LMS J. Comput. Math. 18 (1) (2015) 507–538 © 2015 Authors
doi:10.1112/S1461157015000121

Examples of CM curves of genus two defined over the reflex field

Florian Bouyer and Marco Streng

Abstract

Van Wamelen [*Math. Comp.* 68 (1999) no. 225, 307–320] lists 19 curves of genus two over $\mathbf{Q}$ with complex multiplication (CM). However, for each curve, the CM-field turns out to be cyclic Galois over $\mathbf{Q}$, and the generic case of a non-Galois quartic CM-field did not feature in this list. The reason is that the field of definition in that case always contains 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.

We explain our methods for obtaining this list, including a new height-reduction algorithm for arbitrary hyperelliptic curves over totally real number fields. Unlike Van Wamelen, we also give a proof of our list, which is made possible by our implementation of denominator bounds of Lauter and Viray for Igusa class polynomials.

1. *Introduction*

We say that a curve C/k of genus g has *complex multiplication* (CM) if the endomorphism ring of its Jacobian over $\overline{k}$ 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 $\mathbf{Q}$ with complex multiplication (see for example [**7**, Theorem 7.30(ii)]). Analogously, Van Wamelen [**38**] gives a list of 19 curves of genus two over $\mathbf{Q}$ with CM by a maximal order (proven in [**1**, **39**]).

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. Murabayashi and Umegaki [**23**] 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 $\mathbf{Q}$.

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 $\mathbf{Q}$. Our end result is as follows.

THEOREM 1.1. *For every row of Tables 1a, 1b, and 2b, let* $K = \mathbf{Q}[X]/(X^4 + AX^2 + B)$, *where* $[D, A, B]$ *is as in the first column of the table. Then the curves* $C : y^2 = f(x)$ *where* f *is as in the last column are exactly all curves with complex multiplication by the maximal order of* K, *up to isomorphism over* $\overline{\mathbf{Q}}$ *and up to automorphism of* $\overline{\mathbf{Q}}$.

Received 24 December 2013; revised 22 January 2015.

2010 Mathematics Subject Classification 11G15, 14K22 (primary), 11Y99, 11G05, 11G07 (secondary).

The first-named author was supported by the University of Warwick Undergraduate Research Scholarship Scheme (URSS).

The second-named author was partially supported by EPSRC grant number EP/G004870/1 and by NWO Veni project number 639.031.243.

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 5 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 $\mathrm{End}(J(C)) = \mathcal{O}_K$ such that C is defined over the real quadratic subfield of the reflex field.

Now, let us give a more detailed overview of our methods, which form the bulk of this paper.

Given a quartic CM-field K, we compute the curves $C/\overline{\mathbf{Q}}$ of genus two with $\mathrm{End}(J(C)) \cong \mathcal{O}_K$ in three stages. First we compute the Igusa invariants $i_1(C)$, $i_2(C)$ and $i_3(C)$ as elements of $\overline{\mathbf{Q}}$. Second we compute an arbitrary model of C from its Igusa invariants. Third we reduce this model to a small model, that is, a model with integer coefficients of only a handful of digits.

Section 2 explains Igusa invariants and how to compute them, that is, the first stage of our algorithm. Our new contribution there is an implementation of denominator bounds of Lauter and Viray [**19**], which allows us to be the first to systematically compute and prove correctness of CM Igusa invariants.

Section 3 quickly reviews Mestre's algorithm for computing a model of C from its invariants; the middle stage of our algorithm.

Section 4 explains how to go from any model to a small model which is the final stage of our algorithm. Mestre's algorithm constructs curves with given invariants, but these curves have coefficients of thousands of digits, so we use a reduction algorithm to reduce the coefficient size. Our main new contribution there is a reduction algorithm based on Stoll and Cremona [**30**], including an implementation.

We applied this algorithm to fields in the Echidna database [**17**] and obtained our tables. Section 5 gives a detailed version of Theorem 1.1, explaining all columns of the tables. We end with a cryptographic application in § 6.

2. *Invariants and complex multiplication*

2.1. *Overview*

The first stage of our algorithm is, given a quartic CM-field K, to obtain the Igusa invariants of the curves C of genus two with $\mathrm{End}(J(C)) \cong \mathcal{O}_K$. There are various practical methods for doing so (complex analytic, p-adic, or using the Chinese Remainder Theorem) numerically up to some precision, and results have been collected also in the Echidna database [**17**].

However, we want a proven output and the only prior proven method is that of Streng [**34**], which in practice is too slow even for the relatively small discriminants we consider. This section explains the complex analytic method and shows how to make it into a method that is both practical and proven, using denominator bounds of Lauter and Viray [**19**].

Our algorithm for this part closely follows that of [**34**], so many of the details and proofs of what follows can be found there.

2.2. *Igusa invariants and Igusa class polynomials*

Since the goal of this section is to compute Igusa invariants, let us begin by reviewing them and explaining how they are represented by Igusa class polynomials. For details on Igusa invariants, see Igusa [**16**], and for details on Igusa class polynomials, see Streng [**34**].

For an elliptic curve E/k, the j-invariant $j(E) \in k$ uniquely specifies the isomorphism class of E over $\overline{k}$.

For a (smooth, projective, geometrically irreducible algebraic) 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 [**16**], 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 [**29**]. The last invariant, I_{10}, is related to the discriminant of f and is always non-zero. Actually, for efficiency we use $I_6' = \frac{1}{2}(I_2 I_4 - 3I_6)$ instead of I_6, but one can easily go back and forth using $I_6 = \frac{1}{3}(I_2 I_4 - 2I_6')$, see [**34**].

Isomorphic hyperelliptic curves have Igusa–Clebsch invariants that are equal up to a weighted scaling. In fact, for curves C and C', we have $C_{\overline{k}} \cong C'_{\overline{k}}$ if and only if there is a $\lambda \in \overline{k}^*$ such that for $j = 2, 4, 6, 10$ we have $I_j(C) = \lambda^j I_j(C')$.

In more geometric language, if $\mathbf{P}^{2,4,6,10}$ is the *weighted projective space* of weights $(2, 4, 6, 10)$ with the Igusa–Clebsch invariants as coordinates, then the subspace $\mathcal{M}_2 \subset \mathbf{P}^{2,4,6,10}$ defined by $x_{10} \neq 0$ is a coarse moduli space of genus-two curves in characteristic not dividing $2 \cdot 3 \cdot 5$.

Following [**34**], we make a choice of three *absolute Igusa invariants* i_1, i_2, i_3, which generate the function field of the moduli space

$$i_1 = \frac{I_4 I_6'}{I_{10}}, \quad i_2 = \frac{I_2 I_4^2}{I_{10}}, \quad i_3 = \frac{I_4^5}{I_{10}^2}.$$

Given a curve C, if $I_2(C) \neq 0$, then C is uniquely specified by i_1, i_2, i_3 because of $I_4 = I_2^2 i_2^{-2} i_3$, $I_6' = I_2^3 i_1 i_2^{-3} i_3$, and $I_{10} = I_2^5 i_2^{-5} i_3^2$. And if we are unlucky enough to find $I_2(C) = 0$, then variants of these absolute Igusa invariants will do the trick [**4**].

The Igusa class polynomials of a quartic CM-field K are polynomials that specify the values of $i_n(C)$ where C has CM by $\mathcal{O}_K$. In detail, they are

$$H_{K,1} = \prod_C (X - i_1(C)), \quad \widehat{H}_{K,n} = \sum_C i_n(C) \prod_{C' \ncong C} (X - i_1(C')) \in \mathbf{Q}[X],$$

for $n \in \{2, 3\}$, where C and C' range over isomorphism classes of curves with $\mathrm{End}(J(C)) \cong \mathcal{O}_K$.

One can recover the Igusa invariants $i_1(C), i_2(C), i_3(C)$ from these polynomials by taking all roots $i_1(C)$ of $H_{K,1}$ and letting, for $n \in \{2, 3\}$,

$$i_n(C) = \widehat{H}_{K,n}(i_1(C))/H'_{K,1}(i_1(C)),$$

assuming $H_{K,1}$ has no roots of multiplicity > 1. Again, if we are unlucky, there are ways to work around this [**32**, § III.5].

In particular, our goal in § 2 is to compute $H_{K,1}$ and $\widehat{H}_{K,n}$.

2.3. *Complex approximation of Igusa class polynomials*

Streng [**34**] explains in detail how to compute complex numerical approximations of $H_{K,1}$ and $H_{K,n}$. The only way in which we deviate from the method of [**34**] is by using interval arithmetic in our implementation.

Interval arithmetic is a computational model for $\mathbf{R}$ where real numbers are represented by intervals that contain them. For intervals a_i and a map $f : \mathbf{R}^n \to \mathbf{R}$, when asking the computer for $f(a_1, \ldots, a_n)$, it returns an interval that contains $f(x_1, \ldots, x_n)$ for all $x_i \in a_n$. Rounding is always done in such a way that the intervals are guaranteed to be correct, hence the user does not have to estimate rounding errors by hand.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

Given any integer $N > 0$, we compute F_1, F_2, $F_3 \in \mathbf{Q}[X]$ such that the polynomials $F_1 - H_{K,1}$ and $F_n - \widehat{H}_{K,n}$ are proven to have coefficients of absolute value $<2^{-N}$ as follows. Fix some precision $>N$ and do (floating point) interval arithmetic to that precision. If the output intervals are not small enough, then double the precision and start over.

