee F^\vee \lambda_C F \\ &= F^{-1} \lambda_C^{-1} \eta^\vee \lambda_C F = \iota(\eta^\dagger) = \iota(\overline{\eta}). \end{aligned}$$

Hence $\iota(\mu)^\vee \lambda = \lambda \iota(\mu)$, so that

$$\begin{pmatrix} mx^\vee & \alpha & \beta \\ ma^\vee & \beta^\vee & \gamma \\ mb^\vee & e^\vee\alpha + f^\vee\beta^\vee & e^\vee\beta + f^\vee\gamma \end{pmatrix} = \begin{pmatrix} mx & ma & mb \\ \alpha & \beta & \alpha e + \beta f \\ \beta^\vee & \gamma & \beta^\vee e + \gamma f \end{pmatrix}.$$

This tells us that

$$\begin{aligned} \alpha &= ma, && \text{hence } a \in \mathbb{Q}_{>0} \cap \mathcal{R} = \mathbb{Z}_{>0}, \\ \beta^\vee &= \beta = mb, \\ x &= x^\vee, && \text{hence } x \in \mathbb{Z}, \\ \gamma &= \alpha e + \beta f. \end{aligned} \tag{7.1}$$

Combining this with Lemma 5.4, we find explicit expressions for all entries of $\iota(\mu)$ and λ in terms of x, a, m, and the coefficients of the minimal polynomial of μ. In particular, these entries are all in $\mathbb{Z}$.

Let

$$n = \alpha\gamma - \beta\beta^\vee = m(a\gamma - mb^2) \in m\mathbb{Z}. \tag{7.2}$$

Then Lemma 7.1 and the definition of λ give

$$\begin{pmatrix} n/m & 0 & 0 \\ 0 & \gamma & -\beta \\ 0 & -\beta^\vee & \alpha \end{pmatrix} F^\vee \lambda_C F = [n],$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

so that in particular the condition $[n]\ker(F) = 0$ from (4.2) is satisfied. We have already expressed α, γ, and β in terms of x, a, m, and the coefficients of the minimal polynomial of μ. As m is 1 or 2, it suffices to bound x and a in order to bound n.

As the 3×3 matrix $\iota(\mu^2)$ over $\mathbb{Q}$ satisfies the (cubic) minimal polynomial of μ^2 over $\mathbb{Q}$, we find that its (matrix) trace is the trace of μ^2 from K_+ to $\mathbb{Q}$, which is $t_2 := t_1^2 - 2a_1$. We get

$$\begin{aligned} t_2 &= x^2 + 2a + 2e + f^2 \\ &= x^2 + 2a + \frac{2}{\alpha}\gamma - \frac{2}{\alpha}\beta f + f^2 \\ &= x^2 + 2a + \frac{2}{\alpha}\gamma - \left(\frac{\beta}{\alpha}\right)^2 + \left(\frac{\beta}{\alpha} - f\right)^2 \\ &= x^2 + 2a + \frac{\gamma}{\alpha} + \frac{n}{\alpha^2} + \left(\frac{\beta}{\alpha} - f\right)^2 \qquad (7.3) \\ &\geq x^2 + 2a. \end{aligned}$$

In particular, we get

$$|x| \leq \sqrt{t_2} \quad \text{and} \quad 0 < a \leq \frac{1}{2}(t_2 - x^2). \qquad (7.4)$$

Moreover, by (7.3), we get $n \leq t_2\alpha^2$ and $2a \leq t_2$. Then by (7.1), we obtain $n \leq t_2\alpha^2 \leq t_2 m^2 a^2 \leq t_2^3$ as $m \mid 2$. By Proposition 6.1, we have $p \leq 3$ or $p \mid n$. Hence we get the bound $p \leq \max\{3, t_2^3\}$.

Lemma 7.2 *Let μ be a totally real cubic algebraic integer, and let t_2 be the trace of μ^2. Then we have $t_2 \geq 2$.*

Proof Let a, b, c be the images of μ under the three embeddings into $\mathbb{R}$. Then $t_2 = a^2 + b^2 + c^2 \in \mathbb{Z}$. Suppose $t_2 < 2$. Then $t_2 \leq 1$ and $a^2, b^2, c^2 > 0$. Hence $|a|, |b|, |c| \in (0,1)$; so we get $|abc| \in (0,1)$. On the other hand, we have $|abc| = |N(\mu)| \in \mathbb{Z}$, which is a contradiction. ∎

Proof of the first inequality in Theorem 2.2 As stated above, we proved the inequality $p \leq \max\{3, t_2^3\}$ under the hypotheses of Theorem 2.2. As Lemma 7.2 gives $t_2^3 \geq 2^3 > 3$, we get $p \leq t_2^3$. ∎

8 Intrinsic Bounds From Geometry of Numbers

At the end of Section 7, we finished the proof of the first inequality in Theorem 2.2: $p \leq \mathrm{tr}_{K^+/\mathbb{Q}}(\mu^2)^3$. Next we show that there exists an element μ for which this right-hand side is explicitly bounded in terms of the discriminant of K^+, and hence we prove the rest of Theorem 2.2.

Let $\{\sigma_1, \sigma_2, \sigma_3\}$ be the set of the real embeddings of K_+. This gives us the map $\sigma: K_+ \to \mathbb{R}^3$ by sending y to $(\sigma_i(y))_i$. The order $\mathbb{Z} + 2\mathcal{O}_+ \subset K_+$ is a lattice of covolume $2^{3-1}|\Delta(\mathcal{O}_+)|^{1/2}$ in $\mathbb{R}^3$. Let $R = 4\pi^{-1/2}|\Delta(\mathcal{O}_+)|^{1/4} + \epsilon$ for some $\epsilon > 0$.

