A bound on the primes of bad reduction for CM curves of genus 3

Article

Accepted Version

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

A BOUND ON THE PRIMES OF BAD REDUCTION FOR CM CURVES OF GENUS 3

PINAR KILIÇER, KRISTIN LAUTER, ELISA LORENZO GARCÍA, RACHEL NEWTON, EKIN OZMAN, AND MARCO STRENG

Abstract. We give bounds on the primes of geometric bad reduction for curves of genus three of primitive CM type in terms of the CM orders. In the case of elliptic curves, there are no primes of geometric bad reduction because CM elliptic curves are CM abelian varieties, which have potential good reduction everywhere. However, for genus at least two, the curve can have bad reduction at a prime although the Jacobian has good reduction. Goren and Lauter gave the first bound in the case of genus two.

In the cases of hyperelliptic and Picard curves, our results imply bounds on primes appearing in the denominators of invariants and class polynomials, which are important for algorithmic construction of curves with given characteristic polynomials over finite fields.

1. Introduction

Generating curves over finite fields with a given number of points on the curve or on its Jacobian is a hard and interesting problem, with valuable applications and connections to number theory. The case of elliptic curves, for example, has important applications in cryptography, and current solutions rely on computing Hilbert class polynomials associated to imaginary quadratic fields. For curves of genus 2, already additional interesting problems arise when trying to compute the analogous class polynomials, the Igusa class polynomials, since the coefficients are not integral as in the case of genus 1. This leads to the question of understanding and bounding primes of bad reduction for curves of genus 2 whose Jacobians have complex multiplication (CM), and connections with arithmetic intersection theory ([9, 16]).

The case of genus 3 is more complicated than the genus 2 case. First, an abelian threefold can be non-simple *without* being isogenous to a product of elliptic curves. Second, it is possible for a sextic CM field to have both primitive *and* non-primitive CM types. Third, the rank of the endomorphism algebra can be larger in the genus 3 case than in the genus 2 one. Handling each of these complications requires new ideas.

In this paper, we prove the following result which gives a bound on primes of geometric bad reduction for CM curves of genus 3 with primitive CM type (here and in what follows, we say that a curve has CM if its Jacobian does, and we refer to the CM type of the Jacobian also as the CM type of the curve).

Theorem 1.1. *Let C/M be a smooth, projective, geometrically irreducible curve of genus 3 over a number field M. Suppose that the Jacobian $\mathrm{Jac}(C)$ has CM by an order $\mathcal{O}$ inside a CM field K of degree 6 and that the CM type of $\mathrm{Jac}(C)$ is primitive. Let $\mathfrak{p}$ be a prime of M lying over a rational prime p such that C does not have potential good reduction at $\mathfrak{p}$. Then the following upper bound holds on p. For every $\mu \in \mathcal{O}$ with μ^2 totally real and $K = \mathbb{Q}(\mu)$, we have $p < \frac{1}{8}B^{10}$ where $B = -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$.*

As in the case of genus two [9], in order to prove Theorem 1.1, we use the fact that bad reduction of C gives an embedding of the CM order $\mathcal{O}$ into the endomorphism ring of the reduced Jacobian such that the Rosati involution induces complex conjugation on $\mathcal{O}$ (see Lemma 4.4). We show that such an embedding cannot exist for sufficiently large primes. The proof of Theorem 1.1 is given in Section 5.2.

To deal with the new situation where the reduction is a product of an elliptic curve with an abelian surface with no natural decomposition, we needed to find a suitable and explicit decomposition. Just the existence of a decomposition is not enough, and our first main contribution is to find the 'right' decomposition (Lemma 3.1).

Newton is supported by EPSRC grant EP/S004696/1. Ozman is supported by Bogazici University Research Fund Grant Number 15B06SUP3 and by the BAGEP award of the Science Academy, 2016. Streng is supported by NWO Vernieuwingsimpuls.

The second main new idea is using the primitivity of the CM type in the case where there exist non-primitive CM types. For this we use the reduction of the tangent space in Section 5. Primitivity is crucial for our methods, but we do give the following conjecture in the non-primitive case.

Conjecture 1.2. *There is a constant $e \in \mathbb{R}_{\geq 0}$ such that the following holds. Let C/M be a smooth, projective, geometrically irreducible curve of genus $g \leq 3$ over a number field M. Suppose that C has CM (not necessarily of primitive CM type) by an order $\mathcal{O}$ in a CM field K of degree $2g$.*

Let $\mathfrak{p}$ be a prime of M lying over a rational prime p such that C does not have potential good reduction at $\mathfrak{p}$. Then the following upper bound holds on p. For every $\mu \in \mathcal{O}$ with μ^2 totally real and $K = \mathbb{Q}(\mu)$, we have $p < B^e$ where $B = -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$.

Remark 1.3. *The case $g = 1$ is true even with $e = 0$, as CM elliptic curves have potential good reduction everywhere. The case of primitive CM types is Goren-Lauter* [9] *for $g = 2$ and Theorem 1.1 for $g = 3$. The case of non-primitive CM types is an open problem even for $g = 2$ as far as we know.*

We do have numerical evidence in the case $g = 2$. Bröker-Lauter-Streng [6, Lemma 6.4, Tables 1 and 2] *give CM hyperelliptic curves C_{-3}, C^1_{-6}, C^2_{-6}, C_{-8}, C_{-15}, C^i_{-20}, C^{-i}_{-20} as well as explicit CM orders $\mathcal{O}$, and each time the denominators of the absolute Igusa invariants have only small prime factors. For example, we have $(I_4 I_6/I_{10})(C_{-15}) = -3^2 \cdot 5^3 \cdot 79 \,/\, 2^7$.*

A proof in the case where the CM type is non-primitive cannot use the tangent space in the way we use it in our proof. On the other hand, in the case of non-primitive CM types there are more endomorphisms that one could use. This is because (for $g \leq 3$) the endomorphism ring $\mathrm{End}(J_{\overline{M}})$ has rank $2g^2$ over $\mathbb{Z}$, whereas in the case of primitive CM types we have $\mathrm{End}(J_{\overline{M}}) \cong \mathcal{O}$ of rank $2g$. Here, and throughout, $\overline{M}$ denotes an algebraic closure of M.

The following proposition, which is proven in Section 6, turns the bound of Theorem 1.1 into an intrinsic bound, depending only on the discriminants of the orders involved.

Proposition 1.4. *Let $\mathcal{O} \subset K$ be an order in a sextic CM field.*

1. *If K contains no imaginary quadratic subfield, then there exists μ as in Theorem 1.1 satisfying $0 < -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2) \leq (\frac{6}{\pi})^{2/3}|\Delta(\mathcal{O})|^{1/3}$, where $\Delta(\mathcal{O})$ is the discriminant of the order $\mathcal{O}$.*
2. *If K contains an imaginary quadratic subfield K_1, let K_+ be the totally real cubic subfield and let $\mathcal{O}_i = K_i \cap \mathcal{O}$ where $i \in \{1, +\}$. Then there exists μ as in Theorem 1.1 with $0 < -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2) \leq |\Delta(\mathcal{O}_1)|(1 + 2\sqrt{|\Delta(\mathcal{O}_+)|})$.*

Our next result is a consequence of Theorem 1.1 in the special cases of hyperelliptic and Picard curves. A hyperelliptic curve of genus 3 over a subfield M of $\mathbb{C}$ is a curve with an affine model of the form $C : y^2 = F(x, 1)$ such that F is a separable binary form over M of degree 8. A hyperelliptic curve invariant of weight k for genus 3 is a polynomial I over $\mathbb{Z}$ in the coefficients of F satisfying $I(F \circ A) = \det(A)^k I(F)$ for all $A \in \mathrm{GL}_2(\mathbb{C})$. For example, the discriminant Δ of F (not to be confused with $\Delta(\mathcal{O})$) is an invariant of weight 56. Shioda [21] gives a set of invariants that uniquely determines the isomorphism class of C over $\mathbb{C}$.

A Picard curve of genus 3 over a field M of characteristic 0 is a smooth plane projective curve given by an affine model $C : y^3 = f(x)$ such that f is a monic separable polynomial over M of degree 4. Such a curve can be written as follows (uniquely up to scalings $(x, y) \mapsto (u^3 x, u^4 y)$ with $u \in M^*$, which change a_l into $u^{3l} a_l$):

$$y^3 = f(x) = x^4 + a_2 x^2 + a_3 x + a_4. \tag{1}$$

We define the ring of invariants to be the graded ring generated over $\mathbb{Z}[\frac{1}{3}]$ by the symbols a_2, a_3 and a_4 of respective weights 2, 3, 4. It contains the discriminant Δ of $f(x)$, which is an invariant of weight 12.

The following consequence of Theorem 1.1 is derived in Section 7.

Theorem 1.5. *Let C/M be a hyperelliptic (respectively Picard) curve of genus 3 over a number field M. Suppose that C has CM by an order $\mathcal{O}$ inside a CM field K of degree 6 and that the CM type of C is primitive. Let $l \in \mathbb{Z}_{>0}$ and let $j = u/\Delta^l$ be a quotient of invariants of hyperelliptic (respectively Picard) curves, such that the numerator u has weight $56l$ (respectively $12l$). Let $\mathfrak{p}$ be a prime over a prime number p such that $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$. Then p satisfies the bound of Theorem 1.1.*

Remark 1.6. *In the Picard curve case, subsequent work of Kılıçer, Lorenzo García and Streng* [13] *using the results of Section 5 gives a much stronger analogue of Theorem 1.5 for the alternative invariants a_2a_4/a_3^2 and a_2^3/a_3^2.*

In the Picard curve case, we define $j_1 = a_2^6/\Delta$, $j_2 = a_2^3a_3^2/\Delta$, $j_3 = a_2^4a_4/\Delta$, $j_4 = a_3^4/\Delta$, $j_5 = a_4^3/\Delta$, $j_6 = a_2a_3^2a_4/\Delta$ and $j_7 = a_2^2a_4^2/\Delta$. Over an algebraic closure $\overline{M}$ of M, any Picard curve has a model in one of the following forms:

$y^3 = x^4 + Ax^2 + Ax + B$,	$A = j_1j_2^{-1}$, $B = j_1j_2^{-2}j_3 = j_3j_4^{-1}$	if $j_2 \neq 0$,
$y^3 = x^4 + Ax^2 + Bx + B$,	$A = j_6j_5^{-1}$, $B = j_4j_5^{-1}$	if $j_4j_5 \neq 0$,
$y^3 = x^4 + x^2 + A$,	$A = j_3j_1^{-1}$	if $j_1 \neq 0$, $j_2 = 0$,
$y^3 = x^4 + x$,		if $j_1 = j_5 = 0$,
$y^3 = x^4 + 1$,		if $j_1 = j_4 = 0$.