2.4. *Denominators*

2.4.1. *Using denominator bounds.* The first stage of our algorithm for computing CM curves is computing their Igusa invariants, and we have so far determined that it suffices to compute the Igusa class polynomials $H_{K,1}$, $\widehat{H}_{K,2}$, $\widehat{H}_{K,3} \in \mathbf{Q}[X]$. In this section, we give references for how to compute a positive integer $\mathfrak{D} = \mathfrak{D}_K$ such that $\mathfrak{D}H_{K,1}$, $\mathfrak{D}\widehat{H}_{K,2}$, and $\mathfrak{D}\widehat{H}_{K,3}$ all have *integer* coefficients. In particular, if we use the method of § 2.3 to compute approximations F_1, F_2, F_3 of the Igusa class polynomials such that all coefficients of $F_1 - H_{K,1}$ and $F_n - \widehat{H}_{K,n}$ are proven to be of absolute value $<\frac{1}{2}\mathfrak{D}$, then by rounding the coefficients of $\mathfrak{D}F_i$ to the nearest integer and dividing by $\mathfrak{D}$, we recover the Igusa class polynomials.

The first upper bounds on the primes dividing the denominator of $H_{K,1}$ and $\widehat{H}_{K,n}$ were given by Goren and Lauter [**12**]. More recently they [**13**] also gave upper bounds on the exponents with which these primes occur, and combining these results leads to a correct number $\mathfrak{D}$ as above. This number is studied and used in [**34**], but is too large to yield a practical algorithm. An alternative of Bruinier and Yang [**3**, **40**] does give a very sharp number $\mathfrak{D}$, but puts too many restrictions on the quartic CM-field K. Fortunately, Lauter and Viray [**19**] managed to extend the latter bounds to general number fields in a way that stays sharp enough for our applications.

We have implemented the bounds of Lauter and Viray [**19**] in Sage, and made the implementation available at [**31**]. This finishes the first stage of our algorithm: computing CM Igusa invariants. We applied the denominator formulas of [**19**] quite straightforwardly, but those familiar with the formulas may wish to see a few more details. We give these details in § 2.4.2, but in order not to have to repeat the (complicated) formulas, this may be of use only for those who have [**19**] close by. Other readers may wish to skip to § 3.

Remark 2.1. Computing proven Igusa class polynomials is not possible only with the complex analytic method, but also with the methods based on p-adic numbers (for example [**5**, **10**]) and the Chinese Remainder Theorem (for example [**8**]). These methods first compute the coefficients of the polynomials as elements of $\mathbf{Z}/N\mathbf{Z}$, where N is a large power of a small prime or the product of a large set of small primes, and then recognise the coefficients as elements of $\mathbf{Q}$. For this final step to have a unique solution, one needs to know an upper bound b on the absolute value of the coefficient (given by a crude low-precision complex analytic computation). Suppose $N > 2b\mathfrak{D}$ is coprime to $\mathfrak{D}$, and suppose that a coefficient c is computed modulo N, so we know $a = (c \bmod N) \in \mathbf{Z}/N\mathbf{Z}$. Then take the unique representative $r \in \mathbf{Z}$ of $a\mathfrak{D} \in \mathbf{Z}/N\mathbf{Z}$ with $|r| \leqslant b\mathfrak{D}$. The coefficient is $c = r/\mathfrak{D} \in \mathbf{Q}$.

2.4.2. *Implementation details.* 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 [**19**, Theorem 2.1]. See [**40**, Proof of Theorem 9.1] for how exactly this applies to Igusa class polynomials, where only the constant coefficient $H_{K,1}$ is mentioned, though the proof applies to all coefficients of $H_{K,1}$ and $\widehat{H}_{K,n}$.

We used the obvious and straightforward way to evaluate all the numbers occurring on the right hand side of [**19**, Theorem 2.1], except for $\mathcal{J} = \mathcal{J}(d_u f_u^{-2}, d_x, t)$. For the number $\mathcal{J}$, which counts solutions to a ring embedding problem, we used 0 whenever [**19**, Theorem 2.4] proves it is 0, and we used the upper bound of [**19**, numbered displayed formula in Theorem 2.4] otherwise.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

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 $p \leqslant D/4$, where D is the discriminant of K_0. For each η and each $\ell \nmid I_\eta$, we computed the bound of [**19**, Theorem 2.3] on the ℓ-valuation of the denominator (and took ∞ as upper bound at $\ell \mid I_\eta$). Then, for each ℓ, we took the minimum over all η of this valuation bound. Finally, we sharpened the valuation bounds further using Goren and Lauter [**13**]. This final bound took a little over half an hour to compute, but was then small enough for our class polynomial computation to finish within half an hour. Indeed, the index I_η had to be $> \mathfrak{D}/4$, which made the bounds of [**19**] 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 $\leqslant \mathfrak{D}/4$, and that [**19**, Theorem 2.3] also holds if one only avoids the primes dividing the numbers δ in their formulas.

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

3. *Mestre's algorithm*

At this point, we have a number field k and Igusa invariants in this number field, and we wish to decide whether there is a curve of genus two over k with those Igusa invariants, and if so, compute any model of the form $y^2 = f(x)$ of that curve with $f \in k[x]$. This is done by Mestre's algorithm, which we will explain in this section. Nothing in this section is new, and our reference for this section is Mestre [**21**]. Note that we do not care about the size of the coefficients of f yet, as long as we can compute it. Reducing its size is in § 4.

Let k be any field of characteristic not 2, 3, or 5. Let

$$\mathcal{M}_2(\overline{k}) = \{(x_2, x_4, x_6, x_{10}) \in \overline{k}^4 \mid x_{10} \neq 0\}/k^*,$$

where $\lambda \in k^*$ acts by a weighted scaling $\lambda(x_2, x_4, x_6, x_{10}) = (\lambda^2 x_2, \lambda^4 x_4, \lambda^6 x_6, \lambda^{10} x_{10})$. We say that a point $x \in \mathcal{M}_2(\overline{k})$ is defined over k if $x \in \mathcal{M}_2(\overline{k})$ is stable under the action of $\mathrm{Gal}(\overline{k}/k)$. 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 the 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 [**21**], that finds a model for C given x, but it involves solving a conic, which is not always possible without extending the field. When it is possible to solve a conic over the base field, then it usually introduces large numbers, so that the output polynomial may have coefficients that are much too large to be practical.

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 [**4**] 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 [**21**] or [**35**]). 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 parametrisation $\varphi : \mathbf{P}^1 \to M_x$ over k. Let $\varphi^* : k[U, V, W] \to k[X, Z]$ be the ring homomorphism inducing this parametrisation. We get a hyperelliptic curve $C_\varphi : Y^2 = \varphi^*(T)$, that is, $C_\varphi : y^2 = T(\varphi(x : 1))$. The curve C_φ is a double cover of $\mathbf{P}^1$, ramified at the six points of $\mathbf{P}^1$ that map (under φ) to the six zeroes of T_x on M_x.

THEOREM 3.1 [21]. *Given $x \in \mathcal{M}_2(k)$, assume that the curve $C/\overline{k}$ with $x = (I_n(C))_n$ satisfies* $\mathrm{Aut}(C) = \{1, \iota\}$.
(1) *If $M_x(k) = \emptyset$, then C has no model over k.*
(2) *If $M_x(k) \neq \emptyset$, then C_φ/k as above is a model of C.*

We use Magma [2] to solve conics over number fields and we contributed our Sage implementation of Mestre's algorithm to Sage [29], where it is available (as of version 5.13) through the command `HyperellipticCurve_from_invariants`.

There are, by the way, many quadratic extensions $l \supset k$ over which it *is* possible to solve the conic: simply choose all but one of the coordinates for the conic point at will and solve for the remaining coordinate, which yields a conic point over a quadratic extension $l \supset k$.

4. *Reduction*

In the previous section we described Mestre's algorithm for finding models of genus-two curves over number fields k. However, these hyperelliptic models in practice have coefficients of hundreds of digits. In this section we describe how we make hyperelliptic curve equations over k smaller. We start by explaining the relation between twists of hyperelliptic curves and an action of $\mathrm{GL}_2(k) \times k^*$ on binary forms. The rest of the section is about $(\mathrm{GL}_2(k) \times k^*)$-reduction of binary forms, and our algorithm consists of two parts:
(1) making a binary form integral with discriminant of small norm (§ 4.2);
(2) making the heights of the coefficients small by $(\mathrm{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*)$-transformations, which preserve integrality and affect the discriminant only by units (§ 4.3).

We give the reduction algorithm for binary forms of general degree n, though it only applies to hyperelliptic curves in the case that n is even and $\geqslant 6$.

4.1. *Isomorphisms and twists*

Fix an integer $n \geqslant 3$ and a field k, and let $H_n(k)$ be the set of separable binary forms of degree n in $k[X, Z]$. We interpret $F(X, Z) \in H_n(k)$ also as the pair $(n, f(x))$, where $f(x) = F(x, 1) \in k[x]$ is a polynomial of degree n or $n-1$. In the case where n is even and $\geqslant 6$, let $g = (n-2)/2$ and interpret F as the hyperelliptic curve $C = C_f = C_F$ 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 $\mathbf{P}^{(1,g+1,1)}$.