We choose a symmetric convex body in $\mathbb{R}^3$:

$$\mathcal{C}_R = \left\{ x \in \mathbb{R}^3 : |x_1| < 1, x_2^2 + x_3^2 < R^2 \right\}.$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

We then have $\mathrm{vol}(\mathcal{C}_R) = 2\pi R^2 > 32|\Delta(\mathcal{O}_+)|^{1/2} = 2^3\mathrm{covol}(\mathbb{Z}+2\mathcal{O}_+)$. By Minkowski's first convex body theorem [24, Theorem 10], there is a non-zero $\mu \in (\mathbb{Z}+2\mathcal{O}_+) \cap \mathcal{C}_R$. Note that μ generates K_+. If $\mu \in \mathbb{Q}$, then $\mu \in \mathbb{Z}$. But $|\mu| < 1$, so we get $\mu = 0$, which is a contradiction. Then we get $\mathrm{tr}_{K_+/\mathbb{Q}}(\mu^2) = \sum_i \sigma_i(\mu^2) \leq (1+R^2)$. Since μ is an algebraic integer in K_+, we have $\mathrm{tr}_{K_+/\mathbb{Q}}(\mu^2) \in \mathbb{Z}$. So when we let ϵ tend to 0, we get $t_2 = \mathrm{tr}_{K_+/\mathbb{Q}}(\mu^2) \leq (1+\frac{16}{\pi}|\Delta(\mathcal{O}_+)|^{1/2})$.

Since $p \leq t_2^3$ and $|\Delta(\mathcal{O}_+)| \geq 2$, we get $p \leq (1+\frac{16}{\pi}|\Delta(\mathcal{O}_+)|^{1/2})^3 < 196|\Delta(\mathcal{O}_+)|^{3/2}$. This finishes the proof of Theorem 2.2. ∎

9 Computing the Set of Primes

From the proof of Theorem 2.2, we get much more than just a bound on p as follows. Take a totally real $\mu \in \mathbb{Z}+2\mathcal{O}$. Then list all a and x satisfying the bounds of (7.4) and all $m \in \{1,2\}$. For each, compute $n = n(\mu,a,x)$ using (7.1) and (7.2). Then let N_μ be the product of the numbers $n(\mu,a,x)$. Then p divides $6N_\mu$ by Proposition 6.1. This is already much better than just a bound on p.

However, we can do even better. For each μ, a, x, m, we get a $\mathbb{Q}$-algebra homomorphism $\iota\colon K \to \mathrm{M}_{3\times 3}(\mathbb{Q}(\zeta_3))$ (given on generators in Lemma 5.1, coefficients in $\mathbb{Q}(\zeta_3)$ by Lemma 5.3, and $r_1^2 = -3$). We know by Lemmas 5.1 and 5.3 that all elements of the image of $\mathbb{Z}+2\mathcal{O}$ are matrices with entries in $\frac{1}{n}\mathbb{Z}[\zeta_3]$, with the entries of the top row in $\mathbb{Z}[\zeta_3]$. So we compute a $\mathbb{Z}$-basis of $\mathbb{Z}+2\mathcal{O}$ and throw away all triples (x,a,m) for which an element of this basis maps to a matrix that does not satisfy the integrality condition. We also throw away all triples (x,a,n) for which one of α,β,γ is non-integral or for which γ or n is non-positive. By making the set of pairs (x,a) smaller in this way, the product N_μ of the numbers $n(\mu,a,x)$ becomes much smaller.

We implemented the computation of N_μ in SageMath [26] and made the implementation available online [15].

Theorem 9.1 *Let C be a Picard curve of genus 3 over a number field L and suppose that the endomorphism ring $\mathrm{End}(J_{\overline{L}})$ of $J = \mathrm{Jac}(C)$ over the algebraic closure is isomorphic to an order $\mathcal{O}$ of a number field K of degree 6.*

Let K_+ be the real cubic subfield of K and $\mathcal{O}_+ = K_+ \cap \mathcal{O}$. Let μ be a totally real element in $\mathbb{Z}+2\mathcal{O}_+$ such that $K = \mathbb{Q}(\mu)(\zeta_3)$.

Let $j = u/b^\ell$ be an absolute Picard curve invariant. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$ lying over a rational prime p. If $\mathrm{ord}_\mathfrak{p}(j(C)) < 0$, then p divides the number $6N_\mu$ for N_μ as described in the preceding paragraphs.

Conjecture 9.2 *There are constants $s, e \in \mathbb{Q}_{>0}$ such that the following holds. Let $j = u/b^\ell$ be an absolute Picard curve invariant.*

Let $\mathcal{O}$ be an order in a sextic CM field. Let CM_K be the set of isomorphism classes of Picard curves C over $\overline{\mathbb{Q}}$ of genus 3 with $\mathrm{End}(J_{\overline{\mathbb{Q}}})$ isomorphic to $\mathcal{O}$. Let N_μ be as in Theorem 9.1.

Then for all non-archimedean valuations v of $\overline{\mathbb{Q}}$, we have

$$\sum_{C \in \mathrm{CM}_K} \max\{0, v(j(C))\} \leq \ell(v(s) + e \cdot v(N_\mu)). \tag{9.1}$$

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Remark 9.3 In fact, the examples in Section 10 suggest that when $K/\mathbb{Q}$ is Galois, the constant $e = 1/3$ suffices. The numerology supporting the factor $1/3$ is that K has three CM types up to complex conjugation which are all equivalent, so that every curve should be counted three times, but is only counted once in the left-hand side of (9.1).