We use the same notation j_l also in the hyperelliptic case, but there we take it to mean the following quotients of Shioda invariants appearing in Weng [25, (5)]: $j_1 = I_2^7/\Delta$, $j_3 = I_2^5I_4/\Delta$, $j_5 = I_2^4I_6/\Delta$, $j_7 = I_2^3I_8/\Delta$ and $j_9 = I_2^2I_{10}/\Delta$. Note that these invariants satisfy the hypothesis of Theorem 1.5.

Now suppose that K is a sextic CM field containing a primitive 4th root of unity and consider invariants of hyperelliptic curves. Alternatively, let K be a sextic CM field containing a primitive 3rd root of unity and consider invariants of Picard curves. Let $j = u/\Delta^l$ and $j' = u'/\Delta^l$ be quotients of invariants of hyperelliptic (respectively Picard) curves, such that the numerators u and u' have weight 56l (respectively 12l). We define the class polynomials $H_{K,j}$ and $\widehat{H}_{K,j,j'}$ by

$$H_{K,j} = \prod_C (X - j(C)), \quad \widehat{H}_{K,j,j'} = \sum_C j'(C) \prod_{D \neq C} (X - j(D)) \in \mathbb{C}[X]$$

where the products and sum range over isomorphism classes of curves C and D over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of primitive CM type, which are indeed hyperelliptic (resp. Picard) by Weng [25, Theorem 4.5] (resp. Koike-Weng [14, Lemma 1]). The polynomial $\widehat{H}_{K,j,j'}$ is the modified Lagrange interpolation of the roots of $H_{j'}$ introduced in [8, Section 3]. These polynomials have rational coefficients as they are fixed by $\mathrm{Aut}(\mathbb{C})$. Moreover, the polynomials H_{j_l} and $\widehat{H}_{j_1,j_l}$, where l ranges over $\{3,5,7,9\}$ in the hyperelliptic case and over $\{2,3\}$ in the Picard case, can be used for the CM method for constructing curves over finite fields. See [8, Section 3] as well as [25] (resp. [14]) for how to use these polynomials.

The polynomials $H_{K,j}$ and $\widehat{H}_{K,j,j'}$ can be approximated using the methods of Weng [25] and Balakrishnan-Ionica-Lauter-Vincent [2] in the hyperelliptic case and the methods of Koike-Weng [14] and Lario-Somoza [15] in the Picard case. The (rational) coefficients of the polynomials can then be recognized from such approximations using continued fractions or the LLL algorithm. However, to be absolutely sure of the coefficients, one would need a bound on the denominators. We view the following result as a first step towards obtaining such a bound. It is an immediate consequence of Theorem 1.5.

Theorem 1.7. *Let K be a sextic CM field containing a primitive 4th root of unity and let p be a prime number that divides the denominator of a class polynomial H_j or $\widehat{H}_{j,j'}$ with quotients of hyperelliptic curve invariants j and j' as in Theorem 1.5. Then p satisfies the bound of Theorem 1.1. The statement remains true if one replaces '4th' by '3rd' and 'hyperelliptic' by 'Picard'.* □

1.1. **Applications, further work and open problems.**

Sharper upper bounds, and exponents. We believe that the exponent 10 in Theorem 1.1 is not optimal. For instance, in [3], for the special case of reduction to a product of 3 elliptic curves with K not containing any proper CM subfield, one gets an exponent of 6. In the general case, it may be possible to get smaller exponents using variants of our proof, for example with a different choice of isogeny s in Section 3, or by considering bounds in Section 4 coming not just from the matrix of μ, but also from other elements.

We also believe that it is now possible to combine our proofs with the techniques of Goren and Lauter [10] to get not only a bound on the primes in the denominator of Theorems 1.5 and 1.7, but also a bound on the valuations at those primes. Together, these bounds will give a bound on the denominator itself, which is required if one wants to prove that the output of a class-polynomial-computing algorithm is correct. This

was done for genus 2 by Streng [24]. As in the case of genus 2, the resulting bounds will be so large that the algorithm is purely theoretical and cannot be run in practice. However, we view our results as a first step towards a denominator formula such as that of Lauter and Viray [16], which is small and explicit enough for yielding proven-correct CM curves, as shown by Bouyer and Streng [5, 23].

Denominators for general curves of genus 3. Theorem 1.5 (and hence 1.7) is only for hyperelliptic and Picard curves. The reason why it follows from Theorem 1.1 (as shown in Section 7) is that the primes dividing the denominator $\Delta^l(C)$ of $j(C)$ are exactly the primes of bad reduction for C. In other words, it is because the zero locus of Δ in the compactification of the moduli space of hyperelliptic/Picard curves parametrizes only singular curves. In the case of the moduli space of all curves of genus three, the locus of bad reduction has codimension greater than 1, hence is not the vanishing locus of an invariant. In particular, no generalization of Theorem 1.5 would follow directly from Theorem 1.1 or even from Conjecture 1.2.

The most direct generalization of Theorem 1.5 to arbitrary primitive CM curves of genus 3 would have the discriminant invariant of plane quartics as the denominator of j. Numerical experiments of Kılıçer, Labrande, Lercier, Ritzenthaler, Sijsling and Streng [12] suggest that this generalization would be false.

Lower bounds. Habegger and Pazuki [11, Theorems 1.3 and 4.5(ii)] give lower bounds on the denominators of absolute invariants of CM curves of genus 2. It would be interesting to see whether a similar result is true for hyperelliptic or Picard curves of genus 3.

1.2. **Acknowledgements.** We thank Irene Bouw, Bas Edixhoven, Everett Howe, Christophe Ritzenthaler and Chia-Fu Yu for useful discussions and for pointing out some of the references. We are grateful to the anonymous referees for many helpful suggestions. Part of this work was carried out at Carl von Ossietzky University of Oldenburg, the Istanbul Center for Mathematical Sciences, the Lorentz Center, the Max Planck Institute for Mathematics, UC San Diego, and the University of Warwick.

2. Notation and strategy

For the reader's convenience, we define some well-known concepts that are essential for our approach. By a *curve* over a field M, we mean a smooth, projective, geometrically irreducible curve over M unless we say otherwise.

Definition 2.1. *Let $\mathcal{O}$ be an order in a* CM field *K of degree $2g$ over $\mathbb{Q}$, that is, an imaginary quadratic extension of a totally real number field. We say that a curve C of genus g over a number field M has* complex multiplication *by $\mathcal{O}$ if there exists an embedding ϕ of $\mathcal{O}$ into the endomorphism ring of the Jacobian $\mathrm{Jac}(C)_{\overline{M}}$ of C over the algebraic closure.*

Definition 2.2. *Let K be as in Definition 2.1. A* complex multiplication type (CM type) *of K is a set of g non-conjugate embeddings $K \hookrightarrow \mathbb{C}$. We say that a CM type is primitive if its restriction to any strict CM subfield of K is not a CM type.*

Definition 2.3. *Given J and ϕ as in Definition 2.1 with $\overline{M} \subset \mathbb{C}$, we obtain a CM type by diagonalizing the action of K via ϕ on the tangent space of $\mathrm{Jac}(C)_{\overline{M}}$ at 0, and we call this the* CM type of C.

Now let C be a curve of genus 3 defined over a number field M and such that its Jacobian $J = \mathrm{Jac}(C)$ has complex multiplication by an order $\mathcal{O}$ of a sextic CM field K. Let us assume that the CM type is primitive. We fix a totally imaginary generator $\mu \in \mathcal{O}$ of K over $\mathbb{Q}$. Thus, μ^2 is a totally negative element of $\mathcal{O}$ that generates the totally real subfield K_+ of K.

Let $\mathfrak{p} \mid p$ be a prime such that C does not have potential good reduction at $\mathfrak{p}$. In other words, $\mathfrak{p}$ is a prime of geometric bad reduction for C, in the sense that even after extension of the base field, the curve C still has bad reduction at all primes above $\mathfrak{p}$. As noted in [3, Section 4.2], this is equivalent to the stable reduction of C being non-smooth, where this type of reduction is simply called "bad reduction". As J has complex multiplication, it has potential good reduction at every prime by a result of Serre and Tate [20]. Without loss of generality of our main results, we extend the field M so that C has a stable model for the reduction at $\mathfrak{p}$ and J has good reduction at $\mathfrak{p}$. Let $\overline{J} = (J \bmod \mathfrak{p})$.

By Corollary 4.3 in [3], we know that, possibly after extending the base field again, there exists an isomorphism $\overline{J} \cong E \times A$ as principally polarized abelian varieties (p.p.a.v.) over the new base field, where

E is an elliptic curve with its natural polarization and A is a principally polarized abelian surface. This includes the case where there is an isomorphism $\overline{J} \cong E_1 \times E_2 \times E_3$ as p.p.a.v., where $A \cong E_2 \times E_3$ is a product of elliptic curves. Let us write $\mathrm{End}(E) = \mathcal{R}$ and $\mathcal{B} = \mathcal{R} \otimes \mathbb{Q}$.