Given any element of $H_{2g+2}(k)$, we would like to find an isomorphic hyperelliptic curve with coefficients of small height, so first we determine when two hyperelliptic curves are isomorphic.

Note the natural right group actions of scaling and substitution for any n,

$$H_n(k) \circlearrowleft k^* : (F(X, Z), u) \mapsto uF(X, Z), \quad \text{and}$$
$$H_n(k) \circlearrowleft \mathrm{GL}_2(k) : (F(X, Z), A) \mapsto F(A \cdot (X, Z)),$$

which together induce an action of $\mathrm{GL}_2(k) \times k^*$ on $H_n(k)$.

In terms of the polynomial $f(x) = F(x, 1) \in k[x]$, the action is

$$f(x) \cdot \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] = u\ (cx + d)^n f\left(\frac{ax + b}{cx + d} \right).$$

Note that a hyperelliptic curve C always has the identity automorphism and the *hyperelliptic involution* $\iota : C \to C : (x, y) \mapsto (x, -y)$. We will often assume that these are the only automorphisms.

PROPOSITION 4.1. *Given any two $F, F^\dagger \in H_{2g+2}(k)$, assume* $\mathrm{Aut}((C_F)_{\overline{k}}) = \{1, \iota\}$. *Then C_F and $C_{F^\dagger}$ are isomorphic over $\overline{k}$ if and only if F and $F^\dagger$ are in the same orbit under $\mathrm{GL}_2(k) \times k^*$.*

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

Proof. It is a standard result (see for example [**6**, p. 1] for the case of genus two) that two hyperelliptic curves C_F and $C_{F^\dagger}$ in $H_n(k)$ are isomorphic over k if and only if they are in the same orbit under $\mathrm{GL}_2(k) \times (k^*)^2$. Using $\mathrm{Aut}(C_{\overline{k}}) = \{1, \iota\}$, we get (see for example [**14**, Example C.5.1]) that all twists, up to isomorphisms over k, are given by the action of $H^1(k, \{1, \iota\}) = k^*/k^{*2} = \{1\} \times (k^*/k^{*2})$. □

REMARK 4.2. If $F^\dagger = F \cdot [(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}), v^2]$, then an isomorphism $C_{F^\dagger} \to C_F$ is given by $(x, y) \to ((ax + b)/(cx + d), v^{-1}(cx + d)^{-g-1}y)$.

By Proposition 4.1, finding small-height models over k of hyperelliptic curves C/k with $\mathrm{Aut}(C_{\overline{k}}) = \{1, \iota\}$ is equivalent to finding small elements of $\mathrm{GL}_2(k) \times k^*$-orbits of binary forms of even degree $\geqslant 6$. Lemma 5.6 in § 5.5 will show that the hypothesis $\mathrm{Aut}(C_{\overline{k}}) = \{1, \iota\}$ is satisfied for the curves we deal with, except for one curve for which we do not need a reduction algorithm. If $\mathrm{Aut}(C_{\overline{k}}) \neq \{1, \iota\}$, then $\mathrm{GL}_2(k) \times k^*$-actions may be too restrictive, but by Remark 4.2, they do always give valid twists.

Our goal for the remainder of § 4 is, given a binary form $F \in H_n(k)$, to find a $\mathrm{GL}_2(k) \times k^*$-equivalent form with small coefficients. We start with computing a discriminant-minimal form in § 4.2, followed by discriminant-preserving $\mathrm{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*$-reduction in § 4.3.

4.2. *Reduction of the discriminant*

Given a binary form $F(X, Z) \in k[X, Z]$ of any degree $n \geqslant 3$, we wish to find a $\mathrm{GL}_2(k) \times k^*$-equivalent form with minimal discriminant. First we recall that the discriminant of a separable binary form

$$F(X, Z) = \prod_{i=1}^{n} (\gamma_i X - \alpha_i Z) \in k[X, Z]$$

with $\alpha_i, \gamma_i \in \overline{k}$ is

$$\Delta(F) = \prod_{i<j} (\gamma_j \alpha_i - \gamma_i \alpha_j)^2 \in k^*.$$

In terms of the polynomial $f = F(x, 1)$ of degree n or $n - 1$ with leading coefficient c, this is

$$\Delta(F) = \begin{cases} \Delta(f) & \text{if } \deg f = n, \\ c^2 \Delta(f) & \text{if } \deg f = n - 1. \end{cases}$$

Let $g \in \mathbf{Z}$ be given by $n = 2g + 2$ if n is even and $n = 2g + 3$ if n is odd. If n is even and $\geqslant 6$, then F corresponds to a hyperelliptic curve C_F of genus g with

$$\Delta(C_F) = 2^{4g} \Delta(F).$$

If n is odd, then there is no interpretation in terms of hyperelliptic curves and the number g is simply a convenient number in the algorithms and proofs.

The discriminant changes under the action of the group $\mathrm{GL}_2(k) \times k^*$ via

$$\Delta(F \cdot [A, u]) = u^{2(n-1)} \det(A)^{n(n-1)} \Delta(F). \tag{4.1}$$

REMARK 4.3. In case $n = 6$, the Igusa invariants of § 2.2 satisfy $I_{10}(C) = 2^{12}\Delta(C) = 2^{20}\Delta(F)$ and

$$I_j(C_{F \cdot [A,u]}) = u^j \det(A)^{3j} I_j(C_F).$$

Before we describe how to reduce the discriminant globally over a number field, we first describe how to reduce the discriminant at just one prime.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

4.2.1. *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 π be a uniformiser of v and $\mathfrak{m} = \pi R$ the maximal ideal.

We call F *minimal at* v if $v(\Delta(F))$ is minimal among all $\mathrm{GL}_2(k) \times k^*$-equivalent forms with v-integral coefficients.

PROPOSITION 4.4. *Suppose $F \in H_n(k)$ has coefficients in R. Let $g = \lfloor n/2 \rfloor - 1$ be the largest integer smaller than or equal to $(n-2)/2$, so $n \in \{2g+2, 2g+3\}$. Then F is non-minimal at v if and only if we are in one of the following three cases.*

(1) *The polynomial F is not primitive, so $F^\dagger = F \cdot [\mathrm{id}_2, \pi^{-1}]$ is integral and satisfies $v(\Delta(F^\dagger)) < v(\Delta(F))$.*
(2) *The polynomial $(F(x,1) \bmod \mathfrak{m})$ has a $(g+2)$-fold root $\bar{t}$ in the residue field. Moreover,* for some (*equivalently* every) *lift $t \in R$ of $\bar{t}$, the form $F^\dagger = F \cdot [(\begin{smallmatrix} \pi & t \\ 0 & 1 \end{smallmatrix}), \pi^{-(g+2)}] = F(\pi X + tZ, Z)\pi^{-(g+2)}$ is integral and satisfies $v(\Delta(F^\dagger)) < v(\Delta(F))$.*
(3) *The polynomial $(F(x,1) \bmod \mathfrak{m})$ has degree $\leqslant n-(g+2)$. Moreover, the form $F^\dagger = F \cdot [(\begin{smallmatrix} 1 & 0 \\ 0 & \pi \end{smallmatrix}), \pi^{-(g+2)}] = \pi^{-(g+2)} F(X, \pi Z)$ is integral and satisfies $v(\Delta(F^\dagger)) < v(\Delta(F))$.*

Proof. For the 'if' part, note that in each of the three cases, the proposition gives an explicit equivalent form that proves that F is not minimal.

Conversely, suppose that F is non-minimal. Then there exists $[A, u] \in \mathrm{GL}_2(k) \times k^*$ with $F \cdot [A, u]$ integral of smaller discriminant. Write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let T be the subgroup $T = \{[\mu \mathrm{id}_2, \mu^{-n}] : \mu \in k^*\}$ of the centre of $\mathrm{GL}_2(k) \times k^*$, and note that T acts trivially on $H_n(k)$, so without loss of generality A has coprime coefficients in R, so either (i) $c \in R^*$ or $d \in R^*$ or (ii) $c \equiv d \equiv 0 \bmod \pi$ and a or b is in R^*.

Note also that $\mathrm{GL}(R) \times R^*$ preserves integrality and the discriminant, so we use multiplication by $\mathrm{GL}(R)$ on the right to perform elementary column operations over R on A. We get that without loss of generality either (i) $d = 1$, $c = 0$ or (ii) $a = 1$, $b = 0$, $c \equiv d \equiv 0 \bmod \pi$.

Note that in both cases $a \neq 0$ and $c \neq 0$, so with more $\mathrm{GL}(R) \times R^*$-multiplication, we get $a = \pi^k$, $d = \pi^l$, $u = \pi^{-m}$ with $k, l, m \in \mathbf{Z}$, $k, l \geqslant 0$, and by equation (4.1) also

$$2m > n(k+l). \tag{4.2}$$

We start with case (i).