To prove the conjecture, one would need to retrace our proof, but working over prime-power quotients of $\mathcal{O}_L$ instead of over the field $\mathcal{O}_L/\mathfrak{p}$. Once the conjecture is proved, our implementation of N_μ, together with an interval-arithmetic-version of Lario–Somoza [18], would give a proven algorithm for computing CM Picard curves and Picard class polynomials. In particular, it would prove the conjectured CM curves of Koike–Weng [16] and Lario–Somoza [18].

10 Examples

Finally, we take a few example curves and compare our bounds with previous bounds, and compare our invariants with previous choices.

Given a Picard curve C, let den_1 and den_3 be the denominators of the absolute invariants $j_1(C) = (a^3/b^2)(C)$ and $j_3(C) = (c^3/b^4)(C)$, respectively. Then we define the *absolute denominator* b_{abs} of C by

$$\begin{aligned} b_{\mathrm{abs}} &= \prod_{p \mid \mathrm{den}_1 \cdot \mathrm{den}_3} p^{\max\{v_p(\mathrm{den}_1)/2, v_p(\mathrm{den}_3)/4\}} \\ &= \prod_p p^{v_p(b) - \frac{1}{4}\min\{6v_p(a), 4v_p(b), 3v_p(c)\}}. \end{aligned}$$

Theorem 9.1 tells us that all primes dividing b_{abs}^4 divide $6N_\mu$. In fact, Conjecture 9.2 implies that b_{abs} divides sN_μ^e.

We define the absolute denominator a_{abs} of the Koike–Weng invariants $j_1' = b^2/a^3$ and $j_2' = c/a^2$ in the same way. In other words, let den_1' and den_2' be the denominators of $j_1'(C)$ and $j_2'(C)$, respectively. Then we define

$$a_{\mathrm{abs}} = \prod_{p \mid \mathrm{den}_1' \cdot \mathrm{den}_2'} p^{\max\{v_p(\mathrm{den}_1')/3, v_p(\mathrm{den}_2')/2\}}.$$

Let Δ be the discriminant invariant (2.3), which has weight 12. We define the invariants

$$i_1 = \frac{a^6}{\Delta}, \quad i_2 = \frac{a^3 b^2}{\Delta}, \quad i_3 = \frac{a^4 c}{\Delta}, \quad i_4 = \frac{b^4}{\Delta}, \quad i_5 = \frac{c^3}{\Delta},$$

denoted j_* in [14]. Let Δ_{abs} denote the least common multiple of the denominators of $i_1(C)$, $i_4(C)$, and $i_5(C)$ (equivalently, of all $i_*(C)$).

Let $B = \min\{\mathrm{tr}_{K_+/\mathbb{Q}}(\alpha\overline{\alpha}) : \alpha \in \mathcal{O}_K \backslash \{0\}, \overline{\alpha} = -\alpha\}$. So, as conjectured [14, Remark 1.6] that primes p of bad reduction are $< \frac{1}{8}B^{10}$ and in the case where $K/\mathbb{Q}$ is cyclic and C has CM by $\mathcal{O}_K$, it follows from [13, Proposition 4.1] that p has exactly one or three prime factors in $\mathcal{O}_K$. The number of such primes below this bound is roughly $\frac{1}{16}B^{10}/\log(\frac{1}{8}B^{10})$ by the prime number theorem and the Chebotarev density theorem. The product of them will therefore have a number of digits that is comparable to B^{10} itself.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Example 1 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - x^2 - 2x + 1)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by the maximal order $\mathcal{O}_K$ of K. See [16, 6.1(2)] and [18, 4.1.2] for a conjectural model. Its invariants are

- $i_1 = \frac{7^4}{2^6}$, $i_2 = \frac{-7^2}{2^3}$, $i_3 = \frac{-7^3}{2^8}$,
- $\Delta_{\text{abs}} = 2^{12} \approx 4.1 \cdot 10^3$, $\quad \frac{1}{8}B^{10} \approx 7.2 \cdot 10^{10}$,
- $j_1' = \frac{-2^3}{7^2}$, $j_2' = \frac{-1}{2^2 \cdot 7}$, $\quad a_{\text{abs}} = (2^3 \cdot 7^2)^{\frac{1}{2}} \approx 7.31861142004594$,
- $j_1 = \frac{-7^2}{2^3}$, $j_2 = \frac{7}{2^5}$, $\quad b_{\text{abs}} = 2^3 \approx 8$,
- $N_{-2\alpha^2+3} = (2^{28} \cdot 7 \cdot 13)^3 \approx (2.4 \cdot 10^{10})^3$.

Example 2 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - x^2 - 4x - 1)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by $\mathcal{O}_K$. See [16, 6.1(3)] and [18, 4.1.3] for a conjectural model. Its invariants are

- $i_1 = \frac{(7^6 \cdot 13)^2}{(2 \cdot 5)^6}$, $i_2 = \frac{-7^6 \cdot 13 \cdot 47^2}{2^3 \cdot 5^4}$, $i_3 = \frac{-7^8 \cdot 13^2 \cdot 31}{(2^2 \cdot 5)^4}$,
- $\Delta_{\text{abs}} = (2^2 \cdot 5)^6 \approx 6.4 \cdot 10^7$, $\quad \frac{1}{8}B^{10} \approx 2.6 \cdot 10^{13}$,
- $j_1' = \frac{-2^3 \cdot 5^2 \cdot 47^2}{7^6 \cdot 13}$, $j_2' = \frac{-5^2 \cdot 31}{(2 \cdot 7^2)^2}$, $\quad a_{\text{abs}} = (2^3 \cdot 7^6 \cdot 13)^{\frac{1}{2}} \approx 2.3 \cdot 10^2$,
- $j_1 = \frac{-7^6 \cdot 13}{2^3 \cdot 5^2 \cdot 47^2}$, $j_2 = \frac{7^2 \cdot 13 \cdot 31}{2^5 \cdot 47^2}$, $\quad b_{\text{abs}} = 2^3 \cdot 5 \cdot 47 \approx 1.9 \cdot 10^3$,
- $N_{-2\alpha^2+2\alpha+5} = (2^{51} \cdot 5^6 \cdot 13 \cdot 31 \cdot 47)^3 \approx (6.7 \cdot 10^{23})^3$.

