Abstract

Van Wamelen [29] lists 19 curves of genus two over \( \mathbb{Q} \) with complex multiplication (CM). For each curve, the CM-field turns out to be cyclic Galois over \( \mathbb{Q} \). The generic non-Galois case did not feature in this list, as the field of definition in that case always contains a certain real quadratic field (the real quadratic subfield of the reflex field).

We extend van Wamelen’s list to include curves of genus two defined over this real quadratic field. Our list therefore contains the smallest “generic” examples of CM curves of genus two.

1 Introduction

We say that a curve \( C/k \) of genus \( g \) has \textit{complex multiplication} (CM) if the endomorphism ring of its Jacobian over \( k \) contains an order in a number field \( K \) of degree \( 2g \). Curves of genus one (elliptic curves) and two with complex multiplication are important in the CM-method for constructing (hyper)elliptic curves for cryptography, and for construction of class fields from class field theory.

It is well known that there exist exactly 13 elliptic curves over \( \mathbb{Q} \) with complex multiplication (see e.g. [3, Theorem 7.30(ii)]). Analogously, van Wamelen [29] gives a list of 19 curves of genus two over \( \mathbb{Q} \) with CM by a maximal order (proven in [1, 30]).

In the genus-two case, the (quartic) CM-field \( K \) is either cyclic Galois, biquadratic Galois, or non-Galois with Galois group \( D_4 \). Like van Wamelen, we disregard the degenerate biquadratic case, as the corresponding Jacobians are isogenous to a product of CM elliptic curves. Mura-bayashi and Umegaki [18] then show that van Wamelen’s list is complete. However, the list only contains examples of the cyclic case, not the \( D_4 \) case, because curves in the latter case cannot be defined over \( \mathbb{Q} \).

In this paper, we give a list of the simplest examples of the \( D_4 \) case, namely those defined over certain real quadratic extensions of \( \mathbb{Q} \). This is made possible by a reduction algorithm for hyperelliptic curve equations over real quadratic fields, based on Stoll and Cremona [24] and results of Lauter and Viray [15] on denominators of Igusa class polynomials. Our main result is as follows.

\*University of Warwick, http://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer email: F.Bouyer@Warwick.ac.uk, supported by the University of Warwick Undergraduate Research Scholarship Scheme (URSS)

\†Universiteit Leiden, http://www.math.leidenuniv.nl/~streng email: Marco.Streng@gmail.com, partially supported by EPSRC grant number EP/G004870/1 and by NWO Veni project number 639.031.243
Theorem 1.1. For every row of the tables 1a, 1b, and 2b in this article, the curves \( C : y^2 = f(x) \) are exactly all curves (up to isomorphism over \( \mathbb{Q} \) and up to conjugacy of the base field) with complex multiplication by the maximal order of the field \( K = \mathbb{Q}[X]/(X^4 + AX^2 + B) \), where \([D, A, B]\) is as in the first column of the table and \( f \) is as in the last column.

The number \( a \) that may appear in the coefficients of \( f \) is as follows. In table 1b, let \( D' = D \), and in table 2b, let \([D', A', B']\) be as in the second column. Let \( \epsilon \in \{0, 1\} \) be \( D' \) modulo 4. Then \( a \) is a root of \( x^2 + \epsilon x + (\epsilon - D')/4 = 0 \).

Section 4 contains more detailed statements, including an explanation of the other columns.

Pınar Kılıçer and the second-named author are currently working on a proof of completeness. That is, we believe that the first columns of Tables 1a, 1b, and 2b contain exactly the quartic fields \( K \) for which there exists a curve \( C \) of genus two with \( \text{End}(J(C)) = \mathcal{O}_K \) such that \( C \) is defined over the real quadratic subfield of the reflex field.

Now, let us give a more detailed overview of the content of this article and how we obtained this table.

In Sections 2.1 and 2.1.1, we give an introduction to complex multiplication. This should be enough background for understanding what our tables mean, albeit not how they were constructed. They were constructed by first computing the Igusa invariants of the curves, so we explain Igusa invariants in Section 2.2, including Mestre’s algorithm, which constructs a curve from its invariants. Section 2.3 gives some results about the minimal field of definition in the CM case. Finally, Section 2.4 explains how we obtain the Igusa invariants of CM curves.

Mestre’s algorithm constructs curves with given invariants, but these curves have coefficients of thousands of digits, so we have to use a reduction algorithm to reduce the coefficient size, which we explain in Section 3. Section 4 then gives a detailed version of the main result. We end with a cryptographic application in Section 5.

Acknowledgements

The authors would like to thank Bill Hart for his help with the factoring software GMP-ECM and CADO-NFS, Jeroen Sijsling for useful discussions about models and invariants, Damiano Testa as advisor of the first-named author, and Kristin Lauter and Bianca Viray for help with their formulas [15].

2 Invariants and complex multiplication

2.1 Complex Multiplication

We now give a brief introduction to complex multiplication of abelian varieties. For details, we refer to [13,21]. Let \( C/k \) be a (smooth, projective, geometrically irreducible) algebraic curve of genus 2 over a field \( k \) of characteristic 0. Any such curve has a hyperelliptic model \( y^2 = f(x) \) where \( f(x) \in k[x] \) is a separable polynomial of degree 5 or 6. Our tables therefore specify \( C \) by giving \( f \).

Its Jacobian \( A = J(C) \) is an abelian variety over \( k \) associated to \( C \), and we consider the ring \( \text{End}(A_\mathbb{F}) \) of algebraic group endomorphisms of \( A \) over \( \mathbb{F} \). We say that \( C \) has complex multiplication (CM) if there exists a number field \( K \) of degree 4 inside \( \text{End}(A_\mathbb{F}) \otimes \mathbb{Q} \). In this case, we also write \( \mathcal{O} = K \cap \text{End}(A_\mathbb{F}) \) and say that \( A \) has CM by \( \mathcal{O} \).

We disregard the degenerate case where \( A_\mathbb{F} \) is isogenous to a product of elliptic curves, that is, we assume that \( A \) is simple over \( \mathbb{F} \). Then \( \mathcal{O} \) equals the full endomorphism ring \( \text{End}(A_\mathbb{F}) \) and its fraction field \( K \) is a quartic CM-field, that is, \( K = K_0(\sqrt{r}) \) for some real quadratic field \( K_0 \).
field $K_0$ and some totally negative $r \in K_0$. Without loss of generality, we take $r \in \mathcal{O}_{K_0}$ with $A := -\text{tr}_{K_0/\mathbb{Q}}(r) \in \mathbb{Z}_{>0}$ minimal. Let $B = N_{K_0/\mathbb{Q}}(r) \in \mathbb{Z}_{>0}$ and assume $B$ is minimal for this $A$. Finally, let $D = \Delta_{K_0/\mathbb{Q}}$. Following [12], we use the triple $[D, A, B]$ to represent the isomorphism class of $K$, and note $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B)$.

There are three possibilities for the Galois group of a quartic CM-field ([22, Example 8.4(2)]):  

1. $K/\mathbb{Q}$ is Galois with cyclic Galois group $C_4$ of order 4,

2. $K/\mathbb{Q}$ is not normal, and its normal closure has dihedral Galois group $D_4$ of order 8,

3. $K/\mathbb{Q}$ is Galois over $\mathbb{Q}$ with Galois group $V_4 = C_2 \times C_2$.

It is known that case 3 of a biquadratic CM-field contradicts our assumption that $A$ is simple over $\overline{k}$, so our tables will be partitioned into cases 1 and 2.

2.1.1 CM-types and reflex fields

The CM-type $\Phi$ of $A$ is a set of 2 embeddings $\phi : K \to \overline{k}$, defined as follows. The tangent space $T_0(A_\overline{k})$ of $A$ over $\overline{k}$ at 0 is a two-dimensional $\overline{k}$-vectorspace. Differentiation thus gives a natural map

$$K = \text{End}(A_\overline{k}) \otimes \mathbb{Q} \to \text{End}_{\overline{k}}(T_0(A_\overline{k})).$$

It is known that this map is diagonalizable, so it splits into two embeddings $\phi_i : K \to \overline{k}$. We call the set $\Phi = \{\phi_1, \phi_2\}$ the CM-type of $A$.

The type norm is the multiplicative map $N_{\Phi} : K \to \overline{k} : x \mapsto \prod_i \phi_i(x)$, and its image generates a subfield $K^r$ of $\overline{k}$, known as the reflex field. The CM-type and reflex field are important in the theory of complex multiplication, as they are the link between the field of definition $k$ and the endomorphisms in $K$. In fact, the main theorem of complex multiplication generates abelian extension of $K^r$.

The reflex field is again a non-biquadratic quartic CM-field. In fact, one can compute that it is isomorphic to $\mathbb{Q}[X]/(X^4 + 2AX^2 + (A^2 - 4B))$. Let $[D', A', B']$ be the triple that represents $K^r$ as before. We do not necessarily have $A' = 2A$ and $B' = A^2 - 4B$, because those values are not always minimal. Note that we do have $K_0^r \cong \mathbb{Q}(\sqrt{D'}) \cong \mathbb{Q}(\sqrt{B})$. In our tables, we represent elements of $K_0^r$ as elements of $\mathbb{Q}(a)$, where $\mathbb{Z}[a] = \mathcal{O}_{K_0^r}$ and $\text{Tr}(a) \in \{0, 1\}$. In other words, the number $a$ is a root of $X^2 + \epsilon X + \frac{1}{4}(\epsilon - D')$, where $\epsilon = -\text{Tr}(a) \in \{0, 1\}$ is $D'$ modulo 4.

In case 1, we have $K^r \cong K$ and since $K/\mathbb{Q}$ is Galois, this fixes $K^r$ as a subfield of $\overline{k}$. In case 2, our tables also give $[D', A', B']$ specifying the isomorphism class of $K^r$. However, the real quadratic field $K_0^r = \mathbb{Q}(\sqrt{B}) \subset \overline{k}$ has two extensions isomorphic to $K^r$. Our tables specify which quadratic extension $K^r$ is of $K_0^r$ (equivalently, how to embed $K_0^r$ into $K^r$) by giving $a$ as a polynomial in $\alpha$.

2.2 Invariants and Mestre’s algorithm

2.2.1 Invariant, the field of moduli, and fields of definition

For an elliptic curve $E/k$, the $j$-invariant $j(E) \in k$ uniquely specifies the isomorphism class of $E$ over $k$. Moreover, the curve $E$ always has a model over its field of moduli $k_0 \subset k$, which is the smallest subfield of $k$ containing $j(E)$. In fact, such a model is given by a simple textbook formula, so giving $E/k$ (up to $\overline{k}$-isomorphism) is equivalent to giving $j(E) \in k$.

For a curve $C/k$ of genus two, the situation is a bit more complicated. For simplicity, we assume $k$ has characteristic different from 2, 3, 5. Every curve of genus two is hyperelliptic, that
is, is birational to an affine curve \( y^2 = f(x) \) where \( f \in k[x] \) has degree 5 or 6 and no roots of multiplicity > 1.

The Igusa-Clebsch invariants \( I_2, I_4, I_6, \) and \( I_{10} \) are polynomials in the coefficients of \( f \). They can be found in Igusa [11], where they are denoted \( A, B, C, D \) and are based on invariants of Clebsch. They are also available in the software packages Magma [2] and Sage [23]. The last invariant, \( I_{10} \), is \( 2^{20} \) times the discriminant of \( f \), hence is always non-zero.

Let \( \mathbf{P}^{2,4,6,10}(\overline{k}) \) be the weighted projective space of weights \((2,4,6,10)\), that is, the set of quadruples \( x = (x_n)_{n=2,4,6,10} \neq (0,0,0,0) \) up to the weighted scaling \( \lambda \cdot (x_n)_{n} = (\lambda^n x_n)_{n} \). Let \( \mathcal{M}_2(\overline{k}) \subset \mathbf{P}^{2,4,6,10}(\overline{k}) \) be the subspace defined by \( x_{10} \neq 0 \). Two curves \( C \) and \( C' \) over \( k \) are isomorphic over \( \overline{k} \) if and only if their Igusa invariants define the same point \( x \in \mathcal{M}_2(\overline{k}) \). And given a point \( x \in \mathcal{M}_2(\overline{k}) \), there exists a genus-two curve \( C/\overline{k} \) with \( (I_n(C))_n = x \). In more geometric language, \( \mathcal{M}_2 \) is the coarse moduli space of genus-two curves in characteristic not dividing \( 2 \cdot 3 \cdot 5 \).