Let $H(X, Z) = F(X + bZ, Z)$ and write $H(X, Z) = \sum_i h_i X^i Z^{n-i}$. Then $F \cdot [A, u] = \pi^{-m} H(\pi^k X, Z)$ is integral, so $v(h_i) \geqslant m - ki$. Together with (4.2), this gives

$$v(h_i) > \left(\frac{n}{2} - i\right)k.$$

In particular, if $k = 0$, then H is integral and non-primitive, hence so is $F(X, Z) = H(X - bZ, Z)$ and we are in case 1.

If $k \geqslant 1$, then for all i, we have $v(h_i) > n/2 - i$, hence $v(h_i) > \lfloor n/2 \rfloor - i = g + 1 - i$, so $v(h_i) \geqslant g + 2 - i$. In particular, the form $F \cdot [(\begin{smallmatrix} \pi & b \\ 0 & 1 \end{smallmatrix}), \pi^{-(g+2)}] = H \cdot [(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}), \pi^{-(g+2)}]$ is integral, and of strictly smaller discriminant than F. This proves that we are in case 2 for *some* lift $t = b$ of a $(g+2)$-fold root $\bar{t} = \bar{b}$. To finish the proof of case 2, we need to prove that for *every* t' satisfying $\overline{t'} = \bar{b}$, the transformation $[(\begin{smallmatrix} \pi & t' \\ 0 & 1 \end{smallmatrix}), \pi^{-(g+2)}]$ also gives an integral equation.

Let $y = (t' - b)/\pi \in \mathcal{O}_k$ and note

$$\begin{pmatrix} \pi & t' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pi & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in \begin{pmatrix} \pi & b \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(R),$$

which proves that we are in case 2 for *every* lift t. This finishes case (i).

Now assume that we are in case (ii). Equation (4.2) gives $m > n/2 \geqslant g+1$.

Write $F = \sum_{i=0}^{n} f_i X^i Z^{n-i}$. We will prove by induction that $v(f_j) \geqslant j + g + 2 - n$ holds for all j, which implies that $F(X, \pi Z)\pi^{-(g+2)}$ is integral, so we are in case 3. Note that the assertion is trivial for $j \leqslant n - g - 2$. Now suppose that it is true for all $j < J$.

Note that $F \cdot [A, u] = \pi^{-m} F(X, cX + dZ)$ is integral, so modulo π^{g+2}, we get $0 \equiv \sum_{i=0}^{n} f_i X^i (cX + dZ)^{n-i} \equiv \sum_{i=J}^{n} f_i X^i (cX + dZ)^{n-i}$. Looking at the coefficient of $X^J Z^{n-J}$, we get $f_J d^{n-J} \equiv 0 \bmod \pi^{g+2}$, so $\pi^{g+2-n+J} \mid f_J$. This finishes the proof. □

We use Proposition 4.4 to create the following reduction algorithm.

ALGORITHM 4.5 (Local reduction).
Input: A binary form $F \in H_n(k) \cap R[X, Y]$ and a prime element $\pi \in R$.
Output: A binary form $F^\dagger$ that is $\mathrm{GL}_2(k) \times k^*$-equivalent and minimal at ord_π.
First let $g = \lfloor n/2 \rfloor - 1$.

1. If $F \bmod \pi R$ is zero, then repeat the algorithm with $F^\dagger = F \cdot [\mathrm{id}_2, \pi^{-1}]$. (This corresponds to case 4.4(1).)
2. If $F(x, 1) \bmod \pi R$ has degree $\leqslant n - (g+2)$, then let $F^\dagger = F(X, \pi Z)\pi^{-(g+2)}$. If $F^\dagger$ is integral, then repeat the algorithm with $F^\dagger$. (This corresponds to case 4.4(3).)
3. Factor $\overline{f} = (f \bmod \pi)$ over the finite $R/\pi R$. If $\overline{f}$ has a root $\overline{t}$ of multiplicity $\geqslant g+2$, then let t be a lift of $\overline{t}$ to R. If $F^\dagger = F(\pi X + tZ, Z)\pi^{-(g+2)}$ is integral, then repeat the algorithm with $F^\dagger$. (This corresponds to case 4.4(2).)
4. Return F.

Proof of correctness of Algorithm 4.5. Every step of the algorithm leaves the model integral, and every iteration reduces $v(\Delta(F))$, so the algorithm terminates. It therefore suffices to prove that the output is not in any of the three cases of Proposition 4.4.

In case 1, the algorithm reduces the discriminant in step 1 and starts over. In case 3, the same happens with step 2, and in case 2, it happens with step 3 because a polynomial of degree $\leqslant 2g+3$ has at most one $(g+2)$-fold root $\overline{t}$. □

In many cases, we can do step 3 as follows without having to think about factoring of polynomials.

LEMMA 4.6. *If π is coprime to $n!$, then step 3 can be replaced by the following.*
$3'$. *Let $f = F(x, 1)$, calculate $\gcd(f, f', f'', \ldots, f^{(g+1)})$ over the finite field $R/\pi R$, and write it as $\sum_{i=0}^{s} a_i x^s$ with $a_s \neq 0$. If $s > 0$, then let t be such that $t \equiv -a_{s-1}/(s a_s) \bmod \pi R$. If $F^\dagger = F(\pi X + tZ, Z)\pi^{-(g+2)}$ is integral, then repeat the algorithm with $F^\dagger$.*

Proof. It suffices to show that if $\overline{f}$ has a root $\overline{t}$ of multiplicity $\geqslant g+2$, then it is equal to $(-a_{s-1}/(s a_s) \bmod \pi R)$.

Let a be a root of exact multiplicity m of $\overline{f}$ over the algebraic closure of $R/\pi R$, that is, we have $\overline{f} = (x-a)^m g(x)$ with $g(a) \neq 0$. Then the ith derivative $\overline{f}^{(i)}$ for $i \leqslant m$ is

$$\frac{m!}{(m-i)!}(x-a)^{m-i} g(x) \quad \text{modulo} \quad (x-a)^{m-i+1}.$$

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

In particular, $(x-a)$ is a factor of $\gcd(\overline{f}, \overline{f}', \ldots, \overline{f}^{(m-1)})$, but not of $\overline{f}^{(m)}$. Here we use that $m!$ is coprime to π.

It follows that only the (unique) root of multiplicity $\geqslant g+2$ appears in $\gcd(\overline{f}, \overline{f}', \ldots, \overline{f}^{(g+1)})$, that is, we get $\overline{f} = a_s(x-\overline{t})^s$, hence $a_{s-1} = -s\overline{t}a_s$, so $\overline{t} = -a_{s-1}/(sa_s)$. □

4.2.2. *Global reduction of the discriminant.* Now let us get back to the case where k is a number field with ring of integers $\mathcal{O}_k$. We prefer to have a binary form F where $v(\Delta(F))$ is minimal for all discrete valuations v of k.

If k has class number one, then such a form exists. Indeed, if we take π in Algorithm 4.5 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. See § 4.2.3 for what to do if the class group is non-trivial.

To be able to use our local reduction algorithm one prime at a time, we need to know the valuations v for which $v(\Delta(F))$ is non-minimal. The most straightforward method is to factor $\Delta(F)$. However, factorisation is computationally hard, so we will give some tricks for trying to avoid factorisation below. We needed to use a combination of sophisticated factorisation software and the tricks below for creating our tables. Indeed, on the one hand, without the tricks below, even the state-of-the-art factorisation software left us unable to reduce a couple of the curves. On the other hand, when just using the tricks below and the built-in factorisation functionality of pari-gp [**24**] (through Sage [**29**]), there are some curves that we were still unable to reduce. Only the combination of factoring software and the tricks below allowed us to complete the table.

For serious factoring, we combined the built-in implementation of Pollard's rho method and the elliptic curve method of Magma [**2**], the GMP-ECM implementation of the elliptic curve method [**41**], and the CADO-NFS implementation of the number field sieve [**11**].

The method for avoiding factorisation is based on the following fact.

PROPOSITION 4.7. *Let $\mathfrak{a} = \pi\mathcal{O}_k$ be any (possibly non-prime) principal ideal in a number field k. Modify Algorithm 4.5 as follows.*

(1) *Whenever testing whether an element b of $\mathcal{O}_k$ is zero modulo $\pi^j\mathcal{O}_k = \mathfrak{a}^j$ or whether an element $b/\pi^j \in k$ is integral (in Steps 1, 2, and 3), compute $\mathfrak{d}_i = \gcd(b\mathcal{O}_k, \mathfrak{a}^i)$ for $i = 1, \ldots j-1$. If there exists an i with $\mathfrak{d}_i \notin \{\mathfrak{a}^{i-1}, \mathfrak{a}^i\}$, then for the smallest such i output the non-trivial factor $\mathfrak{d}_i/\mathfrak{a}^{i-1}$ of $\mathfrak{a}$.*
(2) *Replace step 3 with step 3′ of Lemma 4.6 regardless of whether π is coprime to $n!$. Compute gcds of polynomials in $\mathcal{O}_k/\mathfrak{a}$ using Euclid's algorithm. For each division with remainder by a polynomial g, first compute the gcd of the leading coefficient of g with $\mathfrak{a}$ as in item 1.*

Then all steps of Algorithm 4.5 are polynomial-time computable and the output is either a polynomial $F^\dagger$ equivalent to F with $\Delta(F^\dagger) \mid \Delta(F)$ or a non-trivial factor of $\mathfrak{a}$. Moreover, if $\mathfrak{a}$ is square-free and coprime to $n!$ and the algorithm runs without returning a factor of $\mathfrak{a}$, then the output polynomial $F^\dagger$ is minimal at all primes dividing $\mathfrak{a}$.