We will see that there is an isogeny $s : E^2 \to A$ (which is, in fact, already known by [3, Theorem 4.5]). Once we fix an isogeny s, there are natural embeddings

$$\iota : \mathcal{O} \overset{\iota_0}{\hookrightarrow} \mathrm{End}(E \times A) \overset{\iota_1}{\hookrightarrow} \mathrm{End}(E^3) \otimes \mathbb{Q} \cong \mathrm{Mat}_{3\times 3}(\mathcal{B}).$$

Step 1 is to show that for sufficiently large primes p, the entries of $\iota(\mu^2)$ lie in a field $\mathcal{B}_1 \subset \mathcal{B}$ of degree ≤ 2 over $\mathbb{Q}$. This is obvious in the case where E is ordinary, and requires work in the supersingular case. As in Goren-Lauter [9], we prove this by bounding the coefficients of $\iota(\mu)$. The main difficulty here was finding an appropriate isogeny s, as not every isogeny s allows us to find bounds.

Step 2 is to show that in the situation of Step 1, the field $\mathcal{B}_1$ embeds into K and the CM type is induced from $\mathcal{B}_1$, which contradicts the primitivity of the CM type. In order to show this, we use the tangent space of the Néron model at the zero section. No analogue of Step 2 was needed in the case of genus 2 because a quartic CM field containing an imaginary quadratic subfield has no primitive CM types.

The special case of $\overline{J} \cong E_1 \times E_2 \times E_3$ as p.p.a.v. where K does not contain an imaginary quadratic field is the main result of [3].

The following bound will be convenient in the sense that it allows us to formulate Theorem 1.1 and Proposition 4.1 without the need for case distinctions.

Lemma 2.4. *Let $B = -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$. Then B is an integer and $B \geq 2$.*

Proof. Recall that K_+ denotes the totally real cubic subfield of K. Since $\mu^2 \in \mathcal{O} \cap K_+$, we have $B \in \mathbb{Z}$. Since $K = \mathbb{Q}(\mu)$, the element μ^2 is totally negative and hence $B > 0$. Now suppose that $B = 1$. Let $a \geq b \geq c \geq 0$ be such that $-a, -b, -c$ are the images of μ^2 inside $\mathbb{R}$ under the three embeddings of K_+ into $\mathbb{R}$. Then $a + b + c = B = 1$, so each of a, b, c is in the interval $(0, 1)$. In particular, we get $\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^4) = a^2 + b^2 + c^2 < a + b + c = 1$. As this trace is a non-negative integer, it is zero, hence $a = b = c = 0$, contradiction. □

3. An embedding problem

Throughout Sections 3, 4 and 5, we fix a prime $\mathfrak{p} \mid p$ that is of good reduction for $J = \mathrm{Jac}(C)$ and not of potential good reduction for C. In particular, possibly after extending the base field, the reduction satisfies $\overline{J} \cong E \times A$ as polarized abelian varieties for a principally polarized abelian surface A and an elliptic curve E. Let $\mathcal{R} = \mathrm{End}(E)$ and $\mathcal{B} = \mathcal{R} \otimes \mathbb{Q}$, which is either a quaternion algebra or an imaginary quadratic field.

We write $K = \mathbb{Q}(\mu)$ where $\mu^2 \in \mathcal{O}$ is totally negative and generates the totally real subfield K_+ of K.

Let $\iota_0 : \mathcal{O} \hookrightarrow \mathrm{End}(E \times A)$ be the injective ring homomorphism coming from reduction of J at $\mathfrak{p}$ and write

$$\iota_0(\mu) =: \begin{pmatrix} x & y \\ z & w \end{pmatrix}, \tag{2}$$

where we have $x \in \mathcal{R}$, $y \in \mathrm{Hom}(A, E)$, $z \in \mathrm{Hom}(E, A)$ and $w \in \mathrm{End}(A)$; and the sizes of the boxes reflect the dimensions of the domains and codomains of the homomorphisms. We define a homomorphism

$$s = \begin{pmatrix} z & wz \end{pmatrix} : E \times E \longrightarrow A, \quad (P, Q) \longmapsto z(P) + wz(Q).$$

We first quickly eliminate the degenerate case where s is not an isogeny.

Lemma 3.1. *The homomorphism s is an isogeny.*

Proof. We will prove that z is not the zero map, and that the image $wz(E)$ of wz is not contained in $z(E)$. It then follows that the image of s has dimension 2 and hence s is an isogeny.

Suppose that z is the zero map. Then (2) gives that $x \in \mathcal{B}$ is a root of the minimal polynomial of μ, which is irreducible of degree 6, contradiction. Therefore, z is non-zero and $z(E) \subset A$ is an elliptic curve.

Now let $E' \subset A$ be an elliptic curve such that $s' : E \times E' \to A$, given by $(Q, R) \mapsto z(Q) + R$ is an isogeny. It follows that we have an isogeny

$$F' = 1 \times s' = \left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & z & 1 \end{array}\right) : E \times E \times E' \longrightarrow E \times A \text{ given by } (P, Q, R) \longmapsto (P, z(Q) + R)$$

and hence a further embedding $\iota_1' : \mathrm{End}(E \times A) \to \mathrm{End}(E \times E \times E') \otimes \mathbb{Q}$, $f \mapsto (F')^{-1} f F'$.

Let $\iota' = \iota_1' \circ \iota_0 : \mathcal{O} \to \mathrm{End}(E \times E \times E') \otimes \mathbb{Q}$. Next, we compute the matrix $\iota'(\mu)$. The first column is

$$(F')^{-1} \left(\begin{array}{c|c} x & y \\ \hline z & w \end{array}\right) F' \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & z & 1 \end{array}\right)^{-1} \left(\begin{array}{c} x \\ \hline z \end{array}\right) = \begin{pmatrix} x \\ 1 \\ 0 \end{pmatrix}. \tag{3}$$

Now suppose that $wz(E)$ is contained in $z(E)$. Then we get an element $z^{-1}wz \in \mathcal{B}$ and hence

$$\iota'(\mu) = \begin{pmatrix} x & * & * \\ 1 & z^{-1}wz & * \\ 0 & 0 & \delta \end{pmatrix} \quad \text{for some } \delta \in \mathrm{End}(E') \otimes \mathbb{Q}.$$

But then δ is a root of the minimal polynomial of μ, which is a contradiction, hence $wz(E)$ is not contained in $z(E)$ and the image of s has dimension 2. □

It follows that we have an isogeny

$$F = 1 \times s = \left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & z & wz \end{array}\right) \quad : \quad E^3 \longrightarrow E \times A \text{ given by } (P, Q, R) \longmapsto (P, s(Q, R))$$

and hence a further embedding $\iota_1 : \mathrm{End}(E \times A) \to \mathrm{End}(E^3) \otimes \mathbb{Q} \cong \mathrm{Mat}_{3\times 3}(\mathcal{B})$ given by $f \mapsto F^{-1} f F$. Let $\iota = \iota_1 \circ \iota_0 : \mathcal{O} \hookrightarrow \mathrm{Mat}_{3\times 3}(\mathcal{B})$. Let n be a positive integer such that $[n] \cdot \ker(s) = 0$ (from Lemma 4.3 onwards we will use a specific n). Then there exists an isogeny $\tilde{s} : A \to E \times E$ such that $s \cdot \tilde{s} = [n]$.

Lemma 3.2. *We have*

$$\iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix}, \quad \textit{where } x, a, b, c, d \in \mathcal{R}.$$

Proof. The first column is already computed in (3), which is also valid with F instead of F'. For the second column, we compute

$$F^{-1} \left(\begin{array}{c|c} x & y \\ \hline z & w \end{array}\right) F \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & z & wz \end{array}\right)^{-1} \left(\begin{array}{c} * \\ \hline wz \end{array}\right) = \begin{pmatrix} * \\ 0 \\ 1 \end{pmatrix}.$$

As $F^{-1} = 1 \times \frac{1}{n}\tilde{s}$, we get that the entries of the first row of $\iota(\mu)$ are in $\mathcal{R}$ and the others are in $\frac{1}{n}\mathcal{R}$. □

4. Bounds on the coefficients

Our goal in this section is to prove the following.

Proposition 4.1. *If $p > \frac{1}{8}B^{10}$, then the image $\iota(\mathcal{O})$ is inside the ring of 3×3 matrices over a field $\mathcal{B}_1 \subset \mathcal{B}$ of degree ≤ 2 over $\mathbb{Q}$.*

If $\mathcal{B}$ is a field, then we can take $\mathcal{B}_1 = \mathcal{B}$. So in the proof of Proposition 4.1, we assume that E is supersingular and $\mathcal{B}$ is a quaternion algebra. Then $\mathcal{B}$ is $B_{p,\infty}$, the quaternion algebra ramified exactly at p and ∞. Let Tr and N denote the *reduced* trace and norm on $\mathcal{B}$, and let $\cdot^\vee$ denote (quaternion) conjugation, so for all $x \in \mathcal{B}$, we have $\mathrm{N}(x) = xx^\vee = x^\vee x$, $\mathrm{Tr}(x) = x + x^\vee$, and $x^2 - \mathrm{Tr}(x)x + \mathrm{N}(x) = 0$. Note that $\mathcal{B} = B_{p,\infty}$ is a quaternion algebra ramified at infinity, hence a definite quaternion algebra, so the norm $\mathrm{N}(x)$ is a non-negative number and equal to zero if and only if $x = 0$.

To prove Proposition 4.1, we use the following result, which states that small quaternions commute.