We say that a point \( x \in \mathcal{M}_2(\overline{k}) \) is defined over \( k \) if \( x \in \mathcal{M}_2(k) \) is stable under the action of \( \text{Gal}(\overline{k}/k) \). One can show (using Hilbert’s Theorem 90) that this condition is satisfied if and only if \( x \) is the equivalence class of a quadruple with for all \( n \in k \), \( x_n \in k \). The field of moduli \( k_0 \) of \( C/\overline{k} \) is smallest field over which the point \( x = (I_n(C))_n \in \mathcal{M}_2(\overline{k}) \) is defined. We say that a field \( l \subset \overline{k} \) is a field of definition for \( C \) if there exists a curve \( D/l \) with \( D_{\overline{k}} \cong C \).

Unlike the elliptic case, there is no simple formula for \( C \) given \( (I_n(C))_n \), and \( C \) cannot always be defined over its field of moduli. There does exist an algorithm, due to Mestre [17], that finds a model for \( C \) given \( x \), but it involves solving a conic, which is not always possible without extending the field. Also, solving the conic introduces large numbers, so that the output polynomial may have coefficients that are much too large to be practical.

### 2.2.2 Mestre’s algorithm

In more detail, Mestre’s algorithm works as follows. First of all, assume that the curve \( C \) with \( x = (I_n(C))_n \) does not have any automorphisms other than the hyperelliptic involution \( \iota : (x,y) \mapsto (x,-y) \). (If it does, then use the construction of Cardona and Quer [3] instead of Mestre’s.) From the coordinates \( x_n \) in the field of moduli \( k_0 \), one constructs homogeneous ternary forms \( Q = Q_x \) and \( T = T_x \in k_0[U,V,W] \) of degrees 2 and 3 (for equations, see [17] or [27]). Let \( M_x \subset \mathbf{P}^2 \) be the conic defined by \( Q \). If \( M_x \) has a point over a field \( k \supset k_0 \), then this gives rise to a parametrization \( \varphi : \mathbf{P}^1 \to M_x \) over \( k \). Let \( \varphi^* : k[U,V,W] \to k[X,Z] \) be the ring homomorphism inducing this parametrization. We get a hyperelliptic curve \( C_{\varphi} : Y^2 = \varphi^*(T) \), i.e., \( C_{\varphi} : y^2 = T(\varphi(x : 1)) \). The curve \( C_{\varphi} \) is a double cover of \( \mathbf{P}^1 \), ramified at the six points of \( \mathbf{P}^1 \) that map (under \( \varphi \)) to the six zeroes of \( T_x \) on \( M_x \).

**Theorem 2.1** (Mestre [17]). Given \( x \in \mathcal{M}_2(k) \), assume the curve \( C/\overline{k} \) with \( x = (I_n(C))_n \) satisfies \( \text{Aut}(C) = \{1, \iota\} \).

1. If \( M_x(k) = \emptyset \), then \( C \) has no model over \( k \).
2. If \( M_x(k) \neq \emptyset \), then \( C_{\varphi}/k \) as above is a model of \( C \).

In particular, in order to find all genus-two curves over \( l \) with CM, it suffices to find all CM-points \( x \in \mathcal{M}_2(l) \), then test whether \( M_x \) has a point over \( l \), and if so, compute \( C_{\varphi} \) using this point. Once this is done, however, the curves have huge coefficients that make these models impractical and too large for any reasonable table. We use a reduction procedure to make these coefficients smaller, which we will explain in Section 3. First, we explain how we obtained the CM-points \( x \in \mathcal{M}_2 \) over quadratic fields.
2.3 Invariants in the CM case

In the CM case, a little more is known of the relation between fields of moduli and fields of definition. First of all, the following is the reason why \[20\] did not contain any curves with CM by non-Galois CM-fields.

**Proposition 2.2.** Let \( C \) be a curve of genus two with CM by an order in a non-Galois quartic CM-field. Then the field of moduli of \( C \) contains \( K_r^0 \).

**Proof.** This is a special case of \[20\] Proposition 5.17(5)].

**Theorem 2.3.** Let \( C \) be a curve of genus two with CM by the maximal order of a non-biquadratic quartic CM-field, let \( K^r \) be the reflex field and \( k_0 \) the field of moduli.

Then \( K^r k_0 \) is a field of definition and we have \([K^r k_0 : K_r^0 k_0] = 2\).

**Proof.** The first statement is Theorem 11 on page 524 of \[19\], combined with Proposition 2(3.4) on page 514, with the line below Proposition 7 on page 525, and with the fact that there are exactly 2 or 10 roots of unity in \( K \) if \( K \) is cyclic or non-Galois of degree 4.

The second statement is a special case of \[25\] Lemma 2.6].

**Corollary 2.4.** In the notation of Theorem 2.3, the following are equivalent:

1. \( K^r \) is a field of definition,
2. \( K^r \) contains the field of moduli \( k_0 \),
3. \( K_r^0 \) contains the field of moduli \( k_0 \).

In the non-Galois case, these conditions are also equivalent to

4. \( K_r^0 \) equals the field of moduli \( k_0 \).

**Proof.** The implications 1 \( \Rightarrow \) 2 and 3 \( \Rightarrow \) 2 are trivial, so assume 2 is true. Then Theorem 2.3 states that 1 holds and that \([K^r : K_r^0 k_0] = 2\), so 3 also holds.

In the non-Galois case, Proposition 2.2 gives 4 \( \Leftrightarrow \) 3.

**Remark 2.5.** The main theorem of complex multiplication gives the Galois group of \( k_0 K^r / K^r \) as an explicit quotient of the class group of \( K^r \). In particular, the conditions of Corollary 2.4 are equivalent to that quotient being trivial.

2.4 Computing CM invariants

Given a non-biquadratic quartic CM-field \( K \), its *Igusa class polynomials* in \( \mathbb{Q}[X] \) are a list of polynomials that specify the moduli points \( x \in M_2(\mathbb{Q}) \) of the curves with complex multiplication by \( \mathcal{O}_K \). There are various known methods of computing them numerically, but such methods only prove correctness when one knows a bound on the denominators of the (rational) coefficients of these polynomials.

The Echidna database \[12\] contains many quartic CM-fields \( K \) and their Igusa class polynomials (without proof, but computed \( p \)-adically with high precision and verified modulo many small primes). We took all fields \( K \) from the database with \([k_0 : \mathbb{Q}] \leq 2\).

Initially, we also took the (unproven) class polynomials from the database. The provenly correct and polynomial-time algorithm of \[26\] is not directly practical, as the denominator bounds used there are just too large.
As this project progressed, the much sharper bounds of Lauter and Viray [15] for the denominators of Igusa class polynomials became available. Substituting these in the algorithm of [26] enabled us to prove the output. Rather than going through the tedious and error-prone exercise of implementing the rounding error bounds for the numerical approximations in [26], we used interval arithmetic. This way, we computed small intervals that contain the coefficients of the class polynomials. The denominator formulas and the proven intervals together provide a proof of correctness of our class polynomials.

2.4.1 Denominators

We applied the denominator formulas of [15] quite straightforwardly, but those familiar with the formulas may wish to see a few more details. In order not to have to repeat the (complex) formulas, the present section may be of use only for those who have [15] close by. Other readers may wish to skip to Section 2.4.2.

All fields \( K \) in our tables, except for the field \([257, 23, 68]\), satisfy \( \mathcal{O}_K = \mathcal{O}_{K_0}[\eta] \) for some \( \eta \in K \). For those fields, we use the bound of [15, Theorem 2.1]. See [31, Proof of Theorem 9.1] for how exactly this applies to Igusa class polynomials, and note that the proof is not restricted to the constant coefficient, and applies to all class polynomials defined in [26].

We used the obvious and straightforward way to evaluate all the numbers occurring on the right hand side of [15, Theorem 2.1], except for \( J = J(d_u f_{u}^{-2}, d_x, t) \). For the number \( J \), which counts solutions to a ring embedding problem, we used the upper bound of [15, Theorem 2.4], where we used exact formulas whenever they are given in that theorem, and used the upper bound of the theorem otherwise. These bounds turned out to be small enough so that it took only a few hours to compute all class polynomials.

For the field \( K = [257, 23, 68] \), we chose ten different \( \eta \in \mathcal{O}_K \) such that \( I_\eta = [\mathcal{O}_K : \mathcal{O}_{K_0}[\eta]] \) is coprime to all primes \( p \leq D/4 \). For each \( \eta \) and each \( \ell \not| I_\eta \), we computed the bound of [15, Theorem 2.3] on the \( \ell \)-valuation of the denominator (and took \( \infty \) as upper bound at \( \ell \mid I_\eta \)). Then for each \( \ell \), we took the minimum over all \( \eta \) of this valuation bound. Finally, we sharpened the valuation bounds further using Goren and Lauter [8]. This final bound was then small enough for our class polynomial computation to finish within half an hour, though the denominator computation took a little more time in that case. Indeed, the index \( I \) had to be \( > D/4 \), which made the bounds of [15] hard to compute and far from sharp in this case. We were advised afterwards by Kristin Lauter that we did not have to exclude all primes \( \leq D/4 \), and that [15, Theorem 2.3] also holds if one only avoids the primes dividing the numbers \( \delta \) in their formulas.

It would be useful to have a fast algorithm for computing \( J \), rather than only bounds. Fortunately, for our purposes, the bounds were good enough.

2.4.2 Completeness

As for completeness, our tables contain all fields in the Echidna database satisfying the necessary condition \( [k_0 : \mathbb{Q}] \leq 2 \). In particular, by Corollary 2.4, our list contains all fields for which the curve has a model over \( K' \) as far as the Echidna database has them. The proof of completeness of this list of fields is a work in progress of Pınar Kılıçer.

3 Reduction

We will now describe how to make the hyperelliptic curve equations over \( k \) smaller. Note that we only care about the isomorphism class over \( \overline{k} \), while we do want the equation to have coefficients
in $k$, in other words, we would like to find a small equation among all twists of the hyperelliptic curve.

### 3.1 Isomorphisms and twists

Fix an integer $g \geq 2$ and a field $k$, and let $H(k) = H_g(k)$ be the set of separable polynomials $f(x) \in k[x]$ of degree $2g + 1$ or $2g + 2$. We interpret the element $f(x) \in H(k)$ also as the binary form $F(X, Z) = Z^{g+2}f(X/Z)$ of degree $2g + 2$, and as the hyperelliptic curve $C = C_f$ of genus $g$ given by the affine equation $y^2 = f(x)$. We can also write $C$ as the smooth curve given by $Y^2 = F(X, Z)$ in weighted projective space $\mathbb{P}^{(1, g+1, 1)}$.

Given any element of $H(k)$, we would like to find some isomorphic element with small coefficients, so first we determine when two hyperelliptic curves are isomorphic.

Note the obvious right group actions of scaling and substitution

\[
\begin{align*}
H(k) \circ k^* & : (F(X, Z), u) \mapsto uF(X, Z), \text{ and} \\
H(k) \circ \text{GL}_2(k) & : (F(X, Z), A) \mapsto F(A \cdot (X, Z)),
\end{align*}
\]

which together induce an action of $\text{GL}_2(k) \times k^*$ on $H(k)$. Explicitly in terms of $f$, the action is

\[
H(k) \circ \text{GL}_2(k) \times k^* : f \cdot \left( \begin{array}{cc} a & b \\ c & d \end{array} \right), \quad u \mapsto (cx + d)^{g+2}f \left( \frac{ax + b}{cx + d} \right).
\]

**Lemma 3.1.** Two hyperelliptic curves $C_f$ and $C_{f'}$ in $H(k)$ are isomorphic over $k$ if and only if they are in the same orbit under $\text{GL}_2(k) \times (k^*)^2$.