Proof. Since the leading coefficient of a polynomial over $\mathcal{O}_k$ is either invertible modulo $\mathfrak{a}$ or has a non-trivial factor in common with $\mathfrak{a}$, division with remainder either works or provides such a non-trivial factor. This proves the first assertion in Proposition 4.7.

Next suppose that $\mathfrak{a}$ is square-free and coprime to $n!$ and let F be as in Algorithm 4.5. If F is minimal at all primes dividing $\mathfrak{a}$, then we are done. If there is an $i \in \{1, 2, 3\}$ such that all primes dividing $\mathfrak{a}$ are as in Proposition 4.4(1), then the corresponding step (1, 3′ or 2) in Algorithm 4.5 reduces the discriminant of F and we start over with a new F.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

So without loss of generality, there are $i \in \{1, 2, 3\}$ and primes $\mathfrak{p}, \mathfrak{q} \mid \mathfrak{a}$ such that $\mathfrak{p}$ is as in Proposition 4.4(1) and $\mathfrak{q}$ is not. But then the corresponding step (1, $3'$ or 2) in Algorithm 4.5 returns a non-trivial factor of $\mathfrak{a}$. $\square$

Based on Proposition 4.7, we get the following algorithm that tries to minimise the amount of factoring.

ALGORITHM 4.8.
Input: A binary form $F \in H_n(k)$ for a number field k of class number one.
Output: A binary form $F^\dagger$ that is integral, is $\mathrm{GL}_2(k) \times k^*$-equivalent to F, and has minimal discriminant.

1. Let $\mathfrak{a} = \Delta(F)\mathcal{O}_k$ and $A = \{\mathfrak{a}\}$.
2. If the unit ideal is in A, remove it from A. If A is empty, return F.
3. For each $\mathfrak{a} \in A$, test if $\mathfrak{a}$ is a perfect power and replace it by its highest-power root.
4. Fix $B \in \mathbf{Z}$ with $B \geqslant n$ and apply trial division up to B to each element of A to find a small prime factor $\mathfrak{p} = (\pi)$. If no prime is found, go to Step 5. If a prime is found, then reduce the form locally using Algorithm 4.5 on $\mathfrak{p}$, remove all factors $\mathfrak{p}$ from all elements of A, and go to step 2.
5. For each $\mathfrak{a} \in A$, run Algorithm 4.5 on $\mathfrak{a}$ with the modifications of Proposition 4.7.
   (a) If it returns a non-trivial factor $\mathfrak{b}$ of $\mathfrak{a}$, then replace $\mathfrak{a}$ in A by $\mathfrak{b}$ and $\mathfrak{a}/\mathfrak{b}$ and go to step 3.
   (b) If it returns a binary form $F^\dagger \neq F$, then replace all $\mathfrak{a} \in A$ by $\mathfrak{a} + \Delta(F^\dagger)\mathcal{O}_k$, replace F by $F^\dagger$, and go to step 2.
   (c) If it returns F, then go to the next $\mathfrak{a}$ in A.
6. Go to step 4 with a strictly larger trial division bound B (or more sophisticated factoring methods).

Let us first show that this algorithm terminates in finite time and returns a minimal form. For minimality of the form, note that at every step in the algorithm, all primes at which F is non-minimal divide some element of A, and the algorithm terminates only if A is empty. To see that the algorithm ends, note that the norm $N = N_{k/\mathbf{Q}}(\Delta(F))$ never increases, while at every iteration either $N \in \mathbf{Z}$ decreases or $B \in \mathbf{Z}$ increases, so at some point we have $B > N$ after which a repeated application of step 4 finishes the algorithm.

REMARK 4.9. There is no way to completely avoid factoring. Indeed, if one can compute the twist-minimal model of the hyperelliptic curve

$$y^2 = N^2x^6 + x + 1 \quad \text{where } N = pq^2 \text{ with } p, q \text{ prime},$$

then one can also factor the integer $N = pq^2$.

REMARK 4.10. In the genus-two case (that is, $n = 6$) we can replace $\Delta(F)\mathcal{O}_k$ in the algorithm by the ideal $\gcd(I_2(C_F), I_4(C_F), I_6(C_F), \Delta(F))$, where I_2, I_4, I_6 are the Igusa–Clebsch invariants from § 2. Indeed, we have that I_2, I_4, and I_6 satisfy the transformation formula of Remark 4.3, so all primes at which the model is non-minimal divide this gcd. The advantage is that this ideal is smaller than $\Delta(F)$, which speeds up the algorithm.

REMARK 4.11. All of the above works if one wants a hyperelliptic curve model that is isomorphic over $\overline{k}$, but not necessarily over k. To get a minimal model of C_F that is isomorphic over k, one could do the following. First reduce F as above, and do some bookkeeping to find not only a twist-reduced model $C_{F^\dagger}/k$, but also $[A, u] \in \mathrm{GL}_2(k) \times k^*$ with $F^\dagger = F \cdot [A, u]$ and some information on the factorisation of u. Then all one needs is a minimal element

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

$v \in u(k^*)^2 \cap \mathcal{O}_k$, because $C_{vF^\dagger}$ is then a minimal model. Such an element v exists if k has class number one, and can then be found easily if one is able to factor $u\mathcal{O}_k$.

4.2.3. *Class number* > 1. Everything in § 4.2.2 was under the assumption that k had class number one, and hence a global minimal form exists. If k does not have class number one, then this is not always possible. Indeed, let F_v be a $\mathrm{GL}_2(k) \times k^*$-equivalent binary form with $v(\Delta(F_v))$ minimal, and let $\Delta_{\min}$ be the ideal with $v(\Delta_{\min}) = v(\Delta(F_v))$ for all v. If $\Delta_{\min}$ is not principal, then there is no form with that discriminant. In fact, if F is any form, and there exists a globally minimal equivalent form $F_{\min}$ with $\Delta(F_{\min}) = \Delta_{\min}$, then the ideal $\sqrt[\gcd(n,2)(n-1)]{\Delta(F)/\Delta_{\min}}$ is a principal ideal.

So instead of a globally reduced form, we look for an almost-reduced form. Let S be a (small) set of (small) prime ideals that generate the class group. It is easy to change the methods above into an algorithm that finds a form that is reduced outside S. We now give the details of the algorithm that we used for this, which also makes the form reasonably simple at the primes of S.

Let T be any set of prime ideals that generate the class group and $\mathfrak{a}$ an ideal supported outside T. In Algorithm 4.5, to reduce at $\mathfrak{a}$ and stay reduced outside of T, we do the following. Take $\pi_u \in \mathfrak{a}$ and $\pi_l^{-1} \in \mathfrak{a}^{-1}$ such that $\pi_u/\mathfrak{a}$ and $\mathfrak{a}/\pi_l$ are supported on T. Then in Algorithm 4.5 replace the formulas for $F^\dagger$ in cases 1, 2, 3 with

$$\pi_l^{-1} F(X, Z), \quad F(X/\pi_l, Z)\pi_u^{n-(g+2)} \quad \text{and} \quad F(\pi_u X + tZ, Z)\pi_l^{-(g+2)} \tag{4.3}$$

respectively, where we make sure that t is divisible by $\pi_u/\mathfrak{a}$. Note that this gives integral forms, and worsens the discriminant only at T.

Our algorithm starts by taking T disjoint from S. First reduce at all primes of S, possibly worsening at T. Then take $T = S$ and reduce outside of S, possibly worsening at S.

Since we had a minimal form at the primes of S, the only non-minimality of the form at this stage is what was introduced by (4.3). In particular, it can be removed by transformations of the form $a^{-1}b^g F(b^{-1}X, Z)$. So we take $a, b \in \mathcal{O}_k$ with $a^2 b^{n-2g}$ of maximal norm such that $a^{-1}b^g F(b^{-1}X, Z)$ is integral. Note that no hard factoring is required in finding a and b since they are supported on the set of primes S.

We did the above for the field $K = \mathbf{Q}[X]/(X^4 + 46X^2 + 257)$ (denoted $[17, 46, 257]$ in [**17**]). We used $S = \{\mathfrak{p}\}$ for a (non-principal) prime $\mathfrak{p}$ of norm 2 in the quadratic field $K_0^r = \mathbf{Q}(\sqrt{257})$, which has class group of order 3.

4.3. *Reduction of coefficients: Stoll–Cremona reduction*

At this point, we have an integral form $F \in H_n(k)$ where the norm $N(\Delta(F))$ 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 $(\mathrm{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*)$.

We use a notion of 'reduced' based on Stoll and Cremona [**30**]. We do not prove that this notion of 'reduced' yields small coefficients, but in practice it does.