Example 3 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 + x^2 - 10x - 8)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by $\mathcal{O}_K$. See [16, 6.1(4)] and [18, 4.1.4] for a conjectural model. Its invariants are

- $i_1 = \frac{(7^3 \cdot 31 \cdot 73^3)^2}{(2^3 \cdot 23)^6}$, $i_2 = \frac{-2 \cdot 7^3 \cdot 31 \cdot 47^2 \cdot 73^3}{23^6}$, $i_3 = \frac{-7^5 \cdot 31^2 \cdot 73^4 \cdot 11593}{(2^{10} \cdot 23^3)^2}$,
- $\Delta_{\text{abs}} = (2^4 \cdot 23)^6 \approx 2.5 \cdot 10^{15}$, $\quad \frac{1}{8}B^{10} \approx 1.2 \cdot 10^{17}$,
- $j_1' = \frac{-2^{19} \cdot 47^2}{7^3 \cdot 31 \cdot 73^3}$, $j_2' = \frac{-11593}{2^2 \cdot 7 \cdot 73^2}$, $\quad a_{\text{abs}} = (2^3 \cdot 7^3 \cdot 31 \cdot 73^3)^{\frac{1}{2}} \approx 3.2 \cdot 10^3$,
- $j_1 = \frac{-7^3 \cdot 31 \cdot 73^3}{2^{19} \cdot 47^2}$, $j_2 = \frac{7^2 \cdot 31 \cdot 73 \cdot 11593}{2^{21} \cdot 47^2}$, $\quad b_{\text{abs}} = 2^{11} \cdot 47 \approx 9.6 \cdot 10^4$,
- $N_{-\alpha^2+\alpha+7} = (2^{205} \cdot 23^2 \cdot 29^2 \cdot 31 \cdot 47^2 \cdot 61^2 \cdot 89 \cdot 101 \cdot 139)^3 \approx (7.3 \cdot 10^{81})^3$.

Example 4 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - x^2 - 14x - 8)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by $\mathcal{O}_K$. A conjectural model is given in [16, 6.1(5)] and [18, 4.1.5]. Its invariants are

- $i_1 = \frac{(7^3 \cdot 43^2 \cdot 223^3)^2}{(2^4 \cdot 11 \cdot 47)^6}$, $i_2 = \frac{-7^3 \cdot 41^2 \cdot 43^2 \cdot 59^2 \cdot 223^3}{2^{13} \cdot 11^4 \cdot 47^6}$, $i_3 = \frac{-7^4 \cdot 43^3 \cdot 223^4 \cdot 419 \cdot 431}{(2^{13} \cdot 11^2 \cdot 47^3)^2}$,
- $\Delta_{\text{abs}} = (2^5 \cdot 11 \cdot 47)^6 \approx 2.1 \cdot 10^{25}$, $\quad \frac{1}{8}B^{10} \approx 3.1 \cdot 10^{18}$,
- $j_1' = \frac{-2^{11} \cdot 11^2 \cdot 41^2 \cdot 59^2}{7^3 \cdot 43^2 \cdot 223^3}$, $j_2' = \frac{-11^2 \cdot 419 \cdot 431}{2^2 \cdot 7^2 \cdot 43 \cdot 223^2}$, $\quad a_{\text{abs}} = (2^3 \cdot 7^3 \cdot 43^2 \cdot 223^3)^{\frac{1}{2}} \approx 3.8 \cdot 10^4$,
- $j_1 = \frac{-7^3 \cdot 43^2 \cdot 223^3}{2^{11} \cdot 11^2 \cdot 41^2 \cdot 59^2}$, $j_2 = \frac{7 \cdot 43 \cdot 223 \cdot 419 \cdot 431}{2^{13} \cdot 41^2 \cdot 59^2}$, $\quad b_{\text{abs}} = 2^7 \cdot 11 \cdot 41 \cdot 59 \approx 3.4 \cdot 10^6$,
- $N_{-2\alpha+1} = (2^{288} \cdot 11^9 \cdot 41^3 \cdot 43 \cdot 47^2 \cdot 59^3 \cdot 97 \cdot 131 \cdot 173 \cdot 211 \cdot 223 \cdot 269)^3 \approx (4.4 \cdot 10^{124})^3$.

Example 5 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - 21x - 28)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by $\mathcal{O}_K$. A conjectural model is given in [18, 4.2.1.1]. Its invariants are

- $i_1 = \frac{-3^9 \cdot 5^{12} \cdot 7^4}{2^{18}}$, $i_2 = \frac{3^3 \cdot 5^6 \cdot 7^2 \cdot 71^2}{2^3}$, $i_3 = \frac{3^7 \cdot 5^9 \cdot 7^3 \cdot 2621}{2^{20}}$,