**Proof.** This is a standard result, see e.g. [4, p. 1] for the case of genus two. \qed

**Example 3.2.** If $f^1 = f \cdot \left[ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right), v^2 \right]$, then an isomorphism $C_{f^1} \to C_f$ is given by $(x, y) \to (\frac{ax + b}{cx + d}, v^{-1}(cx + d)^{-g-1}y)$.

But we are interested in the best model in the isomorphism class over $\overline{k}$, that is, we also allow twists. To classify twists, we need the automorphism group of our curve $C$. Note that $C$ always has the identity and the hyperelliptic involution $\iota : C \to C : (x, y) \mapsto (x, -y)$.

**Lemma 3.3.** Given any two $C_f, C_{f'} \in H(k)$, assume $\text{Aut}((C_f)_{\overline{k}}) = \{1, \iota\}$. Then $C_f$ and $C_{f'}$ are isomorphic over $\overline{k}$ if and only if they are in the same orbit under $\text{GL}_2(k) \times k^*$.

**Proof.** Using the fact that $\text{Aut}(C_{\overline{k}}) = \{1, \iota\}$, we get (see e.g. [3, Example C.5.1]) that all twists, up to isomorphisms over $k$, are given by the action of $H^1(k, \{1, \iota\}) = k^*/k^{*2} = \{1\} \times (k^*/k^{*2})$. And Lemma 3.1 states that all isomorphisms over $k$ are given by the action of $\text{GL}_2(k) \times (k^*)^2$. \qed

**Lemma 3.4.** Suppose $C$ is a curve of genus two with CM by an order $\mathcal{O} \subset K$, and suppose that we are in case 1 or 2 as in Section 2.1. Then either $\mathcal{O} = \mathbb{Z}[\zeta_5]$ and $C$ is isomorphic over $\overline{k}$ to the curve $y^2 = x^5 - 1$ or we have $\text{Aut}(C_{\overline{k}}) = \{1, \iota\}$.

**Proof.** The automorphisms of $C$ correspond to automorphisms of the principally polarized abelian variety $J(C)$, which are roots of unity in $\mathcal{O} = \text{End}(J(C)_{\overline{k}})$. The only order in cases 1 and 2 with roots of unity is $\mathbb{Z}[\zeta_5]$, and since it has class number one, there is only one curve with CM by that up to isomorphism over the algebraic closure. That curve is the curve $y^2 = x^5 - 1$, since that has an automorphism of order 10. \qed

Note that in the first case, we have nothing to do: we know a small model already, while in the second case, the hypothesis of Lemma 3.3 is satisfied.
3.1.1 Integrality and discriminants

Let \( f = c \prod_{i=1}^{d}(x - \alpha_i) \) be a polynomial of degree \( d \in \{2g + 1, 2g + 2\} \). The discriminant of \( C = C_f \) is defined to be (16)

\[
\Delta(C_f) = 2^{4g}c^{4g + 2}\prod_{i<j}(\alpha_i - \alpha_j)^2 = \begin{cases} 2^{4g}\Delta(f) & d = 2g + 2, \\ 2^{4g}c^2\Delta(f) & d = 2g + 1. \end{cases}
\]

In case \( g = 2 \), we have \( \Delta(C) = 2^{-12}I_{10}(C) \).

Now suppose \( f^1 = f \cdot [A, u] \). Then we have

\[
\Delta(C_{f^1}) = u^{2(g+1)}\det(A)^2(2^{g+1})\Delta(C_f).
\] (3.1)

**Remark 3.5.** In case \( g = 2 \), the Igusa invariants satisfy

\[
I_n(C_{f^1}) = u^n\det(A)^{3n}I_n(C_f).
\]

**Remark 3.6.** Let \( R \) be a domain with field of fractions \( k \), and suppose that \( f, A, \) and \( u \) have coefficients in \( R \), then so does \( f \cdot [A, u] \).

Our reduction algorithm consists of two stages: making \( f \) integral with discriminant of small norm, using \((\text{GL}_2(k) \times k^*)\)-transformations, and then making heights of the coefficients small by \((\text{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*)\)-transformations (which preserve integrality and affect the discriminant only by units).

3.2 Local reduction of the discriminant

Assume for now that \( k \) is the field of fractions of a discrete valuation ring \( R \) with valuation \( v \). Let \( \pi \) be a uniformizer of \( k \) and \( \mathfrak{m} = \pi R \) the maximal ideal.

We call \( C \) minimal at \( v \) if \( v(\Delta(C)) \) is minimal among all twists of \( C \) of the form \( y^2 = f(x) \) with \( v \)-integral coefficients. Note that for \( v \mid 2 \) this notion of minimality may give larger discriminants than the usual notion, since we only allow models of the form \( y^2 = f(x) \). On the other hand, our notion of minimality may give smaller discriminants, since we allow twists instead of only isomorphisms.

**Proposition 3.7.** Suppose \( C = C_f \) has coefficients in \( R \) and satisfies \( \text{Aut}((C_f)_{\overline{k}}) = \{1, \iota\} \). Then \( C_f \) is non-minimal at \( v \) (according to the definition above) if and only if we are in one of the following three cases.

1. The polynomial \( f \) is not primitive, so \( f^1 := f \cdot [\text{id}_2, \pi^{-1}] \) is integral and satisfies \( v(\Delta(C_{f^1})) < v(\Delta(C_f)) \).
2. The polynomial \( (f \mod \mathfrak{m}) \) has a \((g+2)\)-fold root \( \overline{t} \) in the residue field. Moreover, for some (equivalently every) lift \( t \in R \) of \( \overline{t} \), if we let \( A = (\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}) \), then \( f^1 := f \cdot [A, \pi^{-g+2}] = f(\pi x + t)/\pi^{g+2} \) is integral and satisfies \( v(\Delta(C_{f^1})) < v(\Delta(C_f)) \).
3. The polynomial \( (f \mod \mathfrak{m}) \) has degree \( \leq g \). Moreover, if we let \( A = (\begin{smallmatrix} 1 & 0 \\ 0 & \pi \end{smallmatrix}) \), then \( f^1 := f \cdot [A, \pi^{-g+2}] = f(x/\pi)\pi^g \) is integral and satisfies \( v(\Delta(C_{f^1})) < v(\Delta(C_f)) \).

Note that the proposition gives a very simple reduction algorithm. Testing whether case 1 or 3 holds is easy, and for case 2 all we need to do is test whether \( f \) has a \((g+2)\)-fold root modulo \( \mathfrak{m} \) and compute valuations of coefficients (possibly after translation by \( t \)). Finding a \((g+2)\)-fold root \( \overline{t} \) is easy too, as it corresponds to a root of the polynomial \( \gcd(f, f', f'', \ldots, f^{(g+1)}) \) over
the finite field $R/\mathfrak{m}$. In fact, this gcd is a power of a linear polynomial $\sum_{i=1}^{n} a_i x^n = a_n(x - \gamma)^n$, so we recover $t$ as $t \equiv -a_n^{-1}/(na_n) \mod \mathfrak{m}$ if $n > 0$ and $t$ does not exist if $n = 0$.

The remainder of Section 3.2 is devoted to proving Proposition 3.7.

Let $T$ be the subgroup $T = \{(v \text{id}_2, v^{-2g-2}) : v \in k^*\}$ of the centre of $\text{GL}_2(k) \times k^*$, and note that $T$ acts trivially on $H$.

**Lemma 3.8.** Let $k$ be the field of fractions of a discrete valuation ring $\mathcal{O}_k$, and let $\pi$ be a uniformizer. Given any element $[A, u] \in \text{GL}_2(k) \times k^*$, we have $[A, u] \in T \cdot [A', u'](\text{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*)$ where $A' = (a/b, d)$ with $a, b, d, u' \in \pi Z$, and $\gcd(a, b, d) = 1$.

**Proof.** The following proof is taken directly from [16, Lemme 3], which treats the case of isomorphisms of curves, while we treat twists. First, we make $A$ upper triangular. Write $A = (a, b, c, d)$ and let $\eta = d/c$. If $v(\eta) \geq 0$, then right multiplication with $B = (\eta, -1; 1, 0) \in \text{GL}_2(\mathcal{O}_k)$ does the trick. Otherwise, use $B = (1, 0; \eta^{-1}, 1)$.

Next, multiplying by a power of $(\pi \text{id}_2, \pi^{-2g-2}) \in T$, we can make $A$'s coefficients $\pi$-integral and coprime. Now everything is satisfied except $a, d, u \in \pi Z$. For this, we multiply on the right with

$$\begin{pmatrix} \pi^{v(a)} a^{-1} & 0 \\ 0 & \pi^{v(d)} d^{-1} \end{pmatrix}, \pi^{v(u)} u^{-1} \in \text{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*.$$ 

**Proof of Proposition 3.7.** For the “if” part, note that in each of the three cases, the proposition gives an explicit transformation that proves that $C_f$ is not minimal.

Conversely, given any non-minimal $C_f$, let $[A, u]$ be such that $C_{f1} = C_f \cdot [A, u]$ has minimal discriminant. By Lemma 3.8 there is no loss of generality in assuming $A = (a/b, d)$ with $a, b, d, u \in \pi Z$, and $\gcd(a, b, d) = 1$. Write $a = \pi^k, d = \pi^l, u = \pi^{-m}$. Assume first $v(b) \geq l$, so $t = b/d$ is $\pi$-integral.

Let $b(x) = f(x + t)$ and write $b(x) = \sum h_i x^i$. Then $f \cdot [A, u] = ab(ax/d)^{\frac{d(g-1)}{2}}$ is integral.

The fact that $\Delta(C_f)$ is not minimal, but $\Delta(C_{f1})$ implies $m > (g + 1)(k + l)$ by equation 3.11. Moreover, integrality of $f \cdot [A, u]$ implies $v(h_i) \geq m - ki - l(2(g + 1) - i)$. Together, this gives

$$v(h_i) > (g + 1)(k + l) - ki - l(2(g + 1) - i) = (g + 1 - i)(k - l).$$

In particular, if $k = l$, then $h$ is integral and non-primitive, hence so is $f(x) = h(x - t)$ and we are in case 1.

If $k > l$, then for all $i \leq g + 1$, we have $v(h_i) > (g + 1 - i)(k - l)$ with $k - l \geq 1$, so $v(h_i) \geq g + 2 - i$. In particular, the model $C_f \cdot [(\pi t', \pi)^{-g+2}] = C_h \cdot [(\pi 0 \pi t', 0)^{-g+2}]$ is integral, and of strictly smaller discriminant than $C_f$. This proves that we are in case 2 for some lift $t$ of a $(g + 2)$-fold root $\tilde{t}$. To finish the proof of case 2, we need to prove that for any $t' \equiv t \mod \mathfrak{m}$, the transformation $[(\pi t', \pi)^{-g+2}]$ also gives an integral equation with strictly smaller discriminant. So let $y = (t' - t)/\pi \in \mathcal{O}_k$ and note

$$\begin{pmatrix} \pi & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pi & t' \\ 0 & 1 \end{pmatrix},$$

which proves that we are in case 2 for any lift $t$.