4.3.1. *The case* $k = \mathbf{Q}$. Stoll and Cremona [**30**, Definition 4.3] give a definition of *reduced* for binary forms of degree $\geqslant 3$ over $\mathbf{Q}$ under the action of $\mathrm{SL}_2(\mathbf{Z}) \times 1$, which we will summarise here.

Recall that $H_n(k)$ is the set of separable binary forms $F(X, Y)$ of degree n. Let $\mathcal{H} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$ be the complex upper half plane. We turn the standard left $\mathrm{GL}_2(\mathbf{R})^+$-action on $\mathcal{H}$ into a right action by

$$z \cdot A = A^{-1}(z) = \frac{dz - b}{-cz + a}$$

for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

The idea behind [30] is to use an $\mathrm{SL}_2(\mathbf{R})$-covariant map $z : H_n(\mathbf{R}) \to \mathcal{H}$. In $\mathcal{H}$, there is a notion of $\mathrm{SL}_2(\mathbf{Z})$-reduction, and we just pull back that notion to $H_n(\mathbf{Q})$ via z. In other words, we have the following definition.

DEFINITION 4.12. We call $F \in H_n(\mathbf{Q})$ *reduced for* $\mathrm{SL}_2(\mathbf{Z})$ if $z(F) = z = x + iy$ satisfies

(R) $|x| \leqslant \frac{1}{2}$, and

(M) $|z| \geqslant 1$.

This gives rise to the following algorithm.

ALGORITHM 4.13. (Stoll–Cremona reduction)

Input: $F \in H_n(\mathbf{Q})$

Output: an $\mathrm{SL}_2(\mathbf{Z})$-reduced element of the orbit $F \cdot (\mathrm{SL}_2(\mathbf{Z}) \times 1)$.

1. Let m be the integer nearest to $x = \mathrm{Re}(z(F))$ and let $F \leftarrow F \cdot \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) = F(X + mZ, Z)$. This replaces $z(F)$ with $\left(\begin{smallmatrix} 1 & -m \\ 0 & 1 \end{smallmatrix}\right) z(F) = z(F) - m$, which satisfies (R) above.
2. If $|z(F)| < 1$, then let $F \leftarrow F \cdot \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = F(Z, -X)$ and go back to step 1. This replaces $z(F)$ with $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) z(F) = -1/z(F)$, which satisfies (M) above.

Stoll and Cremona [30, after Proposition 4.4] outline how one could extend the definition of reduced to binary forms over any number field k under the action of $\mathrm{SL}_2(\mathcal{O}_k) \times 1$. We work out the details in the case of a totally real field, and give an implementation and an improvement.

To generalise the algorithm, we need two ingredients: a covariant map, and a reduction algorithm on the codomain of that map.

4.3.2. *The covariant for totally real fields.* Let k be a totally real number field of degree d and let $\phi_1, \ldots, \phi_d$ be the d embeddings $k \to \mathbf{R}$. This induces embeddings $k \to \mathbf{R}^d$, $H_n(k) \to H_n(\mathbf{R})^d$ and $\mathrm{SL}_2(k) \to \mathrm{SL}_2(\mathbf{R})^d$, which we will use implicitly. Composing with the covariant map z on every component, we get a map $H_n(k) \to \mathcal{H}^d$, which is $\mathrm{SL}_2(k)$-covariant and which we also denote by z.

REMARK 4.14. The quotient space $\mathrm{SL}_2(\mathcal{O}_k)\backslash\mathcal{H}^d$ is coincidentally the Hilbert moduli space of polarised abelian d-folds with real multiplication by $\mathcal{O}_k$ and a certain polarisation type.

In fact, we can do slightly better. We identify $\mathcal{H}$ with $(\mathbf{C} \setminus \mathbf{R})$ modulo complex conjugation, that is, we identify $z \in -\mathcal{H}$ with $\overline{z} \in \mathcal{H}$. Then the $\mathrm{SL}_2(\mathbf{R})$-action on $\mathcal{H}$ extends to a $\mathrm{GL}_2(\mathbf{R})$-action also given by $z \cdot A = A^{-1}(z) = (dz - b)/(-cz + a)$ (up to complex conjugation). The covariant z of [30] then turns out to also be $\mathrm{GL}_2(\mathbf{R})$-covariant. In particular, we get a map

$$z : H_n(k) \to \mathcal{H}^d,$$

which is $\mathrm{GL}_2(k)$-covariant.

4.3.3. *Reduction for* $\mathrm{GL}_2(\mathcal{O}_k)$ *in* $\mathcal{H}^d$. Let $N : \mathbf{R}^d \to \mathbf{R} : (x_m)_m \mapsto \prod_m x_m$, define $\mathrm{Re}, \mathrm{Im}, |\cdot| : \mathbf{C}^d \to \mathbf{R}^d$ component-wise and let $\log : \mathbf{R}^d \to \mathbf{R}^d : (x_m)_m \mapsto (\log |x_m|)_m$.

DEFINITION 4.15. We call $z \in \mathcal{H}^d$ *reduced* for $\mathrm{GL}_2(\mathcal{O}_k)$ if it satisfies the following conditions:

(R) the point $\mathrm{Re}(z) \in \mathbf{R}^d$ is in some fixed chosen fundamental hyper-parallelogram for addition by $\mathcal{O}_k$;

(I) the point $\log(\mathrm{Im}(z)) \in \mathbf{R}^d$ is in some fixed chosen fundamental domain for addition by $\log(\mathcal{O}_k^*)$; and

(M) the norm $N(\mathrm{Im}(z))$ is maximal for the $\mathrm{GL}_2(\mathcal{O}_k)$-orbit $\mathrm{GL}_2(\mathcal{O}_k)z$.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

Let us first see how this is an analogue of Definition 4.12. Note that in the case $k = \mathbf{Q}$, we can choose the hyper-parallelogram $[-\frac{1}{2}, \frac{1}{2}]$, and then conditions 4.12(R) and 4.15(R) coincide and condition 4.15(I) is empty. It is well known that under condition 4.12(R), we have 4.15(M) if and only if 4.12(M).

REMARK 4.16. Definition 4.15 is also closely related to a standard definition of *reduced* for the action of $\mathrm{SL}_2(\mathcal{O}_k)$ on $\mathcal{H}^d$. Indeed, if k has class number one and we replace $\mathrm{GL}_2(\mathcal{O}_k)$ with $\mathrm{SL}_2(\mathcal{O}_k)$ and $\mathcal{O}_k^*$ with $(\mathcal{O}_k^*)^2$, then we get a fundamental domain of [**37**]. One could use the standard fundamental domain from [**37**] in general, but since we had only one case of class number > 1, we simply used (R), (I) and (M) for that field as well.

The above gives rise to a notion of reduction for $\mathrm{GL}_2(\mathcal{O}_k) \times 1$ on $H_n(k)$. We then get the following sketch of a reduction algorithm.

ALGORITHM SKETCH 4.17. (Reduction for $\mathrm{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*$)
Input: $F \in H_n(k)$.
Output: $F^\dagger \in H_n(k)$ that is $\mathrm{GL}_2(\mathcal{O}_k) \times \mathcal{O}_k^*$-equivalent to F and $\mathrm{GL}_2(\mathcal{O}_k)$-reduced.

1. Compute a fundamental domain $\mathcal{F}$ for addition by $\mathcal{O}_k$ in $\mathbf{R}^d$.
2. Compute a fundamental domain $\mathcal{G}$ for addition by $\log(\mathcal{O}_k^*)$ in $\mathbf{R}^d$.
3. Take $u \in \mathcal{O}_k^*$ such that $\log \mathrm{Im}(z(F)) - (\log|\phi_m(u)|)_m \in \mathcal{G}$ and replace F by
$$F \cdot \left[\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}, 1\right] = F(uX, Z).$$
This replaces $z(F)$ by $u^{-1}z(F)$, and hence makes sure F satisfies (I) and preserves $N(\mathrm{Im}(z))$.
4. Take $b \in \mathcal{O}_k$ such that $\mathrm{Re}(z(F)) - b \in \mathcal{F}$ and replace F by
$$F \cdot \left[\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, 1\right] = F(X + bZ, Z).$$
This replaces $z(F)$ by $z(F) - b$, and hence makes sure F satisfies (R) and preserves (I) and $N(\mathrm{Im}(z))$.
5. Try to find a matrix M such that $N(\mathrm{Im}(Mz)) > N(\mathrm{Im}(z))$. If no such matrix exists, go to step 6. If such a matrix exists, replace F by $F \cdot [M^{-1}, 1]$ and go to step 3.
6. Try to find $u \in \mathcal{O}_k^*$ such that the maximum of the heights of the coefficients of uF is minimal and return $F[1_2, u] = uF$.

Bases of $\mathcal{O}_K$ and $\mathcal{O}_K^*$ are easy to compute using a number theory package like Magma [**2**] or Pari [**24**], hence so are $\mathcal{F}$ and $\mathcal{G}$. Numerical approximation of the covariant $z : H_n(\mathbf{R}) \to \mathcal{H}$ of [**30**] is available in Magma as a standard function (called `Covariant`). So the only steps with missing details are 5 and 6.