Lemma 4.2 (Goren and Lauter)**.** *Let $\mathcal{R}$ be an order in the quaternion algebra $B_{p,\infty}$ and $x, y \in \mathcal{R}$. If $\mathrm{N}(x)\mathrm{N}(y) < p/4$, then x and y commute.*

Proof. We give the main idea for completeness. For details, see Lemma 2.1.1 and Corollary 2.1.2 of Goren and Lauter [9] and the proof of Lemma 9.5 of Streng [24].

If x and y do not commute, then 1, x, y, xy span a $\mathbb{Z}$-lattice $L \subset \mathcal{R} \subset B_{p,\infty}$ of covolume $\leq 4\mathrm{N}(x)\mathrm{N}(y)$, while $\mathcal{R}$ is contained in a maximal order of covolume p. This is a contradiction if $\mathrm{N}(x)\mathrm{N}(y) < p/4$. □

Recall that $\overline{J} \cong E \times A$ as principally polarized abelian varieties, where $A = (A, \lambda_A)$ is a principally polarized abelian surface. In other words, the natural polarization on $\overline{J}$ corresponds to the product polarization $1 \times \lambda_A$.

Lemma 4.3. *The polarization induced by $1 \times \lambda_A$ on E^3 via the isogeny F is*

$$\lambda := F^\vee(1 \times \lambda_A)F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \beta^\vee & \gamma \end{pmatrix} \quad \text{for some } \alpha, \gamma \in \mathbb{Z}_{>0} \text{ and } \beta \in \mathcal{R} \text{ such that } \alpha\gamma - \beta\beta^\vee \in \mathbb{Z}_{>0}.$$

Here $F^\vee$ denotes the dual isogeny. Let $n = \alpha\gamma - \beta\beta^\vee \in \mathbb{Z}_{>0}$. Then we have $GF = [n]$ for some isogeny G, and therefore $[n]\ker(F) = 0$.

Proof. The first column and row of λ are easy to compute. The symmetry (i.e., $\alpha, \gamma \in \mathbb{Z}$ and the occurrence of $\beta^\vee$) is Mumford [19, (3) on page 190] (equivalently the first part of Application III on page 208 of loc. cit.). The positive-definiteness (which implies $\alpha, \gamma, n > 0$) is the last paragraph of Application III on page 210 of loc. cit.). It is now straightforward to compute $GF = [n]$ for

$$G = \begin{pmatrix} n & 0 & 0 \\ 0 & \gamma & -\beta \\ 0 & -\beta^\vee & \alpha \end{pmatrix} F^\vee(1 \times \lambda_A).$$

It follows that the kernel of F is contained in the kernel of $[n]$. □

From now on, take n as in Lemma 4.3.

Lemma 4.4 (Proposition 4.8 in [3])**.** *For every $\eta \in K$, the complex conjugate $\overline{\eta} \in K$ satisfies*

$$\iota(\overline{\eta}) = \lambda^{-1}\iota(\eta)^\vee\lambda,$$

where for a matrix M, we use $M^\vee$ to denote the transpose of M with conjugate entries.

Proof. Complex conjugation is the Rosati involution, so $\iota_0(\overline{\eta}) = (1 \times \lambda_A)^{-1}\iota_0(\eta)^\vee(1 \times \lambda_A)$. Conjugation with F^{-1} now yields exactly the equality in the lemma:

$$\begin{aligned} \iota(\overline{\eta}) &= F^{-1}(1 \times \lambda_A)^{-1}\iota_0(\eta)^\vee(1 \times \lambda_A)F \\ &= (F^{-1}(1 \times \lambda_A)^{-1}F^{-\vee})(F^\vee\iota_0(\eta)^\vee F^{-\vee})(F^\vee(1 \times \lambda_A)F) \\ &= (F^\vee(1 \times \lambda_A)F)^{-1}(F^{-1}\iota_0(\eta)F)^\vee(F^\vee(1 \times \lambda_A)F) = \lambda^{-1}\iota(\eta)^\vee\lambda. \end{aligned}$$

□

For $\eta = \mu$, Lemma 4.4 reads $-\lambda\iota(\mu) = \iota(\mu)^\vee\lambda$, that is,

$$\begin{pmatrix} -x & -a & -b \\ -\alpha & -\beta & -\alpha c/n - \beta d/n \\ -\beta^\vee & -\gamma & -\beta^\vee c/n - \gamma d/n \end{pmatrix} = \begin{pmatrix} x^\vee & \alpha & \beta \\ a^\vee & \beta^\vee & \gamma \\ b^\vee & (c^\vee/n)\alpha + (d^\vee/n)\beta^\vee & (c^\vee/n)\beta + (d^\vee/n)\gamma \end{pmatrix}.$$

We conclude

$$\begin{aligned} x^\vee &= -x \qquad \text{(equivalently } \mathrm{Tr}(x) = 0\text{)}, \\ a &= -\alpha \qquad \text{(and we already knew } \alpha \in \mathbb{Z}_{>0}\text{)}, \\ b &= -\beta = \beta^\vee \qquad \text{(hence } \mathrm{Tr}(\beta) = 0\text{)}, \\ \gamma &= -\alpha c/n - \beta d/n \qquad \text{(and we already knew } \gamma \in \mathbb{Z}_{>0}\text{)}, \\ \mathrm{Tr}(\beta^\vee c) + \mathrm{Tr}(\gamma d) &= 0. \end{aligned} \tag{4}$$

Lemma 4.5 (Lemma 6.12 in [3])**.** *For every $\eta \in K$, the trace $\mathrm{Tr}_{K/\mathbb{Q}}(\eta)$ is equal to the sum of the reduced traces of the three diagonal entries of $\iota(\eta) \in \mathrm{Mat}_{3\times 3}(\mathcal{B})$.*

Proof. Choose a prime $l \nmid np$. Then $\mathrm{Tr}_{K/\mathbb{Q}}(\eta)$ equals the trace of η when acting on $T_l(J) \otimes \mathbb{Q}$, where $T_l(J)$ is the l-adic Tate module of J. This action is preserved by reduction modulo $\mathfrak{p}$. Moreover, the isogeny F induces an isomorphism of l-adic Tate modules, hence $\mathrm{Tr}_{K/\mathbb{Q}}(\eta)$ equals the trace of $\iota(\eta)$ when acting on $T_l(E \times E \times E) \otimes \mathbb{Q}$. The latter trace is exactly the sum of the traces of the actions of the diagonal entries of $\iota(\eta)$ on $T_l(E) \otimes \mathbb{Q}$, which are the reduced traces. □

Remark 4.6. *Lemma 6.12 in* [3] *follows from a special case of Lemma 4.5 in which η is an element of the totally real cubic subfield K_+ of K and the diagonal entries of $\iota(\eta)$ are integers.*

Since both $\mathrm{Tr}_{K/\mathbb{Q}}(\mu)$ and $\mathrm{Tr}(x)$ are 0, Lemma 4.5 applied to μ gives

$$\mathrm{Tr}(d) = 0. \tag{5}$$

Let $B = -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2) \in \mathbb{Z}_{>0}$. Then Lemmas 4.5 and 3.2 give

$$B = -\frac{1}{2}\left(\mathrm{Tr}(x^2) + 2\mathrm{Tr}(a) + 2\mathrm{Tr}\Big(\frac{c}{n}\Big) + \mathrm{Tr}\Big(\frac{d^2}{n^2}\Big)\right). \tag{6}$$

On the other hand, the equality (5) implies $d^\vee = -d$ hence we have $\mathrm{Tr}(d^2/n^2) = -2\mathrm{N}(d/n)$ as $n \in \mathbb{Z}_{>0}$. Similary, by (4) we have $\mathrm{Tr}(x^2) = -2\mathrm{N}(x)$. Moreover, the equality $\gamma = -\alpha c/n - \beta d/n$ in (4) and the fact that γ and α are integers give $\mathrm{Tr}(c/n) = -\mathrm{Tr}(\gamma/\alpha + \beta d/(n\alpha)) = -2\gamma/\alpha - \mathrm{Tr}(\beta d/(n\alpha))$. Therefore, by $a = -\alpha \in \mathbb{Z}$ in (4), we get

$$B = \mathrm{N}(x) + 2\alpha + 2\frac{\gamma}{\alpha} + \mathrm{Tr}\Big(\frac{\beta d}{n\alpha}\Big) + \mathrm{N}\Big(\frac{d}{n}\Big). \tag{7}$$

If we manage to rewrite this as a sum of terms that are all non-negative, then this bounds the individual terms from above by B.

Note that we recognize the final two terms as terms in the expansion

$$\mathrm{N}\Big(\frac{\beta}{\alpha} + \frac{d^\vee}{n}\Big) = \frac{\mathrm{N}(\beta)}{\alpha^2} + \mathrm{Tr}\Big(\frac{\beta d}{\alpha n}\Big) + \mathrm{N}\Big(\frac{d}{n}\Big), \quad \text{so we get} \quad B = \mathrm{N}(x) + 2\alpha + 2\frac{\gamma}{\alpha} - \frac{\mathrm{N}(\beta)}{\alpha^2} + \mathrm{N}\Big(\frac{\beta}{\alpha} + \frac{d^\vee}{n}\Big).$$

Next, by the definition of n in Lemma 4.3, we have $n = \alpha\gamma - \mathrm{N}(\beta)$, so $n/\alpha^2 = \gamma/\alpha - \mathrm{N}(\beta)/\alpha^2$, which again allows us to replace two terms, and get

$$B = \mathrm{N}(x) + 2\alpha + \frac{\gamma}{\alpha} + \frac{n}{\alpha^2} + \mathrm{N}\Big(\frac{\beta}{\alpha} + \frac{d^\vee}{n}\Big), \tag{8}$$

in which finally all terms are non-negative, as the norm of an element of $\mathcal{B}_{p,\infty}$ is non-negative. We immediately get that each of the individual terms is at most B. So e.g., $\mathrm{N}(x) \le B$, $2\alpha \le B$, $\gamma/\alpha \le B$. Hence we obtain

$$\mathrm{N}(\beta)/\alpha^2 = \frac{\alpha\gamma - n}{\alpha^2} \le \gamma/\alpha \le B. \tag{9}$$

In order to bound $\mathrm{N}(d)$, we use the following well-known (in)equalities.