Next, if $k < l$, then $v(h_i) \geq i - g$ for all $i \geq g + 1$. We get that the model $C_f \cdot [(\pi t', \pi)^{-g+2}] = C_h \cdot [(\pi 0 \pi t', 0)^{-g+2}]$ is integral, and of strictly smaller discriminant than $C_f$. We compose this on the right with the transformation $[(\pi t', 1)] \in \text{GL}(\mathcal{O}_k) \times \mathcal{O}_k^*$ to conclude that $C_f \cdot [(\pi 0 \pi t', 1)]$ is integral with smaller discriminant. In other words, we are in case 3.
This leaves only the case where \( v(b/d) < 0 \). In that case, consider the reciprocal \( C_f^* \), where \( f^* = f(1/x)x^{2g+2} = f \cdot [([0 1], 1], \) which has the same discriminant as \( C_f \). We know that its discriminant becomes smaller using the transformation

\[
\left[ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1 \right]^{-1} \cdot \left[ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, u \right] = \left[ \begin{pmatrix} 0 & a \\ b & d \end{pmatrix}, u \right],
\]

which we make upper-triangular following the recipe of Lemma 3.8. This yields that the discriminant of \( C_f^* \) is made smaller by a transformation \([a' b' \ 0 \ d'], u\] with \( v(b'/d') \geq v(d/b) > 0 \). In particular, the model \( C_f^* \) is in case 1, case 3, or case 2 with \( t = 0 \). This implies respectively that \( C_f \) is in case 1, 2, or 3.

### 3.3 Global reduction of the discriminant

Now let’s get back to the case where \( k \) is a number field with ring of integers \( \mathcal{O}_k \). We would prefer to have a model \( C \) where \( v(\Delta(C)) \) is minimal for all discrete valuations \( v \) of \( k \).

#### 3.3.1 Theoretical obstruction: non-principal ideals

If \( k \) has class number one, then such a model exists. Indeed, if we take \( \pi \) in Proposition 3.7 to be a generator of the prime ideal corresponding to \( v \), then this affects only \( v \) and no other valuations, so we can do this for each \( v \) separately.

If \( k \) does not have class number one, then this is not always possible. Indeed, let \( C_v \) be a model with \( v(\Delta(C_v)) \) minimal, and let \( \Delta_{\text{min}} \) be the ideal with \( v(\Delta_{\text{min}}) = v(\Delta(C_v)) \) for all \( v \). If \( \Delta_{\text{min}} \) is not principal, then there is no model with that discriminant. In fact, if \( C \) is any model, and there exists a globally minimal model \( C_{\text{min}} \) with \( \Delta(C_{\text{min}}) = \Delta_{\text{min}} \), then the ideal \( \sqrt[4]{\Delta(C)/\Delta_{\text{min}}} \) is a principal ideal.

Fortunately, for all fields in the Echidna database with curves defined over \( K^r \), we found that \( K^r_0 \) has class number 1, except for the field \( K = [17, 46, 257] \), where \( K^r_0 \) has class number 3. This means that a global minimal model exists for all but one of the fields (if a model exists over \( K^r_0 \) at all).

For general class numbers, if we take a set of generators of the class group, then there exists a model that is minimal everywhere outside that set of generators, and such that the set of generators falls into categories 1 and 2 of Proposition 3.7. We can then make sure the discriminant is reasonably small (though possibly not minimal) at that set of generators too. In particular, this is what we did for \([17, 46, 257]\).

#### 3.3.2 Practical problem: factoring is hard

We want to actually write down models with small discriminants, so if we want to use our local algorithm, then we have to know the valuations \( v \) for which \( v(\Delta(C)) \) is non-minimal. In theory, we could do this by factoring \( v(\Delta(C)) \), but factoring can be computationally hard for large numbers. Even though factoring is inevitable for some curves, such as

\[ y^2 = n^2x^6 + x + 1 \quad \text{where} \quad n = pq^2, \]

it was not strictly necessary for the curves we obtained with Mestre’s algorithm.

Let us now explain our methods for avoiding factorization where possible. First of all, there are other invariants of hyperelliptic curves besides the discriminant. In our case, there are
the Igusa-Clebsch invariants $I_2$, $I_4$, $I_6$, $I_{10}$, and they satisfy the transformation formula of Remark 3.5. So we only need to factor the ideal $a = \gcd(I_2, I_4, I_6, I_{10})$, which only contains the square of the number $u \det(A)^3$ from Remark 3.5, where $\Delta = 2^{-12}I_{10}$ contains the 10-th power.

Next, we find the small factors of $a$ by trial division, and reduce the model locally at those. With the ideal $a$ that we are left with, we could try the algorithm of Proposition 3.7 even though the ideal $a$ may be composite. Division with remainder of polynomials, and hence taking gcd's, either works or provides a non-trivial factor of $a$. This way, we either split up $a$ and reduce factor by factor, or we find that $f$ modulo $a$ has a $g + 2$-fold root $t$ or has degree $\leq g$. In the latter two cases, if $a$ is square-free and $v_p(\Delta(f))$ is non-minimal at all primes $p \mid a$, then we simply apply our reduction algorithm pretending that $a$ is prime. This removes a power of $a$ from the discriminant. In practice at this stage, the ideal $a$ was always a perfect power of a prime ideal, so we simply take the appropriate root and remove the factor $a$ from the discriminant without knowing the prime factors of $a$.

**Remark 3.9.** Before using the above method, we already found most models by using powerful factoring methods. This takes longer, and was unsuccessful in the end for a few curves, but had the advantage of being very straightforward. We used the (randomized) conic solving command from Magma V2.19-1 to solve Mestre’s conic (Section 2.2.2), so when we were unable to factor $a$, we asked Magma for a new parametrization, and hence got a new model $C$, sometimes (but not always) with a discriminant that was easier to factor. For factoring, we used trial division and the elliptic curve method from Magma [2], the elliptic curve method of GMP-ECM [32], and the number field sieve implementation CADO-NFS [7].

### 3.4 Stoll-Cremona reduction

Now suppose that we have our integral model $C$ where the norm $N(\Delta(C))$ is small. Next, we try to make the coefficients small. As we do not want to break integrality or disturb the discriminant, we take transformations in $(\text{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*)$.

Stoll and Cremona [24] give a definition of reduced for binary forms of degree $\geq 4$ over $\mathbb{Q}$ under the action of $\text{SL}_2(\mathbb{Z}) \times 1$. They also explain how to extend it to binary forms over any number field $k$ under the action of $\text{SL}_2(\mathcal{O}_k) \times 1$. We only need the special case of forms of even degree over a totally real field, which we explain now. Recall that $H(k)$ is the set of polynomials of degree $2g + 1$ or $2g + 2$ with no double roots. We interpret $f \in H(k)$ as the binary form $f(X/Z)Z^{2g+2}$ or the hyperelliptic curve $C_f$, and we have a right $\text{GL}_2(k)$-action on $H(k)$, as we have seen before.

Next, let $\mathcal{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ be the complex upper half plane. We turn the standard left $\text{GL}_2(\mathbb{Q})^+$-action on $\mathcal{H}$ into a right action by $z : A = A^{-1}(z) = (dz-b)/(cz+a)$ for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The idea behind [24] is to use an $\text{SL}_2(\mathbb{R})$-covariant map $z : H(\mathbb{R}) \to \mathcal{H}$. For example, let’s take binary forms over $\mathbb{Q}$. In $\mathcal{H}$, there is a notion of $\text{SL}_2(\mathbb{Z})$-reduction, and we just pull back that notion to $H(\mathbb{Q})$ via $z$. In other words, if $F \in H(\mathbb{Q})$ reduced for $\text{SL}_2(\mathbb{Z})$ if $z(F) = z = x + iy$ satisfies $|z| \geq 1$, $|z| \leq \frac{1}{2}$, and if $|z| = 1$, then $x \geq 0$.

More generally, let $k$ be a totally real number field of degree $d$ and let $\phi_1, \ldots, \phi_d$ be the $d$ embeddings $k \to \mathbb{R}$. This induces maps $H(k) \to H(\mathbb{R})^d$ and $\text{SL}_2(k) \to \text{SL}_2(\mathbb{R})^d$. Composing with the covariant map $z$ on every component, we get $H(k) \to \mathcal{H}^d$, which is $\text{SL}_2(k)$-covariant.

In fact, we can do slightly better. We identify $\mathcal{H}$ with $(\mathbb{C} \setminus \mathbb{R})$ modulo complex conjugation, that is, we identify $z \in -\mathcal{H}$ with $\overline{z} \in \mathcal{H}$, then the $\text{SL}_2(\mathbb{R})$-action on $\mathcal{H}$ extends to a $\text{GL}_2(\mathbb{R})$-action also given by $z : A = A^{-1}(z) = (dz-b)/(cz+a)$ (up to complex conjugation). The covariant $z$ of [24] then turns out to also be $\text{GL}_2(\mathbb{R})$-covariant.

So the next step is to define what it means for a point in $\mathcal{H}^d$ to be reduced under $\text{GL}_2(\mathcal{O}_k)$. We choose the following definition: $z = x + iy \in \mathcal{H}^d$ is $\text{GL}_2(\mathcal{O}_k)$-reduced if
1. \( \prod_{m=1}^{d} y_m \) is maximal for the \( \text{GL}_2(\mathcal{O}_k) \)-orbit,
2. \( x \in \mathbb{R}^d \) is in some fixed chosen fundamental parallelogram for addition by \( \mathcal{O}_k \), and
3. \( \log y \in \mathbb{R}_{\geq 0}^d \) is in some fixed chosen fundamental parallelogram for addition by \( \{ \log(|\phi_m(u)|)_m : u \in \mathcal{O}_k^1 \} \).

If \( k \) has class number one and we replace \( \text{GL}_2(\mathcal{O}_k) \) with \( \text{SL}_2(\mathcal{O}_k) \), then this definition of reduced gives a standard fundamental domain for the action of \( \text{SL}_2(\mathcal{O}_k) \) on \( \mathcal{H}^d \) [28]. For general class numbers, one could also use a standard fundamental domain, but since we had only one case of class number > 1, we simply used 1.–3. for all our fields.

We implemented the reduction algorithm of 1.–3. in Sage [23], except that we used Magma [2] for evaluating the covariant \( z(F) \) numerically given \( F \). Indeed, that covariant is available in Magma as a standard function (called \textit{Covariant}).

Repeatedly using 1.–3., we find an integral model that is reduced for \( [\text{GL}_2(\mathcal{O}_k^*)] \). Indeed, that covariant is available in Magma as a standard function (called \textit{Covariant}).

In tables 2b and 2c, let \( [D, A, B] \) be as in the column \( \text{DAB} \). Then let \( K' = \mathbb{Q}(\alpha) \), where \( \alpha \) is a root of \( X^4 + A^r X^2 + B^r \). In tables 1a and 1b, we have \( K' \cong K \) and \([D', A', B'] = [D, A, B] \).

a A root of \( X^2 + \epsilon X + (D^r - \epsilon)/4 \) with \( \epsilon \in \{0, 1\} \) congruent to \( D^r \) modulo 4. In tables 2b and 2c, take \( a \) as in the column \( \text{a} \). We have \( \mathbb{Z}[a] = \mathcal{O}_{K_0' \cap \mathbb{Q}(\sqrt{D^r})} \). In case 1, the quadratic extension \( K'/K_0' = \mathbb{Q}(a)/\mathbb{Q}(\sqrt{D^r}) \) is uniquely determined by \([D', A', B'] \). In case 2, there are two quadratic extensions \( K'/\mathbb{Q}(\sqrt{D^r}) \) given by \( K' = \mathbb{Q}[X]/(X^4 + A^r X^2 + B^r) \), and they are conjugate over \( \mathbb{Q} \), and the expression of \( a \) in terms of \( \alpha \) tells us which of these extensions is \( K' = \mathbb{Q}(\alpha) \).

\( f, C \) The polynomial \( f \in \mathbb{Z}[a] \) given in the final column defines a hyperelliptic curve \( C : y^2 = f(x) \) of genus two.

4 Our results

Recall that we are interested in curves with CM by the maximal order of a quartic CM-field \( K \), which are defined over the reflex field \( K' \). We have separated our list into six different categories. First of all, we distinguish between case 1 (\( K/\mathbb{Q} \) cyclic Galois) and case 2 (\( K/\mathbb{Q} \) non-Galois), and second, we distinguish whether the curves are defined over:

a. \( \mathbb{Q} \),
b. \( K_0' \), but not \( \mathbb{Q} \),
c. \( K' \), but not \( K_0' \).

The motivation for this article was that case 2a is not possible, and during our construction of our list case 1c did not occur. Hence we constructed four tables corresponding to the four cases 1a, 1b, 2b, and 2c.