For step 5, note first that for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{R})$ and $z \in \mathcal{H}$ we have $\mathrm{Im}(Az) = |\det A| \cdot |cz + d|^{-2} \cdot \mathrm{Im}(z)$. In particular, for $A \in \mathrm{GL}_2(\mathcal{O}_k)$ and $z \in \mathcal{H}^g$, we have $N(\mathrm{Im}(Az)) = N(|cz + d|)^{-2} N(\mathrm{Im}(z))$ so the condition in step 5 is equivalent to $N(|cz + d|) < 1$. Given $c, d \in \mathcal{O}_k$, it is easy to find $a, b \in \mathcal{O}_k$ with $ad - bc \in \mathcal{O}_k^*$ if they exist, so for step 5, we need only to find c, d.

A fast first attempt at trying to find c, d for step 5 is to consider the lattice $\{cz + d \in \mathbf{C}^g : c, d \in \mathcal{O}_k\}$ and compute an LLL-reduced $\mathbf{Z}$-basis. If the first vector $cz + d$ of the LLL-reduced basis satisfies $N(|cz + d|) < 1$, then use these c and d. Note that this always works if the covolume $N(\mathrm{Im}(z))$ of the lattice is sufficiently small.

If the first attempt for step 5 fails, then we use an exhaustive search as follows. Note first of all that we only need to consider pairs (c, d) up to multiplication by $\mathcal{O}_k^*$. Note

$$N(|cz+d|)^2 \geqslant N(|c\mathrm{Re}(z)+d|)^2 + |N(c)|^2 \cdot N(|\mathrm{Im}(z)|)^2,$$

so the c, d that we need satisfy $|N(c)| < N(|\mathrm{Im}(z)|)^{-1}$ and $c \neq 0$. We list all such c up to multiplication by units by listing all ideals of norm $< N(|\mathrm{Im}(z)|)^{-1}$. Next, the numbers d that we need satisfy

$$\sqrt{1-|N(c)|^2 \cdot N(|\mathrm{Im}(z)|)^2} > N(|c\mathrm{Re}(z)+d|) \geqslant N(|c\mathrm{Re}(z)|) + \sum_i \left(\prod_{j \neq i} |\phi_j(c)\mathrm{Re}(z_j)| \right) |\phi_i(d)|,$$

which yields a bounded box in $\mathbf{R}^d$ containing d. So we list all $d \in \mathcal{O}_k$ in that box. This exhaustive search is guaranteed to find all relevant c, d, after which we choose the pair c, d with minimal $N(|cz+d|)$. Since we have the minimal $N(|cz+d|)$, we also have the maximal $N(|\mathrm{Im}(Az)|)$ for the whole orbit, hence the algorithm finishes after one more iteration of steps 3, 4, 6. The exhaustive search for c, d can however be very slow, and it is certainly very slow if $N(|\mathrm{Im}(z)|)$ is small.

We implemented Algorithm 4.17 with this method for step 5 (first try the fast attempt, and if it fails use the exhaustive search) and tested it for quadratic fields of small discriminant. In practice, this always was fast, taking less than a second to run. An explanation for this is that if $N(|\mathrm{Im}(z)|)$ is small, then the fast LLL-attempt works, and if the LLL-attempt fails, then $N(|\mathrm{Im}(z)|)$ is large and hence the exhaustive search is fast.

For step 6, write $F = \sum_{i=1}^n f_i X^i Z^{n-i}$ and consider the point $p = (\log(f_i))_i \in \mathbf{R}^{(n+1)d}$. The goal is to find v in the lattice $\{(\log(u), \ldots, \log(u)) \in \mathbf{R}^{(n+1)d} : u \in \mathcal{O}_k^*\}$ of rank $d-1$ that is closest to p for the maximum-norm $|\cdot|_\infty$. In the case $d = 2$, this lattice has rank 1, and finding a nearest vector in a lattice of rank 1 is easy. Indeed, write $v = kb$ for a basis element b and $k \in \mathbf{Z}$ (in our case $b = (\log(\epsilon), \ldots, \log(\epsilon))$ for a fundamental unit ϵ) and note that the norm $N(k) = |p - kb|_\infty$ is convex as a function of k by the triangle inequality. By convexity, every local minimum is a global minimum, so we walk from $k = 0$ towards a local minimum k and then return $\epsilon^{-k} F$.

We implemented this algorithm in Sage and made it available online at [**36**].

REMARK 4.18. If one wants models of hyperelliptic curves that are isomorphic over k, then simply replace $\mathcal{O}_k^*$ with $(\mathcal{O}_k^*)^2$ in step 6.

5. *Results and tables*

In this section, we give our tables. The most important columns (the first and last) of Tables 1a, 1b and 2b are explained already in Theorem 1.1. To explain the rest, we first need to explain what a CM-type is.

5.1. *CM-types and reflex fields*

A *CM-field* is a totally imaginary quadratic extension K of a totally real number field K_0. Note that K has a unique *complex conjugation* automorphism, which is the generator $\rho = \bar{\cdot}$ of $\mathrm{Gal}(K/K_0)$. Let k be a field of characteristic zero. For $\phi : K \to \overline{k}$, write $\overline{\phi} = \phi \circ \rho$. A *CM-type* of K with values in $\overline{k}$ is a set Φ of g embeddings $K \to \overline{k}$ such that $\Phi \cup \overline{\Phi}$ is exactly the set of all $2g$ embeddings.

Let A be an abelian variety of dimension g over a field k of characteristic 0 and suppose that $K \cong \mathrm{End}(A_{\overline{k}})$, where K is a number field of degree $2g$. Choose an isomorphism

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

$i : K \to \mathrm{End}(A_{\overline{k}})$ and note that i induces an action of K on the tangent space of $A_{\overline{k}}$ at zero, which makes this tangent space into a g-dimensional $\overline{k}$-linear representation R of K. By complex multiplication theory [28] the field K is a CM-field and there is a CM-type Φ such that the representation R is isomorphic to a direct sum of the g elements of Φ. We say that (A, i) is *of type* Φ and that Φ is *the CM-type of* (A, i).

The type norm of Φ is the multiplicative map

$$N_\Phi : K \to \overline{k} : \alpha \to \prod_{\phi \in \Phi} \phi(\alpha),$$

which satisfies $N_\Phi(\alpha) = \det R(\alpha)$ if (A, i) is of type Φ. The *reflex field* $K^r \subset \overline{k}$ is defined to be the field generated over $\mathbf{Q}$ by the set of type norms $\{N_\Phi(\alpha) \mid \alpha \in K\}$. 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 involves abelian extension of K^r rather than K.

Note that the reflex field of the CM-type of (A, i) depends only on A, since composition of Φ with elements of $\mathrm{Aut}(K)$ does not change N_Φ.

5.2. *The case distinctions*

There are three possibilities for the Galois group of a quartic CM-field [28, Example 8.4(2)]:

(1) $K/\mathbf{Q}$ is Galois with cyclic Galois group C_4 of order 4;
(2) $K/\mathbf{Q}$ is not normal, and its normal closure has dihedral Galois group D_4 of order 8;
(3) $K/\mathbf{Q}$ is Galois over $\mathbf{Q}$ 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 following the Echidna database [17], our tables will be partitioned into cases 1 and 2.

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^r. We distinguish whether the curves are defined over:

(a) $\mathbf{Q}$;
(b) K_0^{r}, but not $\mathbf{Q}$;
(c) K^{r}, but not K_0^{r}.

The motivation for this article was that case 2a is not possible, and during our construction of our list we found no examples for case 1c. Hence we conjecture that case 1c is empty and we constructed four tables corresponding to the four cases 1a, 1b, 2b, and 2c. Case 1a corresponds to Van Wamelen [38].

5.3. *Legend for the tables*

In case 1, we have $K^r \cong K$ and $\mathrm{Aut}(K) = C_4$, so every abelian variety with CM by $\mathcal{O}_K$ is of all four CM-types, we therefore give K and f, but not Φ or K^r.

In case 2, we have two $\mathrm{Aut}(K)$-orbits of CM-types, and, given A, only one of these orbits corresponds to A. We specify the correct CM-type orbit by specifying its reflex field K^r as an extension of the quadratic field $K_0^r = \mathbf{Q}(a)$.

A quartic CM-field K is given up to isomorphism by a unique triple $[D, A, B]$ as follows, following the Echidna database [17]. Write $K = K_0(\sqrt{r})$ for some real quadratic field K_0 and some totally negative $r \in K_0$. Without loss of generality, we take $r \in \mathcal{O}_{K_0}$ with $A = -\mathrm{tr}_{K_0/\mathbf{Q}}(r) \in \mathbf{Z}_{>0}$ *minimal*. Then let $B = N_{K_0/\mathbf{Q}}(r) \in \mathbf{Z}_{>0}$ and assume B is minimal for this A. Finally, let $D = \Delta_{K_0/\mathbf{Q}}$. We use the triple $[D, A, B]$ to represent the isomorphism class of K, and note $K \cong \mathbf{Q}[X]/(X^4 + AX^2 + B)$.

Let us briefly state what the notation in the table means.