Lemma 4.7 (Parallelogram law)**.** *For all $e, f \in \mathcal{B}$, we have $N(e+f) + N(e-f) = 2(N(e) + N(f))$.*

Proof. By writing it out, the cross terms cancel on the left-hand side and do not appear on the right. □

Corollary 4.8. *For all $f, g \in \mathcal{B}$, we have $N(g) \le 2(N(g+f) + N(f))$.*

Proof. From the lemma, we have $\mathrm{N}(e-f) \le 2(\mathrm{N}(e) + \mathrm{N}(f))$, which we apply to $e = g + f$. □

Corollary 4.8, with (8) and (9), now gives

$$\mathrm{N}(d^\vee/n) \;\le\; 2\mathrm{N}(\beta)/\alpha^2 + 2\mathrm{N}(\beta/\alpha + d^\vee/n) \;\le\; 2(\gamma/\alpha + \mathrm{N}(\beta/\alpha + d^\vee/n)) \;\le\; 2B.$$

As we also have

$$n \le \alpha\gamma \le \alpha^2 B \le \frac{1}{4}B^3, \tag{10}$$

this gives $\mathrm{N}(d^\vee) = n^2\mathrm{N}(d^\vee/n) \le \frac{1}{8}B^7$.

Recall that our goal is to prove the following:

Proposition 4.1. *If $p > \frac{1}{8}B^{10}$, then the image $\iota(\mathcal{O})$ is inside the ring of 3×3 matrices over a field $\mathcal{B}_1 \subset \mathcal{B}$ of degree ≤ 2 over $\mathbb{Q}$.*

Proof. Suppose $p > \frac{1}{8}B^{10}$. As μ generates K, it suffices to show that the entries $\{x, a, b, c/n, d/n\}$ of $\iota(\mu)$ are in a field $\mathcal{B}_1$. Recall that (4) gives $-a = \alpha, \gamma, n \in \mathbb{Z}_{>0}$, $b = -\beta$ and $c = -\frac{n\gamma}{\alpha} - \frac{\beta d}{\alpha}$. In particular, it suffices to prove that the elements of $\{x, \beta, d\}$ lie in a field $\mathcal{B}_1$, for which it suffices to prove that they commute. We have $\mathrm{N}(x) \leq B$, $\mathrm{N}(\beta) \leq \frac{1}{4}B^3$, $\mathrm{N}(d) \leq \frac{1}{8}B^7$ and $B \geq 2$ (Lemma 2.4), hence the product of any pair of distinct elements of $\{x, \beta, d\}$ has norm less than $p/4$. Therefore, by Lemma 4.2, every pair of elements commutes. □

If $p > \frac{1}{8}B^{10}$, then $\iota(\mu)$ is a matrix over $\mathcal{B}_1$. Let f be the minimal polynomial of μ over $\mathbb{Q}$, which has degree 6. Then $f(\iota(\mu)) = 0$, hence f is divisible by the (at most cubic) minimal polynomial of $\iota(\mu)$ over the (at most quadratic) field $\mathcal{B}_1$. Therefore, the field $K = \mathbb{Q}(\mu)$ contains a subfield isomorphic to $\mathcal{B}_1$ and $\mathcal{B}_1$ is quadratic. We now identify $\mathcal{B}_1$ with this subfield through a choice of embedding.

This finishes the proof of Theorem 1.1 in the case where K has no imaginary quadratic subfield.

5. If the CM field contains an imaginary quadratic subfield

In this section, we finish the proof of Theorem 1.1. By the argument at the end of the previous section, we are left with the case where $\iota(\mu)$ has entries in an imaginary quadratic subfield $\mathcal{B}_1$ of $\mathcal{B}$. We have identified $\mathcal{B}_1$ with the subfield $K_1 \subset K$ through a choice of embedding.

Let $p > \frac{1}{8}B^{10}$ be a prime where B is as in Section 4. Recall that we have a curve C over a number field M and a prime $\mathfrak{p} \mid p$ of M such that $J = \mathrm{Jac}(C)$ has good reduction at $\mathfrak{p}$, but C does not have potential good reduction at $\mathfrak{p}$. By extending M if necessary, assume without loss of generality that M contains the images of all embeddings $K \hookrightarrow \overline{M}$.

Recall that the CM type is primitive, hence is not induced by a CM type of $\mathcal{B}_1 = K_1 \subset K$. This means that the CM type induces two distinct embeddings of $\mathcal{B}_1$ into M. This primitivity will play a crucial role in our proof of Theorem 1.1. We will need to be able to distinguish between the two embeddings in characteristic p, for which we will use an element $\sqrt{-\delta} \in \mathcal{O}$ with $\delta \in \mathbb{Z}_{>0}$ and $p \nmid 2\delta$. Such an element automatically exists if $p \nmid 2\Delta(\mathcal{O})$, which is a relatively weak condition to have in a result like Theorem 1.1. However, we do not even need to add such a condition to the theorem because of the following lemma.

Lemma 5.1. *Let $B = -\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$ and suppose that $p > \frac{1}{4}B^{7.5}$. Then there exists a $\delta \in \mathbb{Z}_{>0}$ coprime to p such that $\sqrt{-\delta} \in \mathcal{O} \cap \mathcal{B}_1$.*

Proof. We will prove the lemma with $\delta = -\Delta(\mathcal{O} \cap \mathcal{B}_1)$. Then $\sqrt{-\delta} \in \mathcal{O} \cap \mathcal{B}_1$ and $\delta \in \mathbb{Z}_{>0}$ since $\mathcal{B}_1$ is imaginary quadratic. We must show that δ is coprime to p. Note that $\Delta(\mathcal{O} \cap \mathcal{B}_1) = [\mathcal{O}_{\mathcal{B}_1} : \mathcal{O} \cap \mathcal{B}_1]^2 \Delta(\mathcal{O}_{\mathcal{B}_1})$. So it will suffice to prove that both $[\mathcal{O}_{\mathcal{B}_1} : \mathcal{O} \cap \mathcal{B}_1]$ and $\Delta(\mathcal{O}_{\mathcal{B}_1})$ are coprime to p, which we do by showing that they are smaller than $\frac{1}{4}B^{7.5}$ in absolute value.

Let $a \geq b \geq c \geq 0$ be such that the images of μ for the embeddings $K \to \mathbb{C}$ are $\{\pm ai, \pm bi, \pm ci\}$, so $B = a^2 + b^2 + c^2$. We have

$$\begin{aligned}[\mathcal{O} : \mathbb{Z}[\mu]]^2 [\mathcal{O}_K : \mathcal{O}]^2 |\Delta(\mathcal{O}_K)| = |\Delta(\mathbb{Z}[\mu])| &= (2a)^2(2b)^2(2c)^2(a-b)^4(a+b)^4(a-c)^4(a+c)^4(b-c)^4(b+c)^4 \\ &= 2^6 a^2 b^2 c^2 (a^2-b^2)^4 (a^2-c^2)^4 (b^2-c^2)^4,\end{aligned}$$

which, by the inequality of arithmetic and geometric means, is less than or equal to

$$2^6 \left(\frac{a^2+b^2+c^2}{3}\right)^3 \left(\frac{a^2-b^2+a^2-c^2+b^2-c^2}{3}\right)^{12} \leq 2^{6+12} 3^{-(3+12)} B^{15} < 0.019 B^{15}. \tag{11}$$

Since $\frac{\mathcal{O}_{\mathcal{B}_1}}{\mathcal{O} \cap \mathcal{B}_1} \hookrightarrow \frac{\mathcal{O}_K}{\mathcal{O}}$, by (11) we get $[\mathcal{O}_{\mathcal{B}_1} : \mathcal{O} \cap \mathcal{B}_1]^2 \leq [\mathcal{O}_K : \mathcal{O}]^2 < 0.019 B^{15}$ which gives $[\mathcal{O}_{\mathcal{B}_1} : \mathcal{O} \cap \mathcal{B}_1] < 0.14 B^{7.5}$, as desired. Now for $\Delta(\mathcal{O}_{\mathcal{B}_1})$, we use the tower law for discriminants and (11) to get

$$|\Delta(\mathcal{O}_{\mathcal{B}_1})|^3 \leq |\Delta(\mathcal{O}_{\mathcal{B}_1})^3 N_{\mathcal{B}_1/\mathbb{Q}}(\Delta_{K/\mathcal{B}_1})| = |\Delta(\mathcal{O}_K)| < 0.019 B^{15}.$$

Hence $|\Delta(\mathcal{O}_{\mathcal{B}_1})| < 0.27 B^5 < \frac{1}{4}B^{7.5}$ (by Lemma 2.4) and our proof is complete. □

5.1. **Some facts about tangent spaces.** In order to detect the CM type (and its all-important primitivity), we use the tangent space to $J = \mathrm{Jac}(C)$ at the identity. For our discussion, we collect some necessary notions about tangent spaces. We use the definition of tangent space as given by Demazure in Exposé II of SGA 3 [7] in the special case of a scheme over an affine base scheme. This requires the use of the ring of dual numbers.

Definition 5.2. *For any commutative ring R, let $R[\epsilon]$ denote the R-algebra of dual numbers over R. It is free with basis $1, \epsilon$ as an R-module and the R-algebra structure comes from setting $\epsilon^2 = 0$.*

The natural inclusion $R \hookrightarrow R[\epsilon]$ induces the structure morphism $\rho : \mathrm{Spec}(R[\epsilon]) \to \mathrm{Spec}(R)$. The natural map $R[\epsilon] \to R$ which sends $\epsilon \mapsto 0$ induces a section $\sigma : \mathrm{Spec}(R) \to \mathrm{Spec}(R[\epsilon])$, called the zero section.