Legend for Tables 1a – 2c.

\( \text{DAB} \) With \([D, A, B] \) as in the first column, let \( K = \mathbb{Q}(\beta) \), where \( \beta \) is a root of \( X^4 + AX^2 + B \).

\( \text{DAB}' \) In tables 2b and 2c, let \([D', A', B'] \) be as in the column \( \text{DAB}' \). Then let \( K' = \mathbb{Q}(\alpha) \), where \( \alpha \) is a root of \( X^4 + A^r X^2 + B^r \). In tables 1a and 1b, we have \( K' \cong K \) and \([D', A', B'] = [D, A, B] \).

a A root of \( X^2 + \epsilon X + (D^r - \epsilon)/4 \) with \( \epsilon \in \{0, 1\} \) congruent to \( D^r \) modulo 4. In table 1b, fix any such \( a \), in tables 2b and 2c, take \( a \) as in the column \( \text{a} \). We have \( \mathbb{Z}[a] = \mathcal{O}_{K_0''} \). In case 1, the quadratic extension \( K'/K_0' = \mathbb{Q}(a)/\mathbb{Q}(\sqrt{D^r}) \) is uniquely determined by \([D', A', B'] \). In case 2, there are two quadratic extensions \( K'/\mathbb{Q}(\sqrt{D^r}) \) given by \( K' = \mathbb{Q}[X]/(X^4 + A^r X^2 + B) \), and they are conjugate over \( \mathbb{Q} \), and the expression of \( a \) in terms of \( \alpha \) tells us which of these extensions is \( K' = \mathbb{Q}(\alpha) \).

\( f, C \) The polynomial \( f \in \mathbb{Z}[a] \) given in the final column defines a hyperelliptic curve \( C : y^2 = f(x) \) of genus two.
\[ \Delta(C) \quad \text{The discriminant of the given model } y^2 = f(x) \text{ of } C. \]

\[ \Delta_{\text{stable}} \quad \text{The minimal discriminant of all models of } C \text{ over } \overline{\mathbb{Q}} \text{ of the form } y^2 + h(x)y = g(x) \text{ with coefficients in } \mathbb{Z}. \]

\[ \Phi \quad \text{One fixed CM-type of } K \text{ with reflex field } K^r, \text{ uniquely determined up to right-composition with } \text{Aut}(K) \text{ by the following recipe. In case 1, we have } \text{Aut}(K) = C_4 \text{ and we fix an arbitrary CM-type. In case 2, the type } \Phi \text{ is unique up to complex conjugation and given as follows: } \Phi \text{ is a CM-type of } K \text{ with values in a normal closure of } K^r \text{ and reflex field } K^r. \]

\[ (xa + y)^n \quad \text{The } \Theta \text{th power of the } \mathbb{Z}[a]-\text{ideal of norm } n \text{ generated by } xa + y. \text{ This notation is used in the discriminant and obstruction columns.} \]

We give the following more detailed version of Theorem 1.1.

Theorem 4.1. With the notation as in the legend above, we have the following.

1. For every row of Tables 1a, 1b, and 2b, let \( K \) be as specified in that row (see “DAB” in the legend), and consider the curves \( C \) given in that row. Then the following holds.
   
   (a) In Table 1a, the given curves are exactly all \( \overline{\mathbb{Q}} \)-isomorphism classes of curves satisfying \( \text{End}(J(C)|_\overline{\mathbb{Q}}) \cong \mathcal{O}_K \).
   
   (b) In Tables 1b and 2b, the given curves and their quadratic conjugates over \( \mathbb{Q} \) are exactly all \( \overline{\mathbb{Q}} \)-isomorphism classes of curves satisfying \( \text{End}(J(C)|_\overline{\mathbb{Q}}) \cong \mathcal{O}_K \).
   
   (c) In Tables 1a and 1b, the curves have CM-type \( \Phi \) for every CM-type \( \Phi \) of \( K \).
   
   (d) In Table 2b, the given curve has the given CM-type \( \Phi \), and its quadratic conjugate has CM-type \( \Phi' \) where \( \Phi' \notin \{\Phi, \overline{\Phi}\} \).

2. The curves in tables 1a, 1b, and 2b are all defined over \( K_0^r \), and the entries \( \Delta(C)/\Delta_{\text{stable}} \) and \( \Delta_{\text{stable}} \) are correct.

3. In Tables 1b and 2b, the discriminant \( \Delta(C) \) is minimal (as defined in Section 3.2) among all \( \overline{\mathbb{Q}} \)-isomorphic models of the form \( y^2 = g(x) \) with \( g(x) \in \mathcal{O}_{K_0^r}[x] \), except for the case of the field \([17, 46, 257]\) in Table 2b, where a global minimal model does not exist, and the given model is minimal outside \((2, a + 1)\). In Table 1a, the discriminant is minimal among such models with \( g(x) \in \mathbb{Z}[x] \).

4. The curves in Tables 1b and 2b have Igusa invariants that do not lie in \( \mathbb{Q} \). In particular, they have no model over \( \mathbb{Q} \).

5. For every row of Table 2c, the number in the final column is the number of curves over \( \overline{\mathbb{Q}} \) with \( \text{End}(J(C)|_\overline{\mathbb{Q}}) \cong \mathcal{O}_K \) of type \( \Phi \) up to isomorphism over \( \overline{\mathbb{Q}} \). These curves all have Igusa invariants in \( K_0^r \) but no model over \( K_0^r \). They do have a model over \( K^r \). The obstructions column gives exactly the set of places of \( K_0^r \) at which Mestre’s conic locally has no point.

Before we give the proof, let us note that the curves in 1(a) and Table 1a were already given by van Wamelen [29] and proven correct by van Wamelen [30] and Bisson and Streng [1].

Proof. Our computation of Igusa class polynomials shows that we have the correct number of curves for each field. Since we use interval arithmetic and the denominator formulas of Lauter and Viray [15], these computations even prove that the Igusa invariants themselves are correct. The listed curves have the correct Igusa invariants, which proves that the curves and computed
obstructions are correct. In case 1, all CM-types are in the same orbit for $\text{Aut}(K)$, so they are all correct. In cases 2b and 2c, the correct CM-type is determined using reduction modulo a suitable prime and the Shimura-Taniyama formula [22, Theorem 1(ii) in Section 13.1]. Proposition 3.7 and our reduction algorithm prove that the discriminant is minimal. The stable discriminant is computed directly from Igusa’s arithmetic invariants [11]. The obstructions to the existence of a model over $K_0^r$ are the obstructions to Mestre’s conic having a rational point, so for part 5, we computed Mestre’s conic from the proven Igusa invariants.
Table 1a

| DAB   | $\Delta_{\text{stable}}$ | $\Delta(C)/\Delta_{\text{stable}}$ | $f$, where $C : y^2 = f$ |
|-------|---------------------------|-------------------------------------|--------------------------|
| [5, 5, 5] | 1 | $2^9 \cdot 5^5$ | $x^5 - 1$ |
| [5, 10, 20] | $2^{12}$ | $2^{10} \cdot 5^6$ | $4x^5 - 30x^3 + 45x - 22$ |
| [5, 65, 845] | 11 | $2^{11} \cdot 5^6, 13^{10}$ | $8x^5 + 52x^3 - 250x - 321x - 131$ |
| [5, 85, 1445] | 21 | $2^{-4} \cdot 17^{20}$ | $-73x^5 + 1005x^3 + 14430x^2 - 13024x + 1029840x^2 + 760976x - 2315640$ |

Table 1b

| DAB | $\Delta_{\text{stable}}$ | $\Delta(C)/\Delta_{\text{stable}}$ | $f$, where $C : y^2 = f$ |
|-----|---------------------------|-------------------------------------|--------------------------|
| [5, 15, 45] | $(2)^{12} \cdot (3)^6$ | $(2a + 1)^{10}$ | $-x^6 + (3a + 3)x^3 + (5a + 15)x^2 + (15 - 15a)x - 4(a + 1)$ |
| [5, 30, 180] | $(3a + 2)^{11} \cdot (2a - 1)^{10}$ | $(2a + 1)^{10}$ | $684x^6 + (390a + 90)x^3 + (24a + 3138)x^2 + (217a + 401)x^2 + (96a + 3918)x^2 + (-2112a + 1698)x + 284a + 432$ |
| [5, 35, 245] | $(3a + 2)^{11} \cdot (2a - 1)^{10}$ | $(2a + 1)^{10}$ | $(927a + 2906)x^6 + (5641a + 1882)x^4 + (-35355a - 124380)x^3 + (33417a + 183726)x + 12641a - 31928$ |
| [5, 105, 2205] | $(3a + 1)^{11} \cdot (2a + 9)^{10}$ | $(2a + 1)^{10}$ | $(-452a + 783)x^3 + (6392a + 7811)x^3 + (-4500a - 17085)x^3 + (-6948a + 9783)x - 1687a + 39$ |

Continued on next page
\[
\begin{array}{|c|c|c|c|}
\hline
\text{DAB} & \Delta_{\text{stable}} & \Delta(C)/\Delta_{\text{stable}} & f, \text{ where } C : y^2 = f \\
\hline
[17, 255, 15300] & (2a - 5)b^2 \cdot (a + 2)_{i+2}^2 & (a + 1)_{i+7}^{10} \cdot (5)^{10} & (-1246a - 1320b) x^2 + (9516a - 9411b) x^3 + (331770a - 503670b) x^4 + \\
& \cdot (a - 1)_{i+2}^2 \cdot (3)^b \cdot (2a + 31)_{i+1}^2 & & (-1195640a + 1593625b) x^2 + (1141785a - 2476410b) x^3 + \\
& & & (-69927a + 254047b) x + 301251a - 1280828 \\
\hline
& (2a + 3)_{i+2}^2 \cdot (a + 17)_{i+2}^2 \cdot (2a + 7)_{i+2}^2 & (a + 1)_{i+7}^{10} \cdot (5)^{10} & (3703196a + 9037010b) x^2 + \\
& \cdot (a + 2)_{i+2}^2 \cdot (a - 1)_{i+2}^2 \cdot (3)^b & & (12666396a + 36366348b) x^2 + (331333830a + 56148570b) x^4 + \\
& \cdot (4a + 3)_{i+2}^2 \cdot (2a - 9)_{i+1}^2 \cdot (a + 11)_{i+2}^2 & & (35333760a + 111063545b) x^3 + (71845845a + 45282075b) x^2 + \\
& & & (154100103a - 105860229b) x + 81081415a - 36366223 \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|c|}
\hline
\text{DAB} & \text{DAB}^r & a & \Delta_{\text{stable}} & \Delta(C)/\Delta_{\text{stable}} & f, \text{ where } C : y^2 = f \\
\hline
[5, 11, 29] & [29, 7, 5] & \alpha^2 + 3 & (2)_{i+2}^{12} \cdot (a - 1)_{i+2}^2 \cdot (a + 1)_{i+2}^2 & (a + 2)_{i+5}^{10} & (18a + 60)x^2 + (-76a - 246)x^3 + (127a + 329)x^4 + \\
& & & & & (-77a - 209)x^3 + (-30a + 155)x^2 + \\
[5, 13, 41] & [41, 11, 20] & \alpha^3 + 5 & (a - 3)_{i+2}^2 & (a + 4)^{20} \cdot (2a - 5)_{i+5}^{10} & (a + 4)x + 1 \\
& & & & & (-a + 3)x^2 + (4a - 8)x^3 + 10x^4 + (-a + 20)x^4 + (a + 5)x^2 + \\
[5, 17, 61] & [61, 9, 5] & \alpha^3 + 4 & (a - 3)_{i+2}^2 & (2)_{i+8}^{20} \cdot (a - 4)_{i+5}^{10} & (a - 4)x^2 + (-8a - 42)x^3 + (37a + 117)x^4 + \\
& & & & & (-20a - 240)x^4 + (56a - 9)x^2 + (22a - 114)x + 9a - 28 \\
[5, 21, 109] & [109, 17, 45] & \alpha^2 + 8 & (a - 5)_{i+2}^2 \cdot (3a + 17)_{i+2}^2 & (2)_{i+8}^{20} \cdot (3a - 14)_{i+5}^{10} & (-125a - 8575)x^2 \\
& & & & & + (-1375a - 8575)x^3 + (-9090a - 62160)x^4 + \\
& & & & & (-388862a - 251798)x^3 + (-73257a - 49843)x^2 + \\
& & & & & (-53235a - 347403)x - 12896a - 86314 \\
[5, 26, 149] & [149, 13, 5] & \alpha^2 + 6 & (a + 7)_{i+2}^2 \cdot (a - 5)_{i+2}^2 & (2)_{i+6}^{20} \cdot (a - 6)_{i+5}^{10} & (27a - 96)x^2 + (-9a - 51)x^3 + \\
& & & & & (-34a - 58)x^3 + (-18a - 36)x^2 - 15x - 9a - 27 \\
[5, 33, 261] & [29, 21, 45] & \alpha^2 + 3 & (a + 5)_{i+2}^2 \cdot (3)^6 & (2)_{i+2}^{20} \cdot (a + 2)_{i+5}^{10} & (-283a + 2246)x^2 + \\
& & & & & (-4563a + 33800)x^3 + (-11932a + 103166)x^4 = \\
& & & & & (127408a - 1032304)x^3 + (998576a - 755808)x^2 + \\
& & & & & (2429792a - 18969664)x^2 + 2110776a - 16149072 \\
[5, 34, 269] & [269, 17, 5] & \alpha^2 + 8 & (a - 7)_{i+2}^2 \cdot (2a - 15)_{i+3}^2 \cdot (a + 9)_{i+2}^2 & (2)_{i+8}^{20} \cdot (a - 8)_{i+5}^{10} & ((124a - 11695)x^5 + \\
& & & & & (-1609a + 150611)x^5 + (37185a - 349530)x^4 + \\
& & & & & (250806a - 2359698)x^3 + (-97208a + 9046728)x^2 + \\
& & & & & (-942318a + 8701533)x + 4994791a - 46866753 \\
[5, 41, 389] & [389, 37, 245] & \alpha^2 + 18 & (2a + 1)_{i+2}^2 \cdot (8a + 83)_{i+3}^2 \cdot (5a + 52)_{i+2}^2 \cdot (3a - 28)_{i+2}^2 & (2)_{i+31}^{20} \cdot (3a + 31)_{i+5}^{10} & (-340a - 1674)x^2 + \\
& & & & & (-4179a - 26820)x^3 + (-2643a - 11880)x^4 + \\
& & & & & (-38358a - 315240)x^3 + (-46686a - 41130)x^2 + \\
& & & & & (40761a - 15348)x - 13013a + 39100 \\
[5, 66, 909] & [101, 33, 45] & \alpha^2 + 5 & (a - 2)_{i+2}^2 \cdot (3)^6 \cdot (2a + 13)_{i+2}^2 \cdot (a - 4)_{i+2}^2 & (2)_{i+5}^{20} \cdot (a + 5)_{i+5}^{10} & \\
\hline
\end{array}
\]