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

- $\Delta_{\mathrm{abs}} = (2^8 \cdot 3)^3 \approx 4.5 \cdot 10^8$, $\quad \frac{1}{8}B^{10} \approx 2.1 \cdot 10^{15}$,
- $j_1' = \frac{-2^{15} \cdot 71^2}{(3^3 \cdot 5^3 \cdot 7)^2}$, $j_2' = \frac{-2621}{2^2 \cdot 3^2 \cdot 5^3 \cdot 7}$, $\quad a_{\mathrm{abs}} = (2^3 \cdot 3^6 \cdot 5^6 \cdot 7^2)^{\frac{1}{2}} \approx 1.6 \cdot 10^3$,
- $j_1 = \frac{-(3^3 \cdot 5^3 \cdot 7)^2}{2^{15} \cdot 71^2}$, $j_2 = \frac{3^4 \cdot 5^3 \cdot 7 \cdot 2621}{2^{17} \cdot 71^2}$, $\quad b_{\mathrm{abs}} = 2^9 \cdot 71 \approx 3.6 \cdot 10^4$,
- $N_{2\alpha} = 2^{433} \cdot 3^{55} \cdot 7^{11} \cdot 31^3 \cdot 47^3 \cdot 59^3 \cdot 61^3 \cdot 71^3 \cdot 173^3 \approx (1.3 \cdot 10^{66})^3$.

Example 6 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - 21x - 35)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by $\mathcal{O}_K$. A conjectural model is given in [18, 4.2.1.2]. Its invariants are

- $i_1 = \frac{-2^{12} \cdot 3^9 \cdot 7^4 \cdot 37^6}{(5 \cdot 11 \cdot 23)^6}$, $i_2 = \frac{2^6 \cdot 3^3 \cdot 7^2 \cdot 37^3 \cdot 149^2 \cdot 257^2}{(5^2 \cdot 11^3 \cdot 23^3)^2}$, $i_3 = \frac{2^9 \cdot 3^7 \cdot 7^3 \cdot 37^4 \cdot 2683}{(5^2 \cdot 11^3 \cdot 23^3)^2}$,
- $\Delta_{\mathrm{abs}} = (3 \cdot 5^2 \cdot 11^2 \cdot 23^2)^3 \approx 1.1 \cdot 10^{20}$, $\quad \frac{1}{8}B^{10} \approx 2.1 \cdot 10^{15}$,
- $j_1' = \frac{-(5 \cdot 149 \cdot 257)^2}{2^6 \cdot 3^6 \cdot 7^2 \cdot 37^3}$, $j_2' = \frac{-5^2 \cdot 2683}{2^3 \cdot 3^2 \cdot 7 \cdot 37^2}$, $\quad a_{\mathrm{abs}} = (2^6 \cdot 3^6 \cdot 7^2 \cdot 37^3)^{\frac{1}{2}} \approx 4.9 \cdot 10^3$,
- $j_1 = \frac{-2^6 \cdot 3^6 \cdot 7^2 \cdot 37^3}{(5 \cdot 149 \cdot 257)^2}$, $j_2 = \frac{2^3 \cdot 3^4 \cdot 7 \cdot 37 \cdot 2683}{(149 \cdot 257)^2}$, $\quad b_{\mathrm{abs}} = 5 \cdot 149 \cdot 257 \approx 1.9 \cdot 10^5$,
- $N_{-2\alpha^2+4\alpha+28} = 2^{245} \cdot 3^{58} \cdot 5^{36} \cdot 7^8 \cdot 11^{12} \cdot 23^6 \cdot 71^3 \cdot 149^3 \cdot 257^3 \approx (5.9 \cdot 10^{57})^3$.

Example 7 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - 39x - 26)$, let $K = K_+(\zeta_3)$. Then there is exactly one curve with primitive CM by $\mathcal{O}_K$. A conjectural model is given in [18, 4.2.1.3]. Its invariants are

- $i_1 = \frac{-3^9 \cdot 5^{12} \cdot 7^6 \cdot 11^6 \cdot 13^2}{(2^5 \cdot 29)^6}$, $i_2 = \frac{3^3 \cdot 5^6 \cdot 7^3 \cdot 11^5 \cdot 13 \cdot 59^2 \cdot 149^2}{2^{19} \cdot 29^6}$, $i_3 = \frac{3^7 \cdot 5^9 \cdot 7^5 \cdot 11^4 \cdot 13^2 \cdot 17 \cdot 17669}{(2^{16} \cdot 29^3)^2}$,
- $\Delta_{\mathrm{abs}} = (2^{12} \cdot 3 \cdot 29^2)^3 \approx 1.1 \cdot 10^{21}$, $\quad \frac{1}{8}B^{10} \approx 1. \cdot 10^{18}$,
- $j_1' = \frac{-2^{11} \cdot 59^2 \cdot 149^2}{3^6 \cdot 5^6 \cdot 7^3 \cdot 11 \cdot 13}$, $j_2' = \frac{-17 \cdot 17669}{2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11^2}$, $\quad a_{\mathrm{abs}} = (2^3 \cdot 3^6 \cdot 5^6 \cdot 7^3 \cdot 11^3 \cdot 13)^{\frac{1}{2}} \approx 8.1 \cdot 10^4$,
- $j_1 = \frac{-3^6 \cdot 5^6 \cdot 7^3 \cdot 11 \cdot 13}{2^{11} \cdot 59^2 \cdot 149^2}$, $j_2 = \frac{3^4 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 17 \cdot 17669}{2^{13} \cdot 11 \cdot 59^2 \cdot 149^2}$, $\quad b_{\mathrm{abs}} = 2^7 \cdot 11 \cdot 59 \cdot 149 \approx 1.2 \cdot 10^7$,
- $N_{-\frac{1}{2}\alpha^2+\frac{3}{2}\alpha+13} = 2^{921} \cdot 3^{100} \cdot 11^{21} \cdot 13^8 \cdot 29^6 \cdot 53^3 \cdot 59^6 \cdot 109^3 \cdot 113^3 \cdot 149^6 \cdot 233^3 \cdot 359^3 \cdot 467^3 \cdot 541^3 \cdot 577^3 \approx (2. \cdot 10^{148})^3$.