Let $X \to S = \mathrm{Spec}(R)$ be a morphism of schemes and let $u \in X(S) = \mathrm{Hom}_S(S, X)$. In [7], Demazure defines a commutative S-group scheme called the tangent space of X/S at u. We will denote the tangent space of X/S at u by $T^u_{X/S}$. For a commutative R-algebra R', let $t : \mathrm{Spec}(R') \to \mathrm{Spec}(R)$ denote the structure morphism. The set $T^u_{X/S}(R')$ is defined to be the collection of S-morphisms $\theta : \mathrm{Spec}(R'[\epsilon]) \to X$ making the following diagram commute:

$$\begin{array}{ccc} \mathrm{Spec}(R'[\epsilon]) & \xrightarrow{\theta} & X \\ \uparrow{\scriptstyle \sigma} & & \uparrow{\scriptstyle u} \\ \mathrm{Spec}(R') & \xrightarrow[t]{} & \mathrm{Spec}(R) \end{array}$$

We now gather some general facts about tangent spaces that we will need in our discussion.

Proposition 5.3. *The set $T^u_{X/S}(R')$ has a canonical R'-module structure. The zero element is the map $u \circ t \circ \rho$ where $\rho : \mathrm{Spec}(R'[\epsilon]) \to \mathrm{Spec}(R')$ denotes the structure morphism.*

Proof. This is a slight generalization of the lemma with tag 0B2B in the Stacks Project [1]. The proof is the same; we recall the main ingredients here for the reader's convenience. We have a pushout in the category of schemes

$$\mathrm{Spec}(R'[\epsilon]) \sqcup_{\mathrm{Spec}(R')} \mathrm{Spec}(R'[\epsilon]) = \mathrm{Spec}(R'[\epsilon_1, \epsilon_2])$$

where $R'[\epsilon_1, \epsilon_2]$ is the R'-algebra with basis $1, \epsilon_1, \epsilon_2$ and $\epsilon_1^2 = \epsilon_1\epsilon_2 = \epsilon_2^2 = 0$. Given two S-morphisms $\theta_1, \theta_2 : \mathrm{Spec}(R'[\epsilon]) \to X$, we construct an S-morphism

$$\theta_1 + \theta_2 \quad : \quad \mathrm{Spec}(R'[\epsilon]) \longrightarrow \mathrm{Spec}(R'[\epsilon_1, \epsilon_2]) \xrightarrow{\theta_1, \theta_2} X \tag{12}$$

where the first arrow is given by $\epsilon_i \mapsto \epsilon$. Now for scalar multiplication, given $\lambda \in R'$ there is a selfmap of $\mathrm{Spec}(R'[\epsilon])$ corresponding to the R'-algebra endomorphism of $R'[\epsilon]$ which sends ϵ to $\lambda\epsilon$. Precomposing $\theta : \mathrm{Spec}(R'[\epsilon]) \to X$ with this selfmap gives $\lambda \cdot \theta$. The axioms of a vector space are verified by exhibiting suitable commutative diagrams of schemes. The statement about the zero element follows immediately from the description of the addition law (12). □

Proposition 5.4. *Let v be the composition $v : \mathrm{Spec}(R') \xrightarrow{t} S \xrightarrow{u} X$. Then there is an isomorphism of R'-modules $T^u_{X/S}(R') \cong \mathrm{Hom}_{R'}(v^*(\Omega^1_{X/S}), R')$, where $\Omega^1_{X/S}$ denotes the sheaf of relative differentials of X/S.*

Proof. See Remark 3.6.1 and footnote (25) in [7]. □

Proposition 5.5. *Let X and Y be schemes over S and let $f : X \to Y$ be an S-morphism. Then f induces an S-morphism $T(f) : T^u_{X/S} \to T^{f\circ u}_{Y/S}$, called the derived morphism, with the following properties:*

(1) $T(f \circ g) = T(f) \circ T(g)$;
(2) $T(f)$ induces an R'-module homomorphism $T^u_{X/S}(R') \to T^{f\circ u}_{Y/S}(R')$.

Furthermore, suppose that G is a group scheme over S with identity section e and $n_G : G \to G$ is the S-morphism $g \to g^n$ for $n \in \mathbb{Z}$. Then the derived morphism $T(n_G) : T^e_{G/S} \to T^e_{G/S}$ is multiplication by n, meaning it sends $x \in T^e_{G/S}(R')$ to nx.

Proof. See [7], Proposition 3.7.bis and Corollaire 3.9.4. If $\theta : \mathrm{Spec}(R'[\epsilon]) \to X$ is an element of $T^u_{X/S}(R')$, then $T(f)$ sends θ to $f \circ \theta$. This clearly preserves the R'-module structure described in Proposition 5.3. □

Proposition 5.6 (Proposition 3.8 in [7])**.** *Let X and Y be schemes over S. Then $T^u_{X/S} \times_S T^w_{Y/S} \cong T^{(u,w)}_{(X\times_S Y)/S}$.*

5.2. **The proof of Theorem 1.1.** Now we will apply these general facts about tangent spaces to our specific case. We want to relate the tangent space of J at the identity to the tangent space of its reduction modulo $\mathfrak{p}$ at the identity. For this we will use the tangent space at the identity section of a Néron model of J/M.

Let $\mathcal{O}_\mathfrak{p}$ be the valuation ring of $\mathfrak{p}$ and let $\mathfrak{K} = \mathcal{O}_M/\mathfrak{p}$ be the residue field. Let $\mathcal{J}/\mathcal{O}_\mathfrak{p}$ be a Néron model for J/M and let $\overline{J}/\mathfrak{K}$ be the special fibre of $\mathcal{J}$. Let $\tilde{e} : \mathrm{Spec}(\mathcal{O}_\mathfrak{p}) \to \mathcal{J}$, $e : \mathrm{Spec}(M) \to J$ and $e_0 : \mathrm{Spec}(\mathfrak{K}) \to \overline{J}$ be the identity sections of $\mathcal{J}$, J and $\overline{J}$ respectively.

Lemma 5.7. *The $\mathcal{O}_\mathfrak{p}$-module $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p})$ is free of rank 3. Furthermore, there are natural isomorphisms*

$$T^{e}_{J/M}(M) \cong T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}) \otimes_{\mathcal{O}_\mathfrak{p}} M \qquad \text{and} \qquad T^{e_0}_{\overline{J}/\mathfrak{K}}(\mathfrak{K}) \cong T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}) \otimes_{\mathcal{O}_\mathfrak{p}} \mathfrak{K} \tag{13}$$

as vector spaces over M and $\mathfrak{K}$ respectively. Moreover, the isomorphisms (13) *respect the action of $T(f)$ for $f \in \mathrm{End}_{\mathcal{O}_\mathfrak{p}}(\mathcal{J}) = \mathrm{End}_M(J)$.*

Proof. By [18, Proposition 6.2.5], $\Omega^1_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}$ is free of rank 3 in a neighborhood of the image of e_0. Note that any such neighborhood contains the image of $\tilde{e}$. Therefore, $\tilde{e}^*(\Omega^1_{\mathcal{J}/\mathcal{O}_\mathfrak{p}})$ is a free $\mathcal{O}_\mathfrak{p}$-module of rank 3. Now Proposition 5.4 implies that the same is true of $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p})$. Likewise, $T^{e}_{J/M}(M)$ and $T^{e_0}_{\overline{J}/\mathfrak{K}}(\mathfrak{K})$ are vector spaces of dimension 3 over M and $\mathfrak{K}$, respectively.

We have canonical identifications $T^{e}_{J/M}(M) = T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(M)$ and $T^{e_0}_{\overline{J}/\mathfrak{K}}(\mathfrak{K}) = T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathfrak{K})$. Let $F \in \{M, \mathfrak{K}\}$ and let $t : \mathrm{Spec}(F[\epsilon]) \to \mathrm{Spec}(\mathcal{O}_\mathfrak{p}[\epsilon])$ be the natural map. Then precomposing an element $\theta \in T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p})$ with t gives an element of $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(F)$. The $\mathcal{O}_\mathfrak{p}$-bilinear map $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}) \times F \to T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(F)$ given by $(\theta, \lambda) \mapsto \lambda \cdot (\theta \circ t)$ induces a homomorphism of F-vector spaces $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}) \otimes_{\mathcal{O}_\mathfrak{p}} F \to T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(F)$. One can check that this map is injective using the description of the zero element given in Proposition 5.3. Surjectivity follows by comparing dimensions. Finally, the action of $T(f)$, as described in Proposition 5.5, is clearly preserved. □

The main ingredient for the proof of Theorem 1.1 is the following proposition.

Proposition 5.8. *Let B and δ be as in Lemma 5.1, and suppose that $p > \frac{1}{8}B^{10}$. Then there is an invertible matrix $P \in \mathrm{Mat}_{3\times 3}(\mathcal{B}_1)$ such that*

$$P\iota(\sqrt{-\delta})P^{-1} = \pm \begin{pmatrix} \sqrt{-\delta} & 0 & 0 \\ 0 & \sqrt{-\delta} & 0 \\ 0 & 0 & -\sqrt{-\delta} \end{pmatrix}.$$

Proof. By Proposition 4.1, reduction at a prime above $p > \frac{1}{8}B^{10}$ induces a $\mathbb{Q}$-algebra homomorphism $\iota : K \hookrightarrow \mathrm{End}(E^3) \otimes \mathbb{Q} = \mathrm{Mat}_3(\mathcal{B})$ with image contained in $\mathrm{Mat}_3(\mathcal{B}_1)$, the ring of 3×3 matrices over $\mathcal{B}_1$. Since $\iota(\sqrt{-\delta})^2 = -\delta I_3$ and $\sqrt{-\delta} \in \mathcal{B}_1$, we can take a change of basis over $\mathcal{B}_1$ to diagonalize the matrix $\iota(\sqrt{-\delta})$. Moreover, the eigenvalues of $\iota(\sqrt{-\delta})$ are in $\{\pm\sqrt{-\delta}\}$. It suffices to show that $\iota(\sqrt{-\delta})$ has two distinct eigenvalues, i.e. $\iota(\sqrt{-\delta}) \neq \pm\sqrt{-\delta} I_3$. For this we will use the primitivity of the CM type. In order to detect the CM type, we will use the tangent space to $J = \mathrm{Jac}(C)$ at the identity.