Continued on next page
| DAB | DAB' | $a$ | $\Delta_{\text{stable}}$ | $\Delta(C)/\Delta_{\text{stable}}$ | $f$, where $C : y = f$ |
|-----|------|-----|--------------------------|-----------------------------------|---------------------------------|
| [8, 10, 17] | [17, 5, 2] | $\alpha^2 + 2$ | $(a + 2)^\frac{21}{2}$ | $(a + 2)^{20} \cdot (a - 1)^{20}$ | $x^6 + (2a + 4)x^5 + (3a + 14)x^4 + (10a + 8)x^3 + (9a + 32)x^2 + (16a - 16)x - 4a - 8$ |
| [8, 18, 73] | [73, 9, 2] | $\alpha^2 + 4$ | $(a - 4)^\frac{6}{2} \cdot (a + 5)^{12}$ | $(a - 4)^{45}$ | $(a + 5)x^8 + (28a + 132)x^7 + (214a + 1026)x^6 + (349a + 1658)x^5 + (259a + 1242)x^4 + (47a + 222)x - 3a - 14$ |
| [8, 22, 89] | [89, 11, 8] | $\alpha^2 + 5$ | $(a - 4)^\frac{6}{2} \cdot (a + 5)^{12}$ | $(a + 5)^{45}$ | $(a - 4)x^8 + (8a - 36)x^7 + (16a - 62)x^6 + (-13a + 57)x^5 + (-17a + 73)x^4 + (13a - 57)x^3 - a - 5$ |
| [8, 34, 281] | [281, 17, 2] | $\alpha^2 + 8$ | $(42a - 331)^\frac{12}{2} \cdot (a - 8)^6 \cdot (a + 9)^{24} \cdot (76a + 675)^{12}$ | $(a - 8)^{45}$ | $(a + 5024a + 118185)x^6 + (3190153a - 2435026)x^5 + (-2658057a + 2099048)x^4 + (12047831a - 97400942)x^3 + (-33280854a + 23138092)x^2 + (34989188a - 413796872)x - 37610304a + 81055944$ |
| [8, 38, 233] | [233, 19, 32] | $\alpha^2 + 9$ | $(38a - 271)^\frac{12}{2} \cdot (a - 8)^{12} \cdot (a - 7)^2 \cdot (8a + 65)^{12}$ | $(a - 7)^{45}$ | $(-166628a - 1355047)x^6 + (-354121a - 2879769)x^5 + (-318274a - 2588269)x^4 + (-153661a - 1249743)x^3 + (-418274a - 339754)x^2 + (-6158a - 48444)x + 414a - 2400$ |
| [8, 50, 425] | [17, 25, 50] | $\frac{1}{3}\alpha^2 + 2$ | $(a + 2)^\frac{21}{2} \cdot (a - 1)^{24} \cdot (5)^6$ | $(a + 2)^{45} \cdot (5)^{15}$ | $(34a + 80)x^8 + (140a + 224)x^7 + (110a - 220)x^6 + (-455a + 220)x^5 + (-5a + 190)x^4 + (91a - 104)x + 254a + 395$ |
| | | | $(2a + 3)^{12} \cdot (2a - 5)^{12}$ | $(a + 2)^{45} \cdot (5)^{15}$ | $(-1455a + 1511) x^8 + (-1004a - 2656)x^6 + (-19100a + 20290)x^4 + (-3805a - 4380)x^3 + (-72745a + 108600)x^2 + (-7451a + 10748)x - 99295a + 155108$ |
| [8, 66, 1017] | [113, 33, 18] | $\frac{1}{3}\alpha^2 + 5$ | $(a - 6)^\frac{12}{2} \cdot (a + 6)^{12}$ | $(a - 5)^{45}$ | $(-4215a - 14698)x^8 + (30030a + 338652)x^7 + (-549576a - 134610)x^6 + (-2954519a + 22716733)x^5 + (12849441a - 7660151) x^4 + (234523575a - 1115687637)x - 843111919a + 405444133$ |
| [13, 9, 17] | [17, 15, 52] | $\alpha^2 + 7$ | $(a + 2)^\frac{21}{2}$ | $(a - 2)^{10} \cdot (a - 1)^{20}$ | $(a - 2)x^7 + (-8a + 8)x^6 + (14a - 32)x^5 + (-19a + 27)x^4 + (6a - 21)x^3 + (3a + 9)x - 4a - 7$ |
| [13, 18, 29] | [29, 9, 13] | $\alpha^2 + 4$ | $(a - 1)^\frac{21}{2}$ | $(a - 4)^{10} \cdot (2)^{20}$ | $(9a - 22)x^7 + (-19a + 21)x^6 + (8a - 95)x^5 + (-70a - 6)x^4 + (-14a - 148)x^3 + (-7a - 127)x - 18a - 7$ |
| [13, 29, 181] | [181, 41, 13] | $\frac{1}{3}\alpha^2 + \frac{19}{4}$ | $(6a - 37)^\frac{12}{2} \cdot (a - 6)^{12}$ | $(3a - 19)^{10} \cdot (2)^{20}$ | $(-16581a - 119826)x^9 + (-52472a - 379062)x^8 + (-67729a - 508419)x^4 + (-78876a - 162464)x^3 + (-44960a + 21657)x^2 + (14402a - 141141)x - 21885a + 131494$ |