Example 8 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - 61x - 183)$, let $K = K_+(\zeta_3)$. Then there are exactly four curves with primitive CM by $\mathcal{O}_K$. Conjectural models are given in [18, 4.3.1 (corrected with respect to arXiv version 1)]. Let $H_{j_1} = H_{\mathcal{O}_K,1}$ and $\widehat{H}_{j_1,j_2} = \widehat{H}_{\mathcal{O}_K,2}$ be the polynomials as in (2.4)–(2.5), and let $H_{j_1'}$ and H_{i_1} be defined as in (2.4), but with the invariants j_1' and i_1 instead of j_1. These polynomials are numerically approximable with the methods of Koike–Weng [16] and Lario–Somoza [18] and satisfy $H_{j_1}(j_1(C)) = 0$ and $j_2(C) = \widehat{H}_{j_1,j_2}(j_1(C))/H_{j_1}'(j_1(C))$ (see [9]). Then the denominators of these polynomials are

- $\mathrm{den}(H_{j_1}) = 2^3 \cdot 3^{39} \cdot 11^2 \cdot 23^2 \cdot 41^2 \cdot 53^4 \cdot 89^2 \cdot 113^2 \cdot 149^2 \cdot 191^2 \approx 2.3 \cdot 10^{51}$
  $\mathrm{den}(\widehat{H}_{j_1,j_2}) = 2^5 \cdot 3^{39} \cdot 11^3 \cdot 23^2 \cdot 41^2 \cdot 53^4 \cdot 89^2 \cdot 113^2 \cdot 149^2 \cdot 191^2 \approx 9.9 \cdot 10^{52}$,
- $\mathrm{den}(H_{j_1'}) = 2^{18} \cdot 7^{12} \cdot 11 \cdot 61^2 \cdot 1289^3 \cdot 6551^3 \cdot 20707^3 \approx 7.9 \cdot 10^{53}$,
- $\mathrm{den}(H_{i_1}) = (2^2 \cdot 3^9 \cdot 11^6 \cdot 23^4 \cdot 53^2 \cdot 131^2)^3 \approx 6.7 \cdot 10^{72}$,
- $N_{-4\alpha^2+18\alpha+163} = (2^{235} \cdot 3^{148} \cdot 11^{12} \cdot 23^6 \cdot 37^3 \cdot 41^3 \cdot 53^3 \cdot 61 \cdot 89 \cdot 113 \cdot 131 \cdot 149 \cdot 191 \cdot 367 \cdot 613 \cdot 643 \cdot 733 \cdot 907)^3 \approx (1.2 \cdot 10^{203})^3$.

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

Example 9 For the field $K_+ = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - x^2 - 22x - 5)$, let $K = K_+(\zeta_3)$. Then there are exactly four curves with primitive CM by $\mathcal{O}_K$. See [18, 4.3.2] for conjectural models. In the notation of Example 8, we have

- $\operatorname{den}(H_{j_1}) = (2^6 \cdot 3^{15} \cdot 5^4 \cdot 89 \cdot 137 \cdot 149 \cdot 179 \cdot 269)^2 \approx 2.5 \cdot 10^{45}$
  $\operatorname{den}(\widehat{H}_{j_1,j_2}) = (2^6 \cdot 3^{15} \cdot 5^3 \cdot 89 \cdot 137 \cdot 149 \cdot 179 \cdot 269)^2 \approx 1. \cdot 10^{44}$,
- $\operatorname{den}(H_{j_1'}) = 7^{12} \cdot 53^3 \cdot 67 \cdot 107^3 \cdot 179^3 \cdot 3029017^3 \approx 2.7 \cdot 10^{49}$,
- $\operatorname{den}(H_{i_1}) = (2^4 \cdot 3^5 \cdot 5^4 \cdot 53 \cdot 59 \cdot 107)^6 \approx 2.9 \cdot 10^{71}$,
- $N_{-\frac{2}{3}\alpha^2+\frac{29}{3}} = (2^{253} \cdot 3^{155} \cdot 5^{32} \cdot 43^2 \cdot 53^3 \cdot 59^2 \cdot 67 \cdot 89^2 \cdot 107 \cdot 109 \cdot 137 \cdot 149 \cdot 179^2 \cdot 223 \cdot 241 \cdot 263 \cdot 269 \cdot 397 \cdot 643 \cdot 997 \cdot 1087)^3 \approx (1.2 \cdot 10^{224})^3$.

Remark 10.1 Notice that the sizes of the denominators of the absolute invariants j_1 and j_2 of Section 2.3 are similar to the denominators of the Koike–Weng invariants and much smaller than the denominators of the invariants defined by using the discriminant. Theorem 1.3 in [14] suggests a bound for the primes appearing in the discriminant, while we do not have a bound at all for the primes in the denominator of the Koike–Weng invariants. That the primes in the denominators of the Koike–Weng invariants are small, and even smaller than those for our invariants, is a mystery that needs further research.

For our absolute invariants, we have the best bound. Hence among the three kind of invariants, the more suitable ones for constructing Picard curves with CM by a given order $\mathcal{O}$ are the absolute invariants j_1 and j_2.

A A Lemma About Components of Bad Reduction

Most of this appendix is an edited copy of an email from Bas Edixhoven to the authors. Lemma A.1 and its proof are well known to many experts, but it seems that neither is written down in the literature. For completeness, as we use it in our proof of the singular case of Proposition 3.3, we state the lemma and provide details of the proof.