By the Néron mapping property, $\sqrt{-\delta}$ has a unique extension to an $\mathcal{O}_\mathfrak{p}$-endomorphism of the Néron model $\mathcal{J}$, which we will denote by φ. Applying Proposition 5.5, we get an endomorphism $T(\varphi)$ of $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}$ which induces an $\mathcal{O}_\mathfrak{p}$-linear endomorphism of $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p})$. By the definition of primitivity of the CM type (Definitions 2.2 and 2.3), the action of $T(\varphi)$ on $T^{e}_{J/M}(M)$ has two distinct eigenvalues, $\sqrt{-\delta}$ and $-\sqrt{-\delta} \in \mathcal{O}_\mathfrak{p}$. By Lemmas 2.4 and 5.1, the two eigenvalues $\pm\sqrt{-\delta}$ remain distinct in the residue field $\mathfrak{K}$, which has characteristic $p > \frac{1}{8}B^{10} \geq \frac{1}{4}B^{7.5} > 2$. Therefore, applying Lemma 5.7 again, we see that the action of $T(\varphi)$ on $T^{e_0}_{\overline{J}/\mathfrak{K}}(\mathfrak{K})$ has two distinct eigenvalues.

Now, let the isogeny $F : E^3 \to \overline{J}$ be as in Sections 3 and 4. By Lemma 4.3, there is an integer $n > 0$ and an isogeny $G : \overline{J} \to E^3$ such that GF is multiplication by n on E^3. Then $\iota(\sqrt{-\delta}) = n^{-1}G\overline{\varphi}F$, where $\overline{\varphi}$ denotes the $\mathfrak{K}$-endomorphism of $\overline{J}$ induced by φ. Recall from (10) in Section 4 that $0 < n \leq \frac{B^3}{4} < \frac{1}{8}B^{10} < p$. Therefore, n is invertible in $\mathfrak{K}$ and Proposition 5.5 gives

$$T(G\overline{\varphi}F) = T(G) \circ T(\varphi) \circ T(F) = nn^{-1}T(G) \circ T(\varphi) \circ T(F) = nT(F)^{-1} \circ T(\varphi) \circ T(F).$$

The right-hand side is n times a conjugate of $T(\varphi)$, whereby its eigenvalues in $\overline{\mathfrak{K}}$ are n times those of $T(\varphi)$. Therefore, $T(G\overline{\varphi}F)$ has two distinct eigenvalues in $\mathfrak{K}$ for its action on the tangent space $T^0_{E^3/\mathfrak{K}}(\mathfrak{K})$ of E^3 at the identity. By Proposition 5.6, we have $T^0_{E^3/\mathfrak{K}}(\mathfrak{K}) \cong T^0_{E/\mathfrak{K}}(\mathfrak{K}) \oplus T^0_{E/\mathfrak{K}}(\mathfrak{K}) \oplus T^0_{E/\mathfrak{K}}(\mathfrak{K})$ where $T^0_{E/\mathfrak{K}}(\mathfrak{K})$ denotes the tangent space of E at the identity. Now suppose that $n\iota(\sqrt{-\delta}) = \pm n\sqrt{-\delta}I_3$. Then $T(G\overline{\varphi}F) = T(n\iota(\sqrt{-\delta})) = \pm n\sqrt{-\delta}I_3$ has only one eigenvalue. Contradiction. □

Proof of Theorem 1.1. Suppose that $p > \frac{1}{8}B^{10}$. Recall from the end of Section 4 that $\iota(\mu)$ has coefficients in a quadratic field $\mathcal{B}_1 \ni \sqrt{-\delta}$. Applying Proposition 5.8, we see that since μ commutes with $\sqrt{-\delta}$, the matrix $P\iota(\mu)P^{-1}$ is of the form

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

But this means that the bottom right entry of $P\iota(\mu)P^{-1}$ is a root of the (irreducible degree six) minimal polynomial of μ over $\mathbb{Q}$. This gives a contradiction because the entries of the matrix $P\iota(\mu)P^{-1}$ lie in the quadratic field $\mathcal{B}_1$. This completes the proof of Theorem 1.1. □

6. Geometry of numbers

The following is a reformulation and proof of Proposition 1.4.

Proposition 6.1. *Let $\mathcal{O}$ be an order in a sextic CM field K with totally real cubic subfield K_+.*

(1) If K contains no imaginary quadratic subfield, then there exists $\mu \in \mathcal{O}$ such that $K = \mathbb{Q}(\mu)$ and μ^2 is a totally negative element in K_+ with $0 < -\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) \le (\frac{6}{\pi})^{2/3}|\Delta(\mathcal{O})|^{1/3}$.

(2) If K contains an imaginary quadratic subfield K_1, we write $\mathcal{O}_i = K_i \cap \mathcal{O}$ for $i \in \{1, +\}$. Then $\exists\ \mu \in \mathcal{O}$ such that $K = \mathbb{Q}(\mu)$ and μ^2 is a totally negative element in K_+ satisfying

$$0 < -\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) \le |\Delta(\mathcal{O}_1)|(1 + 2\sqrt{|\Delta(\mathcal{O}_+)|}).$$

Proof. Let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the set of embeddings of K into $\mathbb{C}$ up to complex conjugation. We identify $K \otimes_{\mathbb{Q}} \mathbb{R}$ with $\mathbb{C}^3$ via the $\mathbb{R}$-algebra isomorphism $K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}^3 : x \otimes a \mapsto (a\phi_1(x), a\phi_2(x), a\phi_3(x))$.
(1) The order $\mathcal{O} \subset K$ is a lattice of co-volume $2^{-3}|\Delta(\mathcal{O})|^{1/2}$ in $\mathbb{C}^3$. We define the symmetric convex body

$$\mathcal{C}_R = \{x = (x_1, x_2, x_3) \in \mathbb{C}^3 : |\mathrm{Re}(x_i)| < 1 \text{ for all } i,\ \sum_i \mathrm{Im}(x_i)^2 < R^2\} \subset \mathbb{C}^3.$$

Next, we claim that if $R = (\frac{3}{4\pi})^{1/3}|\Delta(\mathcal{O})|^{1/6} + \epsilon$ for some $\epsilon > 0$, then there is a non-zero $\gamma \in \mathcal{O} \cap \mathcal{C}_R$ such that $K = \mathbb{Q}(\gamma)$. Indeed, suppose that $R = (\frac{3}{4\pi})^{1/3}|\Delta(\mathcal{O})|^{1/6} + \epsilon$. Then we have

$$\mathrm{vol}(\mathcal{C}_R) = 2^3(\frac{4}{3}\pi R^3) > 2^3|\Delta(\mathcal{O})|^{1/2} = 2^6 \mathrm{covol}(\mathcal{O}).$$

By Minkowski's first convex body theorem (see Siegel [22, Theorem 10]), there is a non-zero element γ in $\mathcal{O} \cap \mathcal{C}_R$. If $\gamma \in K_+$, then we have $|\mathrm{N}_{K_+/\mathbb{Q}}(\gamma)| = \prod_{\phi_i \in \Phi} |\mathrm{Re}(\phi_i(\gamma))| < 1$, so we get $\gamma = 0$, a contradiction. Hence $\gamma \in \mathcal{O} \cap \mathcal{C}_R$ and $\gamma \notin K_+$. To prove the claim, it only remains to prove that γ generates K. As K has degree 6, the field generated by γ has degree 1, 2, 3 or 6. Since any subfield of a CM field is either totally real or a CM field, we find that either γ is totally real (hence in K^+, contradiction), or generates a CM subfield of K. As CM fields have even degree and we are in case (1), where K has no imaginary quadratic subfield, we find that $\mathbb{Q}(\gamma) = K$. This proves the claim.

Let $\mu = \gamma - \overline{\gamma}$. Then μ^2 is a totally negative element in K_+, hence $\mathbb{Q}(\mu) = K$. We get

$$-\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) = -\sum_i \phi_i(\mu^2) = -\sum_{\phi_i \in \Phi} \phi_i((\gamma - \overline{\gamma})^2) = 4\sum_i \mathrm{Im}(\phi_i(\gamma))^2 < 4R^2.$$

Since γ 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 $-\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) \le 4(\frac{3}{4\pi})^{2/3}|\Delta(\mathcal{O})|^{1/3} = (\frac{6}{\pi})^{2/3}|\Delta(\mathcal{O})|^{1/3}$, which proves (1).
(2) The order $\mathcal{O}_+ \subset K_+$ is a lattice of co-volume $|\Delta(\mathcal{O}_+)|^{1/2}$ in $\mathbb{R}^3$. We define the symmetric convex body

$$\mathcal{C}_R = \{x = (x_1, x_2, x_3) \in \mathbb{R}^3 : |x_1| < 1, |x_2| < R, |x_3| < R\} \subset \mathbb{R}^3.$$

Next, we claim that if $R = |\Delta(\mathcal{O}_+)|^{1/4} + \epsilon$ for some $\epsilon > 0$, then there is a non-zero $\gamma \in \mathcal{O}_+ \cap \mathcal{C}_R$ such that $\gamma \in K_+ \smallsetminus \mathbb{Q}$. Indeed, we then have $\mathrm{vol}(\mathcal{C}_R) = 2^3 R^2 > 2^3 |\Delta(\mathcal{O}_+)|^{1/2} = 2^3 \mathrm{covol}(\mathcal{O}_+)$. By Minkowski's first convex body theorem (see Siegel [22, Theorem 10]), there is a non-zero element γ in $\mathcal{O}_+ \cap \mathcal{C}_R$. If $\gamma \in \mathbb{Q}$, then $\gamma \in \mathbb{Z}$, but $|\gamma| < 1$, so we get $\gamma = 0$, a contradiction. Hence $\gamma \in \mathcal{O}_+ \cap \mathcal{C}_R$ and $\gamma \notin \mathbb{Q}$. This proves the claim.