Continued on next page
| DAB     | DAB'   | $a$          | $\Delta_{stable}$                                                                 | $\Delta(C)/\Delta_{stable}$         | $f$, where $C : y^2 = f$                                                                 |
|---------|--------|--------------|-----------------------------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------|
| [13, 41, 157] | [157, 25, 117] | $\alpha^2 + 12$ | $(3a + 20)\frac{12}{11} \cdot (a - 7)\frac{12}{11} \cdot (a + 6)\frac{12}{11} \cdot (a + 7)\frac{12}{11}$ | $(2a - 11)\frac{10}{13} \cdot (2)^{20}$ | $(-1181a + 7035)x^9 + (18395a - 104353)x^5 + (116071a + 664673)x^4 + (386042a - 2282384)x^3 + (-742970a + 4253365)x^2 + (784564a - 4063679)x - 253294a + 2224205$ |
| [17, 5, 2] | [8, 10, 17] | $\frac{1}{10}a^2 + \frac{1}{5}$ | 1 | $(3a + 1)\frac{10}{13} \cdot (a)^{20}$ | $(-3a + 4)x^2 - x^3 + (6a - 2)x^2 + (9a - 5)x^2 + (6a + 8)x - 3a + 6$ |
| [17, 15, 52] | [13, 9, 17] | $\alpha^2 + 4$ | $(a)^{12} \cdot (a)^{12}$ | $(a - 4)\frac{10}{13} \cdot (2)^{20}$ | $-x^2 - 2ax^2 + (3a - 3)x^4 + (8a + 4)x^3 + (-19a + 39)x^2 + (16a - 30)x + 3a - 36$ |
| [17, 25, 50] | [8, 50, 425] | $\frac{1}{10}a^2 + \frac{5}{2}$ | $(a)^{12} \cdot (2a + 1)\frac{12}{13}$ | $(3a + 1)\frac{10}{13} \cdot (5)^{10}$ | $(6a - 2)x^2 + (-50a - 64)x^5 + (285a + 485)x^4 + (-485a - 435)x^3 + (-70a + 90)x^2 + (244a + 92)x + 70a - 166$ |
| [17, 46, 257] | [257, 23, 68] | $\alpha^2 + 11$ | $(11a + 5)\frac{12}{11} \cdot (13a + 10)\frac{12}{11} \cdot (2a)\frac{12}{11} \cdot (2, a + 1)\frac{24}{25}$ | $(17a + 6)\frac{10}{13} \cdot (2, a + 1)\frac{20}{21}$ | $(-22a - 1802)x^9 + (3596a + 11488)x^5 + (-3070a - 354072)x^4 + (243927a + 18439299)x^3 + (-616892a + 5576996)x^2 + (647768a + 5283496)x - 198146a - 1755298$ |
| [17, 47, 548] | [137, 35, 272] | $\alpha^2 + 17$ | $(14a - 75)\frac{12}{11} \cdot (4a + 25)\frac{12}{13} \cdot (3a - 16)\frac{12}{11} \cdot (3a + 19)\frac{12}{13}$ | $(8a + 51)\frac{10}{13}$ | $(285a + 1620)x^9 + (-2683a - 19110)x^5 + (13341a + 76698)x^4 + (28642a - 195577)x^3 + (40284a + 245904)x^2 + (27600a - 177408)x + 8154a + 51670$ |
| [29, 7, 5] | [5, 11, 29] | $\alpha^2 + 5$ | $(2)\frac{12}{11} \cdot (2a + 1)\frac{12}{13}$ | $(a - 5)\frac{10}{13} \cdot (29)^{20}$ | $(-4a - 5)x^5 + (11a + 37)x^3 + (-65a - 62)x^4 + (111a + 104)x^3 + (-28a - 189)x^2 + (28a + 157)x - 19a - 76$ |
| [29, 9, 13] | [13, 18, 29] | $\frac{1}{10}a^2 + \frac{1}{5}$ | $(a)^{12}$ | $(2)\frac{20}{13} \cdot (3a + 2)\frac{10}{13}$ | $(-25a + 56)x^5 + (172a - 39)x^4 + (-39a + 561)x^3 + (312a + 234)x^3 + (73a + 354)x^2 + (76a + 141)x + 15a + 37$ |
| [29, 21, 45] | [5, 33, 261] | $\alpha^2 + 6$ | $(4a + 1)\frac{12}{11} \cdot (3)^{6}$ | $(2)\frac{20}{13} \cdot (a - 5)\frac{10}{13}$ | $(-a + 20)x^5 + (-87a - 18)x^4 + (-48a + 198)x^4 + (-8a - 296)x^3 + (384a + 360)x^2 + (-384a - 480)x + 14a + 216$ |
| [29, 26, 53] | [53, 13, 29] | $\alpha^2 + 6$ | $(a - 1)\frac{12}{11} \cdot (a + 1)\frac{12}{13} \cdot (a + 6)\frac{12}{11}$ | $(2)\frac{20}{13} \cdot (a - 6)\frac{10}{13}$ | $(-790a + 1564a)x^9 + (241a - 12431)x^5 + (-15139a - 14345)x^4 + (-2950a - 165614)x^3 + (-51588a - 116086)x^2 + (-58139a - 53507)x + 12653a - 123381$ |
| [41, 11, 20] | [5, 13, 41] | $\alpha^2 + 6$ | 1 | $(a + 4)x^5 + (6a - 2)x^4 + (12a - 16)x^4 + (24a - 5)x^2 + (5a - 16)x + 33a + 9$ | |
| [53, 13, 29] | [29, 26, 53] | $\frac{1}{10}a^2 + \frac{1}{5}$ | $(a + 6)\frac{12}{11} \cdot (a - 1)\frac{12}{13} \cdot (a)^{12}$ | $(2)\frac{20}{13} \cdot (3a + 5)\frac{10}{13}$ | $(-31a + 70)x^5 + (151a - 322)x^4 + (-405a + 658)x^4 + (238a - 846)x^3 + (3288a + 2437)x^2 + (-3262a + 12157)x - 27420a - 58255$ |
| DAB     | DAB'   | $a$          | $\Delta_{\text{stable}}$ | $\Delta(C)/\Delta_{\text{stable}}$ | $f$, where $C : y^* = f$          |
|---------|--------|--------------|--------------------------|-------------------------------------|----------------------------------|
| [61, 9, 5] | [5, 17, 61] | $\frac{1}{2}a^2 + \frac{9}{4}$ | 1 | $(2a)^{20} \cdot (7a + 4)^{10}_{61}$ | $(a + 2)x^6 + (2a - 16)x^5 + (36a - 4)x^4 + (72a + 24)x^3 + (8a - 24)x^2 + (48a - 80)x - 24a - 40$ |
| [73, 9, 2] | [8, 18, 73] | $\frac{1}{2}a^2 + \frac{9}{4}$ | $(a)^{24}_2 \cdot (2a - 1)^{12}$ | $(a - 9)^{10}_{73}$ | $(-12a - 6)x^7 + (8a + 82)x^5 + (-51a + 92)x^4 + (-126 - 36a + 35)x^2 + (32a + 50)x + 10a + 8$ |
| [73, 47, 388] | [97, 94, 657] | $\frac{1}{2}a^2 + \frac{41}{9}$ | $(20a + 109)^{12}_{73} \cdot (7a + 3)^{24}_{388}$ | $(2a + 11)^{12}_{73} \cdot (30a + 163)^{12}_{97}$ | $(22a + 119)^{10}_{657}$ | $(23a - 43)x^9 + (-149a - 1221)x^7 + (867a + 44883)x^4 + (-12083a - 690879)x^3 + (928849a + 5037588)x^2 + (123515a + 671208)x + 40236a + 21640$ |
| [89, 11, 8] | [8, 22, 89] | $\frac{1}{2}a^2 + \frac{11}{7}$ | $(a)^{24}_2 \cdot (2a + 1)^{12}$ | $(7a + 3)^{10}_{118}$ | $-x^8 + (-4a + 2)x^6 + 21x^4 + (-16a + 64)x^2 + (-160a + 142a - 190$ |
| [97, 94, 657] | [73, 47, 388] | $\frac{1}{2}a^2 + \frac{22}{7}$ | $(4a + 3)^{12}_{73} \cdot (4a + 1)^{12}_{94} \cdot (3a + 3)^{12}_{388}$ | $(2a + 1)^{12}_{73} \cdot (3a + 1)^{12}_{47}$ | $(24a + 115)^{10}_{657}$ | $(-12825a - 611298)x^6 + (-984572a - 4709700)x^5 + (-3071730a - 15394554)x^4 + (-6889060a - 20077475)x^3 + (-39056057a + 105535530)x^2 + (174191751a - 679661406)x + 256866552a - 97371416$ |
| [101, 33, 45] | [5, 66, 909] | $\frac{1}{12}a^2 + \frac{9}{4}$ | $(3)^6 \cdot (2a + 1)^{12} \cdot (7a + 3)^{12}_{66}$ | $(9a + 5)^{10}_{101} \cdot (2)^{20}$ | $(-216a + 464)x^8 + (-230a - 48)x^7 + (-3984a - 960)x^6 + (-864a + 3088)x^5 + (-720a + 1422)x^4 + (-404a - 5322)x + 818a + 2423$ |
| [109, 17, 45] | [5, 21, 109] | $\alpha^2 + 10$ | $(2a + 1)^{12}_{109}$ | $(-8a - 10^0_{109} \cdot (2)^{20}$ | $(-8a - 8)x^6 - 8a + 72)x^5 + (152a + 184)x^4 + (6a + 84)x^3 + (-255a - 339)x + 319a - 524$ |
| [113, 33, 18] | [8, 66, 1017] | $\frac{1}{2}a^2 + \frac{11}{7}$ | $(3a + 11)^{12}_{113}$ | $(3a + 1)^{12}_{8} \cdot (2a + 1)^{12}$ | $(2a - 11)^{10}_{113}$ | $(122a + 800)x^6 + (-1509a - 909)x^5 + (36762a - 85470)x^4 + (-11687a + 265713)x^3 + (-467682a + 704460)x^2 + (-480582a + 365352)x - 7616a + 220442$ |
| [137, 35, 272] | [17, 47, 548] | $\alpha^2 + 23$ | $(2a - 5)^{12}_{137} \cdot (a + 2)^{12}_{47} \cdot (a - 1)^{12}_{52}$ | $(6a - 1)^{10}_{137}$ | $(4a + 6)x^6 + (8a + 36)x^5 + (-4a + 42)x^4 + (586a + 1289)x^3 + (1066a + 2808)x^2 + 4ax + 25596a + 6556$ |
| [149, 13, 5] | [5, 26, 149] | $\frac{1}{2}a^2 + \frac{11}{7}$ | $(3a + 1)^{12}_{149}$ | $(11a + 7)^{10}_{149} \cdot (2)^{20}$ | $8x^6 + 96x^5 + (-24a + 168)x^4 + (-576a - 808)x^3 + (66a - 132)x^2 + (292a + 47)x + 86a - 87$ |
| [157, 25, 117] | [13, 41, 157] | $\frac{1}{2}a^2 + \frac{11}{7}$ | $(a - 4)^{12}_{157} \cdot (3a - 1)^{12}_{41} \cdot (a + 1)^{12}_{157}$ | $(7a + 5)^{10}_{157} \cdot (2)^{20}$ | $(-3328a - 7633)x^6 + (-17510a - 39323)x^5 + (-32518a - 68044)x^4 + (-17960a - 66720)x^3 + (256a - 51704)x^2 + (5184a - 22864)x + 1432a - 5264$ |
| [181, 41, 13] | [13, 29, 181] | $\frac{1}{2}a^2 + \frac{13}{7}$ | $(a + 5)^{12}_{181} \cdot (3a + 2)^{12}_{41} \cdot (a + 1)^{12}_{29}$ | $(3a - 13)^{10}_{181} \cdot (2)^{20}$ | $(330a + 1417)x^6 + (11102a + 1701)x^5 + (1396a + 59742)x^4 + (24016a + 92792)x^3 + (74408a + 38064)x^2 + (3524a + 26160)x - 5784a + 21888$ |
| [233, 19, 32] | [8, 38, 233] | $\frac{1}{2}a^2 + \frac{20}{7}$ | $(a)^{24}_2 \cdot (a - 5)^{12}_{23} \cdot (a + 5)^{12}_{23} \cdot (2a + 1)^{12}_7$ | $(11a + 3)^{10}_{233}$ | $(2348a - 3554)x^6 + (11828a - 12348)x^5 + (4498a - 23598)x^4 + (12704a + 9133)x^3 + (-3151a - 14433)x^2 + (5344a - 1974)x + 18a - 604$ |
| DAB       | DAB′  | a             | $\Delta_{\text{stable}}$                                                                 | $\Delta(C)/\Delta_{\text{stable}}$ | $f$, where $C : y^2 = f$                                                                 |
|-----------|-------|---------------|-----------------------------------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------|
| [257, 23, 68] | [17, 46, 257] | $\frac{1}{8}a^2 + \frac{19}{8}$ | $(2a + 3)\frac{12}{13} \cdot (a + 2)\frac{12}{13}$  
$\cdot (a - 1)\frac{12}{13} \cdot (4a - 3)\frac{12}{13}$  
$\cdot (2a + 9)\frac{12}{13} \cdot (4a + 13)\frac{12}{13}$ | $(8a - 19)\frac{10}{257}$ | $(-2809a - 7326)x^8 +$  
$(5069a + 3572)x^7 + (52427a - 51416)x^4 +$  
$(249518a + 105951)x^3 + (-311115a - 180355)x^2 +$  
$(156533a - 20215)x - 34657a + 19003$ |
| [269, 17, 5] | [5, 34, 269] | $\frac{1}{4}a^2 + \frac{15}{4}$ | $(3a + 1)\frac{12}{11} \cdot (2a + 1)\frac{12}{11}$ | $(2)\frac{20}{15a + 11}$ | $(-168a - 272)x^9 + (960a + 1696)x^8 + (472a - 1008)x^9 +$  
$(-448a - 1552)x^8 + (358a + 904)x^2 + (945a + 1690)x$ |
| [281, 17, 2] | [8, 34, 281] | $\frac{1}{2}a^2 + \frac{17}{2}$ | $(a)\frac{36}{31} \cdot (4a + 1)\frac{12}{31}$  
$\cdot (2a - 1)\frac{12}{31} \cdot (2a + 1)\frac{12}{31}$ | $(2a - 17)\frac{10}{281}$ | $(-835a + 1960)x^5 + (1343a + 7589)x^6 + (19630a + 6428)x^4 +$  
$(26923a + 13601)x^3 + (-6743a + 44228)x^2 +$  
$(-5762a + 18262)x + 17138a - 23184$ |
| [389, 37, 245] | [5, 41, 389] | $\frac{1}{6}a^2 + \frac{18}{5}$ | $(3a + 1)\frac{12}{15} \cdot (3a + 2)\frac{12}{15}$  
$\cdot (4a + 3)\frac{12}{15} \cdot (4a + 1)\frac{12}{15}$  
$\cdot (a + 6)\frac{12}{15} \cdot (2a + 1)\frac{12}{15}$ | $(2)\frac{20}{18a + 13}$ | $(-22952a - 6848)x^9 +$  
$(162272a - 61136)x^5 + (296568a + 208208)x^4 +$  
$(-212600a - 959344)x^3 + (89874a + 1610270)x^2 +$  
$(-428348a - 1023457)x + 315516a + 343397$ |
5 Application

Obviously, we hope that our list is useful for experimenting with complex multiplication and hyperelliptic curves. Additionally, this final section gives a cryptographic application: the small coefficients of the curves in our table allow for faster communication and arithmetic.