Lemma A.1 *Let R be a discrete valuation ring with fraction field M and residue field k. Let X be a projective R-scheme, of dimension 2, flat over R such that X_M is smooth, and geometrically connected over M, of genus at least 1. Let C be an irreducible component of X_k and assume that C is geometrically irreducible and birational to a smooth geometrically irreducible projective curve C' over k of genus at least 1.*

Suppose that there exists an open subscheme U of X such that U is smooth over R, and such that U_k is a non-empty open subset of C.

Let $M \to M'$ be a finite separable field extension such that X_M has stable reduction over the integral closure R' of R in M'. Then the open subscheme $U_{R'}$ of $X_{R'}$ is isomorphic to an open subscheme of the stable model of X. Moreover, the normalization of the special fibre of the stable model of X contains a copy of $C'_{k'}$, where k' is the residue field of R'.

Proof Let $X_{R'}$ be the pullback of X via $R \to R'$, which is integral by [20, Proposition 4.3.8], and let $X^{\mathrm{stab}}_{R'}$ be the (unique) stable model of $X_{M'}$ over R'.

We apply [20, Corollary 8.3.51] to $X_{R'}$ (see [20, Definition 8.3.39] for a definition of "in the strong sense"). This gives us $f\colon X^{\mathrm{res}}_{R'} \to X_{R'}$ birational, with $X^{\mathrm{res}}_{R'}$ projective

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

over R' and regular, with f an isomorphism over the open subscheme $U_{R'}$ of $X_{R'}$. Here we use that U is smooth over R. Hence $U_{R'}$ is smooth over R'; hence $U_{R'}$ is regular.

Liu [20, Theorem 9.3.21] stated that there is a unique minimal regular model $X^{\mathrm{res}}_{R'} \to X^{\mathrm{min}}_{R'}$ of $X^{\mathrm{res}}_{R'}$ that is in fact (see the proof) isomorphic to every relatively minimal model. This morphism is the identity on the generic fibres, and by the construction (Castelnuovo's criterion (Theorem 9.3.8) and Proposition 9.3.19 in [20]), it contracts precisely the irreducible components E of the closed fibre of $X^{\mathrm{res}}_{R'}$ such that E is isomorphic to $\mathbb{P}^1_{k_E}$ with $k_E := H^0(E, O_E)$ (a finite extension of the residue field k' of R' over which E lies) and $E \cdot E = -[k_E : k']$.

Note that the open subscheme $U_{R'}$ of $X^{\mathrm{res}}_{R'}$ is mapped isomorphically to an open subscheme of $X^{\mathrm{min}}_{R'}$, because its closed fibre is an open part of a curve of genus at least 1.

Furthermore, there is a unique morphism to $X^{\mathrm{stab}}_{R'}$ from its minimal desingularization $(X^{\mathrm{stab}}_{R'})^{\mathrm{mindes}}$ and this morphism only contracts $\mathbb{P}^1$'s in the closed fibres of self-intersection -2 [20, Corollary 10.3.25]. As the geometric special fibre of $X^{\mathrm{stab}}_{R'}$ has no $\mathbb{P}^1$'s, except with self-intersection ≤ -3 [20, Definitions 10.3.1–2], we get that the geometric special fibre of $(X^{\mathrm{stab}}_{R'})^{\mathrm{mindes}}$ has no $\mathbb{P}^1$'s except with self-intersection ≤ -2.

Exactly like $X^{\mathrm{res}}_{R'}$, the surface $(X^{\mathrm{stab}}_{R'})^{\mathrm{mindes}}$ also has a morphism to $X^{\mathrm{min}}_{R'}$ that only contracts curves that are (after field extension) $\mathbb{P}^1$'s of self-intersection -1, and as $(X^{\mathrm{stab}}_{R'})^{\mathrm{mindes}}$ has no such $\mathbb{P}^1$'s, this morphism is an isomorphism.

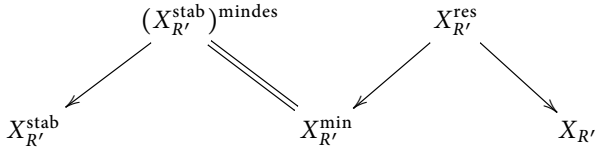

Figure 1: The fibred surfaces in the proof of Lemma A.1.

Therefore, through the maps of Figure 1, the open subscheme $U_{R'} \subset X_{R'}$ is mapped isomorphically to an open subscheme of $X^{\mathrm{stab}}_{R'}$.

When we base change $U_{R'}$ to the residue field k', we get an embedding $U_{k'} \to X^{\mathrm{stab}}_{k'}$, where $U_{k'}$ is a base change of a non-empty open smooth part of C, hence a base change of a dense part of C'. Let C'' be the closure of the image of this embedding of curves. Then we get a birational map of curves $C'_{k'} \to C''$, hence an isomorphism to the normalization. ∎

Corollary A.2 *Let R be a discrete valuation ring with maximal ideal $\mathfrak{m}$, field of fractions M, and residue field $k = R/\mathfrak{m}$ of characteristic not 2 or 3. Let D be a smooth projective, geometrically irreducible curve over M and suppose that R is such that D has stable reduction over R.*

(i) *If D over M is given by $y^3 = x^4 + ax^2 + bx + 1$ with $b, a \pm 2 \in \mathfrak{m}$, then the stable reduction $\overline{D}$ of D has an irreducible component birational to the elliptic curve $C' : Y^2 = X^3 \pm 1$,*

https://doi.org/10.4153/S0008414X18000111 Published online by Cambridge University Press

(ii) *If D over M is given by $y^3 = x^4 + x^2 + bx + c$ with $b, c \in \mathfrak{m}$, then the stable reduction $\overline{D}$ of D has an irreducible component birational to the hyperelliptic curve $C' : Y^2 = X^6 - 4$.*

Proof Let X (respectively, C) be the plane projective R-scheme (respectively, k-scheme) given by the defining polynomial f of D. Let

$$U = \mathrm{Spec}(R[x, y, y^{-1}]/(f)).$$

By Lemma A.1, it now suffices to check that C is birational to C', which we did in the proof of Lemma 3.1. ∎

Acknowledgements The authors would like to thank Irene Bouw, Peter Bruin, Christophe Ritzenthaler, Matthieu Romagny, and Anna Somoza for helpful discussions, the anonymous referees for helpful criticism of the exposition in an earlier version, and Bas Edixhoven for providing the proof in Appendix A. Most of Kılıçer's work was done during her stay in Universiteit Leiden and Carl von Ossietzky Universität Oldenburg.