Let $\mu = \sqrt{\Delta(\mathcal{O}_1)}\gamma$. Then μ^2 is a totally negative element in K_+. We get $-\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) = |\Delta(\mathcal{O}_1)| \sum_i \phi_i(\gamma^2) \leq |\Delta(\mathcal{O}_1)|(1 + 2R^2)$. Since γ 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 $-\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) \leq |\Delta(\mathcal{O}_1)|(1 + 2|\Delta(\mathcal{O}_+)|^{1/2})$, as desired. □

7. Invariants

In this section, we prove Theorem 1.5. Let $j = \frac{u}{\Delta^l}$ be as in that theorem: a quotient of invariants of hyperelliptic (respectively Picard) curves $y^2 = F(x, 1)$ (respectively $y^3 = f(x)$) of genus 3, where Δ is the discriminant of F (respectively f) and u is an invariant of weight $56l$ (respectively $12l$). Let C be such a curve, not necessarily with CM, over a number field M.

Theorem 7.1. *In the situation above, if $j(C)$ has negative valuation at a prime $\mathfrak{p}$ with $\mathfrak{p} \nmid 6$, then C does not have potential good reduction at $\mathfrak{p}$.*

Proposition 7.2 (Example 10.1.26 in [18])**.** *Let $S = \mathrm{Spec}(\mathcal{O}_\mathfrak{p})$, where $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring with field of fractions M and residue field $\mathfrak{K}$ with $\mathrm{char}(\mathfrak{K}) \neq 2$. Let C be a hyperelliptic curve of genus $g \geq 1$ over M defined by an affine equation $y^2 = P(x)$, with $P(x) \in M[x]$ separable. Then C has good reduction if and only if C is isomorphic to a curve given by an equation as above with $P(x) \in \mathcal{O}_\mathfrak{p}[x]$ such that the image of $P(x)$ in $\mathfrak{K}[x]$ is separable of degree $2g + 1$ or $2g + 2$. Furthermore, any such isomorphism is given by a change of variables as in* [18, Corollary 7.4.33]. □

Proof of Theorem 7.1. For the Picard case: let C be a Picard curve of potentially good reduction at $\mathfrak{p}$, given by an affine equation as in (1). Corollary 3.20 in Lercier, Liu, Lorenzo García and Ritzenthaler [17] says that $v(a_2) \geq \frac{2}{12} v(\Delta)$ and $v(a_4) \geq \frac{4}{3} v(\Delta)$, where v is the $\mathfrak{p}$-adic valuation. In order to prove $v(j(C)) \geq 0$, it now suffices to prove $v(a_3) \geq \frac{3}{12} v(\Delta)$. So suppose $v(a_3) = \frac{3}{12} v(\Delta) - e$ with $e > 0$. Writing out the discriminant gives $a_3^4 + 3^{-3}(4a_2^3 - 144a_2a_4)a_3^2 + 3^{-3}(-16a_2^4a_4 + 128a_2^2a_4^2 - 256a_4^3 + \Delta) = 0$, but the term a_3^4 has strictly lower valuation than all other terms, which is impossible, hence $v(j(C)) \geq 0$.

For the hyperelliptic case: assume that C has potential good reduction at $\mathfrak{p}$ with $\mathfrak{p} \nmid 6$. Extend the base field so that C has good reduction, and then take a model $y^2 = P(x) \in \mathcal{O}_\mathfrak{p}[x]$ such that the image of $P(x)$ in $\mathfrak{K}[x]$ is separable of degree $2g + 1$ or $2g + 2$, as in Proposition 7.2. This changes the coefficients, but not the normalized invariant $j = \frac{u}{\Delta^l}$ by the definition of hyperelliptic curve invariants. Since $P(x)$ has coefficients in $\mathcal{O}_\mathfrak{p}$, it follows that $u(P(x)) \in \mathcal{O}_\mathfrak{p}$. Also, we have $\Delta(P(x)) \in \mathcal{O}_\mathfrak{p}^*$ by Proposition 7.2, hence $j(C) \in \mathcal{O}_\mathfrak{p}$. This contradicts the assumption and, therefore, the theorem follows. □

Remark 7.3. *Results of Bouw, Koutsianas, Sijsling and Wewers* [4] *give an alternative proof of Theorem 7.1 for Picard curves as follows. Numbered results referenced below are from* [4]*; some assume $\mathfrak{p} \nmid 3$.*

First of all, [4] *distinguishes between "special" Picard curves ($\overline{M}$-isomorphic to $S : y^3 = x^4 - 1$, Lemma 1.17) and "non-special" Picard curves (the rest). We compute $\Delta(S) = -2^8$, so $v(\Delta(S)) = 0$, hence all special Picard curves C satisfy $v(j(C)) \geq 0$.*

Now let C be a non-special Picard curve with potential good reduction. Extend the base field to have good reduction. Then choose a model of the form $y^3 = cf(x)$ with $v(c) \in \{0, 1, 2\}$ and f monic quartic and "reduced" as in Definitions 3.1.1/4 and Corollary 3.1.18. Proposition 3.2.1 gives $v(c) = 0$ and $v(\Delta(f)) = 0$. Extend M with $\sqrt[3]{c}$ to get the model $y^2 = f(x)$. Then complete the 4th power to get rid of the x^3 coefficient in f. Now we have $v(a_2)$, $v(a_3)$, $v(a_4) \geq 0$ and $v(\Delta) = 0$, hence $v(j(C)) \geq 0$.

Proof of Theorem 1.5. By Lemma 2.4, the bound B appearing in Theorem 1.1 satisfies $B \geq 2$. Therefore, for $p \leq 3$ we have $p < \frac{1}{8} B^{10}$. Hence we assume that $p > 3$. In the situation of Theorem 1.5, we showed in Theorem 7.1 that the curve does not have potential good reduction, hence Theorem 1.1 applies. □

References

[1] The Stacks Project Authors. Stacks project. `http://stacks.math.columbia.edu`, 2016.

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

[3] Irene Bouw, Jenny Cooley, Kristin E. Lauter, Elisa Lorenzo García, Michelle Manes, Rachel Newton, and Ekin Ozman. Bad reduction of genus 3 curves with complex multiplication. Women in Numbers Europe, Research Directions in Number Theory, Association for Women in Mathematics Series Volume 2, Springer, 2015.

[4] Irene Bouw, Angelo Koutsianas, Jeroen Sijsling, and Stefan Wewers. Conductor and discriminant of Picard curves. Preprint, arXiv:1902.09624, 2019.

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

[6] Reinier Bröker, Kristin Lauter, and Marco Streng. Abelian surfaces admitting an (l, l)-endomorphism. *J. Algebra*, 394:374–396, 2013. `https://arxiv.org/abs/1106.1884`.

[7] Michel Demazure. Fibrés tangents, algèbres de Lie. In *Schémas en Groupes (Sém. Géométrie Algébrique, Inst. Hautes Études Sci., 1963), Fasc. 1, Exposé 2*, page 40. Inst. Hautes Études Sci., Paris, 1963.

[8] 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*, volume 4284 of *Lecture Notes in Comput. Sci.*, pages 114–129. Springer, Berlin, 2006.

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

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

[11] Philipp Habegger and Fabien Pazuki. Bad reduction of genus 2 curves with CM jacobian varieties. *Compos. Math.*, 153(12):2534–2576, 2017.

[12] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arith.*, 185(2):127–156, 2018.

[13] Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng. Primes dividing invariants of CM Picard curves. *Canadian Journal of Mathematics*, (Published online), 2018. `https://doi.org/10.4153/S0008414X18000111`.

[14] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518 (electronic), 2005.

[15] Joan-Carles Lario and Anna Somoza. A note on Picard curves of CM-type. arXiv:1611.02582, 2016.

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

[17] Reynald Lercier, Qing Liu, Elisa Lorenzo García, and Christophe Ritzenthaler. Reduction type of smooth quartics. Preprint, arXiv:1803.05816, 2018.

[18] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[19] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[20] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[21] Tetsuji Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967.

[22] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[23] Marco Streng. RECIP – REpository of Complex multIPlication SageMath code. `http://pub.math.leidenuniv.nl/~strengtc/recip/`.

[24] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.

[25] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001.

Pinar Kiliçer, Bernoulli Institute for Mathematics, Computer Science and AI, Nijenborgh 9, 9747 AG Groningen, The Netherlands
Email address: p.kilicer@rug.nl

Kristin Lauter, Microsoft Research, Cryptography, One Microsoft Way, Redmond, WA, 98052 USA
Email address: klauter@microsoft.com

Elisa Lorenzo García, IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes cedex, France
Email address: elisa.lorenzogarcia@univ-rennes1.fr

Rachel Newton, Department of Mathematics and Statistics, University of Reading, Whiteknights, PO Box 220, Reading RG6 6AX, UK
Email address: r.d.newton@reading.ac.uk

Ekin Ozman, Bogazici University, Faculty of Arts and Sciences, Mathematics Department, Bebek, Istanbul, 34342, Turkey
Email address: ekin.ozman@boun.edu.tr

Marco Streng, Mathematisch Instituut, Universiteit Leiden, PO Box 9512, 2300 RA Leiden, The Netherlands
Email address: streng@math.leidenuniv.nl