Cryptographic hyperelliptic curves are constructed as follows using the theory of complex multiplication (for details, see [6]).

1. Compute the Igusa invariants $I_0(\tilde{C})$ of a genus-two curve $\tilde{C}$ with CM by an order $O_K$ over a number field $L$.

2. Reduce these invariants modulo a prime $p$ of $L$, which yields elements of the residue field $k = O_L/p$.

3. Construct a curve $C$ over the finite field $k$ with these invariants, using Mestre’s algorithm.

Then there is a relation between the CM-type $(K, \Phi)$ of $\tilde{C}$ and the number of $k$-points in the Jacobian groups of $C$ and its quadratic twist $C'$. So with a good choice of $\Phi$ and $p$, we can construct curves $C$ for which $J_C(k)$ has a prescribed prime order, or other interesting cryptographic properties.

In the end, the coefficients of the curve are random-looking elements of $k$, so if $k$ has $q$ elements, these coefficients take up about $\log_{10}(q)$ digits each, where $q$ is a cryptographically large prime power.

Now if the CM-field $K$ is one of the fields in our table, we can do better: we can take $\tilde{C}$ from our table, and let $C$ be $(\tilde{C} \mod p)$. This curve then has coefficients of a simple and elegant shape. This saves bandwidth when communicating this curve. It also saves “carries” in multiplication operations involving curve coefficients, making them potentially much more efficient.

For example, in [10] Section 8, Example of Algorithm 3 a curve $C$ is constructed following the recipe 1., 2., 3. with $\Phi$ a certain CM-type of $K = [5, 13, 41]$ This curve is defined over a finite
field $k = \mathbb{F}_{p^2}$, where

\[
p = 1420038565807482747635387048977088071520136032341569
\]

\[
014612056864049709760143646636956724980664377491196079
\]

\[
73051961772352102985564946217214869939358968636852107
\]

\[
696147277436345811056227385195781997362304851932650270
\]

\[
514293705125991379
\]

and $J_C(k)$ has a cryptographic subgroup of order $r = 2^{192} + 18513$. The curve $C$ is given by $C : y^2 = \sum_{n=0}^{6} a_n x^n$, and simple transformations make $a_0$ small (either 1 or a small non-square in $k$) and ensure $a_0 = 0$. Then there are five coefficients $a_0, \ldots, a_4 \in \mathbb{F}_{p^2}$, each taking up twice as much space as the number $p$ written above, hence more than 2000 digits in total.

Now let us look up $K = [5, 13, 41]$ in the table. Let $a$ be a root of $X^2 + 10$ over $\mathbb{Q}$. We find that up to twist and up to conjugation of $K^0 = \mathbb{Q}(a)/\mathbb{Q}$, we have $C : y^2 = f(x)$, where

\[
f(x) = (-a + 3) x^6 + (4a - 8) x^5 + 10 x^4 + (-a + 20) x^3 + (4a + 5) x^2 + (a + 4) x + 1.
\]

Consequently, if we write by abuse of notation $a$ also for a root of $X^2 + X - 10$ generating a quadratic extension $k = \mathbb{F}_{p^2}/\mathbb{F}_p$, then the curve $C$ is given by the same equation. Again up to twist and conjugation of $k/\mathbb{F}_p$.

Conjugation does not affect the number of points of $C(k)$, and as $(a - 2)$ is a non-square in $k^*$, we find that the only non-isomorphic twist of $C$ is given by $y^2 = (a - 2) f(x)$, which also has very simple coefficients.

**Remark 5.1.** For completeness, we determine which twist of $C$ gives a subgroup of order $r$ in $J_C(k)$. Let $\pi \in K$ be the Frobenius endomorphism of $C$. Then $[\pi] = p\mathfrak{B}_2$ where $p\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$ by [10] Lemma 21]. This fixes $\pi$ up to complex conjugation and roots of unity, hence gives two candidates $N(\pi - 1)$ and $N(-\pi - 1)$ for the order of $J_C(k)$. We compute these candidates and find that one of them, let’s call it $n_1$, is divisible by $r$ and the other, $n_2$, is not. Now let $D = 2(0, 1) - \infty$, that is, $D$ is the divisor given by twice $P = (0, 1)$ minus both points at infinity. We use Magma to check $n_2[D] \neq 0 \in J_C(k)$, which proves $\# J_C(k) = n_1$, so $C$ is itself the correct twist (and indeed we easily verify $n_1[D] = 0$). We also check $(n_1/r)(D) \neq 0 \in J_C(k)$, which proves that $(n_1/r)(D)$ generates the group of order $r$ in $J_C(k)$.

The following theorem gives our CM construction as a canned result.

**Theorem 5.2.** Let $K$, $K'$, $f$, and $\Delta(C)$ be as in an entry of Table 1a, 1b, or 2b other than $\Delta(\mathcal{O}_K) = [5, 5, 5]$. Let $p \mid \Delta(C)$ be a prime of $K_0$ that is not inert in $K'/K_0$ and let $k_\mathfrak{p}$ be its residue field. Let $\mathcal{T} = (f \bmod p)$ and let $b \in k_\mathfrak{p}$ be a non-square. Let $C_1$, $C_2$ be the curves $y^2 = \mathcal{T}$ and $y^2 = \mathcal{T}$ over $k_\mathfrak{p}$.

Let $\mathfrak{B}$ be a prime of $K'$ and $\Phi^\ast$ the CM-type of $K'$ with reflex field $K$ (uniquely determined up to complex conjugation). Then the ideal $N_{\mathfrak{B} \mathfrak{P}}(\mathfrak{P}) \subset \mathcal{O}_K$ is principal, and generated by an element $\pi$ such that $\pi \mathfrak{P} \subset \mathfrak{Q}$.

Moreover, the endomorphism rings of $J(C_i)$ over $k_\mathfrak{p}$ contain subrings isomorphic to $\mathcal{O}_K$ and the isomorphisms can be chosen in such a way that $\{\text{Frob}_{C_i,N(\mathfrak{p})}\} = \{\pm \pi\}$. In particular, we have $\# J(C_i)(k_\mathfrak{p}) = \{N_{K/(\mathfrak{Q} - \pi - 1)}\}$.

The computation of $\pi \in \mathcal{O}_K$ is straightforward using algebraic number theory. Deciding which of the $C_i$ has Frobenius $\pi$ and which has Frobenius $-\pi$ can be done by checking whether a random point on the Jacobian is annihilated by $N_{K/\mathbb{Q}(\pi - 1)}$. 

The following theorem gives our CM construction as a canned result.
If $p$ is totally split in $K$ and $p | p$, then we have $k_p = F_p = F_p$ and the $J(C_i)$ are ordinary abelian surfaces with endomorphism rings $\cong \mathcal{O}_K$. Note that we have a surjective map $\mathcal{O}_{K_0} = \mathbb{Z}[X]/(X^2 + \epsilon X + (\epsilon - D^r)/4) \to k_p$, and the coefficients of $C_i$ are represented by small elements of the ring $\mathcal{O}_{K_0}$, hence operations in the group $J(C_i)$ can be performed with a smaller number of carrying operations compared to when using curves with random coefficients.

**Proof of Theorem 5.2.** Our assumptions imply $k_p = k_p$, and our $\Phi^r$ is the reflex of $\Phi$ as defined in [21]. Moreover, they have good reduction at $p$ by $p | \Delta(C)$. Therefore, by the Shimura-Taniyama formula ([21 Theorem 1(ii) in Section 13.1] or [14 Theorem 4.1.2]), we have $	ext{Frob}_{C_i,N}(p)\mathcal{O}_K = \mathcal{O}_{K_0}(\Phi)$. This proves that the latter ideal has a generator $\pi$ with $\pi \pi \in \mathbb{Q}$. Such a generator is unique up to roots of unity, of which $\mathcal{O}_K$ contains only $\pm 1$. Since $b$ is a non-square, twisting by it changes the root of unity, hence $\{\pm \pi\}$ occurs exactly for $\{\Phi, b\}$.

**References**

[1] Gaetan Bisson and Marco Streng. On polarised class groups of orders in quartic CM-fields. preprint, arXiv:1302.3756, 2013.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Scientific, 2005.

[4] John William Scott Cassels and E. Victor Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge University Press, 1996.

[5] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[6] Gerhard Frey and Tanja Lange. Complex multiplication. In H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors, *Handbook of elliptic and hyperelliptic curve cryptography*, pages 455–473. Chapman & Hall/CRC, 2006.

[7] P. Gaudry, A. Kruppa, F. Morain, L. Muller, E. Thome, and P. Zimmermann. cado-nfs 1.1. An implementation of the number field sieve method. http://cado-nfs.gforge.inria.fr/

[8] Eyal Z. Goren and Kristin Lauter. Genus 2 curves with complex multiplication. *Int Math Res Notices*, 2012(5):1068 – 1142, 2012.

[9] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[10] Laura Hitt, Gary McGuire, Michael Naehrig, and Marco Streng. A CM construction for curves of genus 2 with $p$-rank 1. *Journal of Number Theory*, 131(5):920–935, 2011. arXiv:0811.3434.

[11] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.
[12] David Kohel et al. ECHIDNA algorithms for algebra and geometry experimentation. http://echidna.maths.usyd.edu.au/~kohel/dbs/complex_multiplication2.html, 2007.

[13] Serge Lang. Complex Multiplication, volume 255 of Grundlehren der mathematischen Wissenschaften. Springer, 1983.

[14] Serge Lang. Complex Multiplication, volume 255 of Grundlehren der mathematischen Wissenschaften. Springer, 1983.

[15] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. arXiv:1210.7841, 2012.

[16] Qing Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. Trans. Amer. Math. Soc., 348(11):4577–4610, 1996.

[17] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In Effective methods in algebraic geometry (Castiglioncello, 1990), volume 94 of Progr. Math., pages 313–334, Boston, MA, 1991. Birkhäuser Boston.

[18] Naoki Murabayashi and Atsuki Umegaki. Determination of all $\mathbb{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces. J. Algebra, 235(1):267–274, 2001.

[19] Goro Shimura. On the zeta function of an abelian variety with complex multiplication. The Annals of Mathematics, 94(2):504–533, 1971.

[20] Goro Shimura. Introduction to the Arithmetic Theory of Automorphic Functions. Princeton University Press, 1994.

[21] Goro Shimura. Abelian Varieties with Complex Multiplication and Modular Functions. Princeton University Press, 1998. Sections 1–16 essentially appeared before in [22].

[22] Goro Shimura and Yutaka Taniyama. Complex multiplication of abelian varieties and its applications to number theory, volume 6 of Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, Tokyo, 1961.

[23] William Stein et al. Sage mathematics software 4.7.2, 2011. http://www.sagemath.org/

[24] Michael Stoll and John E. Cremona. On the reduction theory of binary forms. J. Reine Angew. Math., 565:79–99, 2003.

[25] Marco Streng. An explicit reciprocity law for Siegel modular functions. preprint, arXiv:1201.0020, 2011.

[26] Marco Streng. Computing Igusa class polynomials. Accepted for publication by Mathematics of Computation, arXiv:0903.4766, 2012.

[27] Marco Streng and Florian Bouyer. Implementation of Mestre’s algorithm in Sage. http://trac.sagemath.org/sage_trac/ticket/6341

[28] Gerard van der Geer. Hilbert modular surfaces, volume 16 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Springer, Berlin, 1988.

[29] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. Mathematics of Computation, 68(225):307–320, 1999.
[30] Paul van Wamelen. Proving that a genus 2 curve has complex multiplication. *Math. Comp.*, 68(228):1663–1677, 1999.

[31] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. [http://www.math.wisc.edu/~thyang/RecentPreprint.html](http://www.math.wisc.edu/~thyang/RecentPreprint.html) 2007.

[32] Paul Zimmermann et al. GMP-ECM 6.4.2 (elliptic curve method for integer factorization), 2012. [https://gforge.inria.fr/projects/ecm/](https://gforge.inria.fr/projects/ecm/)