References

[1] Sonny Arora and Kirsten Eisentraeger, Constructing Picard curves with complex multiplication using the Chinese Remainder Theorem. To appear in Algorithmic Number Theory Symposium, 13. Open Book Series. Mathematical Sciences Publishers, Berkeley, CA. http://www.math.grinnell.edu/~paulhusj/ants2018/paper-arora.html.

[2] 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. https://doi.org/10.1112/S1461157016000322.

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

[4] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*. In: *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, Springer-Verlag, Berlin, 1990.

[5] 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*. In: *Women in numbers Europe*, Assoc. Women Math. Ser., 2., Springer, Cham, 2015, pp. 109–151.

[6] Florian Bouyer and Marco Streng, *Examples of CM curves of genus two defined over the reflex field*. LMS J. Comput. Math. 18(2015), 1, 507–538. https://doi.org/10.1112/S1461157015000121.

[7] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*. Invent. Math. 163(2006), 2, 229–288. https://doi.org/10.1007/s00222-005-0459-7.

[8] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*. In: *Arithmetics, geometry, and coding theory*, Sémin. Congr., 21, Soc. Math. France, Paris, 2010, pp. 161–176.

[9] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*. In: *Advances in cryptology—ASIACRYPT 2006*, Lecture Notes in Comput. Sci., 4284, Springer, Berlin, 2006, pp. 114–129.

[10] Eyal Z. Goren and Kristin E. Lauter, *Class invariants for quartic CM fields*. Ann. Inst. Fourier (Grenoble) 57(2007), 2, 457–480. https://doi.org/10.5802/aif.2264.

[11] Eyal Z. Goren and Kristin E. Lauter, *Genus 2 curves with complex multiplication*. Int. Math. Res. Not. IMRN 2012(2012), 5, 1068–1142. https://doi.org/10.1093/imrn/rnr052.

[12] Rolf-Peter Holzapfel, *The ball and some Hilbert problems*, Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 1995.

[13] Pınar Kılıçer, Hugo Labrande, Raynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng, *Plane quartics over $\mathbb{Q}$ with complex multiplication*. Acta Arith. 185(2018), 127–156. https://doi.org/10.4064/aa170227-16-3.

[14] Pınar Kılıçer, 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. arxiv:1609.05826.
[15] Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng, Implementation of the denominator bounds of 'Primes dividing invariants of CM Picard curves' and 'A bound on the primes of bad reduction for CM curves of genus 3', 2018. https://bitbucket.org/mstreng/picard_primes/src/master/primes_CM_Picard.sage.
[16] Kenji Koike and Annegret Weng, *Construction of CM Picard curves*. Math. Comp. 74(2005), 499–518. https://doi.org/10.1090/S0025-5718-04-01656-4.
[17] Serge Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften, 255, Springer-Verlag, New York, 1983.
[18] Joan-C. Lario and Anna Somoza, A note on Picard curves of CM-type. arxiv:1611.02582.
[19] Kristin Lauter and Bianca Viray, *An arithmetic intersection formula for denominators of Igusa class polynomials*. Amer. J. Math. 137(2015), 2, 497–533. https://doi.org/10.1353/ajm.2015.0010.
[20] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, 6, Oxford University Press, Oxford, 2002.
[21] David Mumford, *Prym varieties. I*. In: *Contributions to analysis (a collection of papers dedicated to Lipman Bers)*, Academic Press, New York, 1974, pp. 325–350.
[22] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, 5, Hindustan Book Agency, New Delhi, 2008.
[23] Christophe Ritzenthaler and Matthieu Romagny, *On the Prym variety of genus 3 covers of genus 1 curves*. Épijournal Geom. Algébrique 2(2018), Art. 2, 8 arxiv:1612.07033.
[24] Carl Ludwig Siegel, *Lectures on the geometry of numbers*, Springer-Verlag, Berlin, 1989.
[25] Anne-Monika Spallek, Kurven vom geschlecht 2 und ihre anwendung in public-key-kryptosystemen. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
[26] William A. Stein, *et al.*, SageMath, the Sage Mathematics Software System (Version 7.4). The SageMath Development Team, 2016. http://www.sagemath.org.
[27] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*. Math. Comp. 68(1999), 225, 307–320.
[28] Annegret Weng, *A class of hyperelliptic CM-curves of genus three*. J. Ramanujan Math. Soc. 16(2001), 4, 339–372.

Johann Bernoulli Instituut voor Wiskunde en Informatica, Rijksuniversiteit Groningen, Nijenborgh 9, 9747 AGGroningen, Nederland
e-mail : p.kilicer@rug.nl

IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France
e-mail : elisa.lorenzogarcia@univ-rennes1.fr

Mathematisch Instituut, Universiteit Leiden, P.O. box 9512, 2300 RA Leiden, The Netherlands
e-mail : streng@math.leidenuniv.nl