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

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

a A root of $X^2 + \epsilon X + (D^r - \epsilon)/4$ with $\epsilon \in \{0, 1\}$ congruent to D^r modulo 4. We have $\mathbf{Z}[a] = \mathcal{O}_{K_0^r}$. In case 1, the field K^r is uniquely determined as a subset of $\overline{k}$ by $K^r \cong K$. In case 2, there are two quadratic extensions $K^r/\mathbf{Q}(a)$ that satisfy $K^r \cong \mathbf{Q}[X]/(X^4 + AX^2 + B)$, and they are conjugate over $\mathbf{Q}$. The expression of a in terms of α (in the column 'a') tells us which of these extensions is $K^r = \mathbf{Q}(\alpha)$.

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

$\Delta(C)$ The discriminant of the given model $y^2 = f(x)$ of C.

Δ_{stable} The minimal discriminant of all models of C over $\overline{\mathbf{Q}}$ of the form $y^2 + h(x)y = g(x)$ with coefficients in $\overline{\mathbf{Z}}$.

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

$(xa + y)_n^e$ The eth power of the principal $\mathbf{Z}[a]$-ideal of norm n generated by $xa + y$. This notation is used in the discriminant and obstruction columns.

5.4. *Statement and proof of results regarding the table*

We give the following more detailed version of Theorem 1.1.

THEOREM 5.1. *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 $\overline{\mathbf{Q}}$-isomorphism classes of curves satisfying* $\mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) \cong \mathcal{O}_K$.
   (b) *In Tables 1b and 2b, the given curves and their quadratic conjugates over $\mathbf{Q}$ are exactly all $\overline{\mathbf{Q}}$-isomorphism classes of curves satisfying* $\mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) \cong \mathcal{O}_K$.
   (c) *In Tables 1a and 1b, the curves have CM-type Φ for every CM-type Φ of K.*
   (d) *In Table 2b, the given curve has the given CM-type Φ, and its quadratic conjugate has CM-type Φ' where $\Phi' \notin \{\Phi, \overline{\Phi}\}$.*

(2) *The curves in Tables 1a and 1b, and 2b are all defined over K_0^r, and the entries $\Delta(C)/\Delta_{\text{stable}}$ and Δ_{stable} are as explained in the legend above.*

(3) *In Tables 1b and 2b, the discriminant $\Delta(C)$ is minimal (as defined in § 4.2.1) among all $\overline{\mathbf{Q}}$-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 $g(x) \in \mathbf{Z}[x]$.*

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

(5) *For every row of Table 2c, the number in the final column is the number of curves over* $\overline{\mathbf{Q}}$ *with* $\mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) \cong \mathcal{O}_K$ *of type* Φ *up to isomorphism over* $\overline{\mathbf{Q}}$*. 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 [**38**] and proven correct by Van Wamelen [**39**] and Bisson and Streng [**1**].

Proof. We compute the isomorphism class of the reflex field as follows. The reflex field is again a non-biquadratic quartic CM-field. In fact, one can compute that it is isomorphic to $\mathbf{Q}[X]/(X^4 + 2AX^2 + (A^2 - 4B))$. 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 $K_0^r \cong \mathbf{Q}(\sqrt{D'}) \cong \mathbf{Q}(\sqrt{B})$.

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 [**19**], these computations even prove that the Igusa invariants themselves are correct, including the ones for Table 2c, which are not listed. We used the Igusa invariants to compute the curves and obstructions with Mestre's algorithm, which proves that the curves and obstructions are correct. In case 1, all CM-types are in the same orbit for $\mathrm{Aut}(K)$, 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 [**28**, Theorem 1(ii) in § 13.1]. Proposition 4.4 and our reduction algorithm prove that the discriminant is minimal. The stable discriminant is computed directly from Igusa's arithmetic invariants [**16**]. The set of obstructions in Table 2c is non-empty, hence there is no model over K_0^r. It remains to prove that there is a model over K^r, which can be verified by checking that the obstructions are inert or ramified in K^r/K_0^r, but which also follows from Theorem 5.3 below. □

5.5. *Theoretical results*

The following known result is the reason why Van Wamelen's table [**38**] did not contain any curves with CM by non-Galois CM-fields and why we have no Table 2a.

PROPOSITION 5.2. *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_0^r*.*

Proof. This is a special case of [**26**, Proposition 5.17(5)]. □

While the result above gives a lower bound for the field of definition and the field of moduli, the following result gives an upper bound.

THEOREM 5.3. *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 $K^{\mathrm{r}}k_0$ *is a field of definition and we have* $[K^{\mathrm{r}}k_0 : K_0^{\mathrm{r}}k_0] = 2$*.*

Proof. The first statement is a special case of the main theorem of [**22**]. Alternatively, it is Theorem 11 on p. 524 of [**25**], combined with Proposition 2(3.4) on p. 514, with the line below Proposition 7 on p. 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 [**33**, Lemma 2.6]. □

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

COROLLARY 5.4. *In the notation of Theorem 5.3, the following are equivalent:*

(1) K^{r} *is a field of definition;*

(2) K^{r} *contains the field of moduli* k_0*;*

(3) K_0^{r} *contains the field of moduli* k_0.

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

(4) K_0^{r} *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 5.3 states that 1 holds and that $[K^{\mathrm{r}} : K_0^{\mathrm{r}} k_0] = 2$ holds, so 3 also holds.

In the non-Galois case, Proposition 5.2 gives $4 \Leftrightarrow 3$. $\square$

REMARK 5.5. 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 5.4 are equivalent to that quotient being trivial.

The following lemma justifies that we worked under the assumption $\mathrm{Aut}(C_{\overline{k}}) = \{1, \iota\}$ in this paper.

LEMMA 5.6. *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* § 5.2. *Then either $\mathcal{O} = \mathbf{Z}[\zeta_5]$ and C is isomorphic over $\overline{k}$ to the curve $y^2 = x^5 - 1$ (in particular we already know a small model) or we have $\mathrm{Aut}(C_{\overline{k}}) = \{1, \iota\}$.*

Proof. The automorphisms of C correspond to automorphisms of the principally polarised abelian variety $J(C)$, which are roots of unity in $\mathcal{O} = \mathrm{End}(J(C)_{\overline{k}})$. The only order in cases 1 and 2 with roots of unity is $\mathbf{Z}[\zeta_5]$, and since it has class number one, there is only one curve with CM by that ring 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. $\square$

5.6. *Completeness*

As for completeness, our tables contain all fields in the Echidna database satisfying $[k_0 : \mathbf{Q}] \leqslant 2$. In particular, by Corollary 5.4, our list contains all fields for which the curve has a model over K^{r} 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.

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

Table 1a.

DAB	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[5, 5, 5]$	1	$2^8 \cdot 5^5$	$x^5 - 1$
$[5, 10, 20]$	2^{12}	$2^{10} \cdot 5^5$	$4x^5 - 30x^3 + 45x - 22$
	$2^{12} \cdot 11^{12}$	$2^{10} \cdot 5^5$	$8x^6 + 52x^5 - 250x^3 + 321x - 131$
$[5, 65, 845]$	11^{12}	$2^{20} \cdot 5^5 \cdot 13^{10}$	$8x^6 - 112x^5 - 680x^4 + 8440x^3 + 28160x^2 - 55781x + 111804$
	$31^{12} \cdot 41^{12}$	$2^{20} \cdot 5^5 \cdot 13^{10}$	$-9986x^6 + 73293x^5 - 348400x^3 - 118976x - 826072$
$[5, 85, 1445]$	71^{12}	$2^{20} \cdot 5^5 \cdot 17^{10}$	$-73x^6 + 1005x^5 + 14430x^4 - 130240x^3 - 1029840x^2 + 760976x - 2315640$
	$11^{12} \cdot 41^{12} \cdot 61^{12}$	$2^{20} \cdot 5^5 \cdot 17^{10}$	$2160600x^6 - 8866880x^5 + 2656360x^4 - 582800x^3 + 44310170x^2 + 6986711x - 444408$
$[8, 4, 2]$	2^6	2^{15}	$x^5 - 3x^4 - 2x^3 + 6x^2 + 3x - 1$
$[8, 20, 50]$	$2^6 \cdot 7^{12} \cdot 23^{12}$	$2^{15} \cdot 5^{10}$	$-8x^6 - 530x^5 + 160x^4 + 64300x^3 - 265420x^2 - 529x$
	$2^6 \cdot 7^{12} \cdot 17^{12} \cdot 23^{12}$	$2^{15} \cdot 5^{10}$	$4116x^6 + 64582x^5 + 139790x^4 - 923200x^3 + 490750x^2 + 233309x - 9347$
$[13, 13, 13]$	1	$2^{20} \cdot 13^5$	$x^6 - 8x^4 - 8x^3 + 8x^2 + 12x - 8$
$[13, 26, 52]$	$2^{12} \cdot 3^{12} \cdot 23^{12}$	$2^{10} \cdot 13^5$	$-243x^6 - 2223x^5 - 1566x^4 + 19012x^3 + 903x^2 - 19041x - 5882$
	$2^{12} \cdot 3^{12} \cdot 23^{12} \cdot 131^{12}$	$2^{10} \cdot 13^5$	$59499x^6 - 125705x^5 - 801098x^4 + 1067988x^3 + 2452361x^2 + 707297x - 145830$
$[13, 65, 325]$	3^{12}	$2^{20} \cdot 5^{10} \cdot 13^5$	$36x^5 - 1040x^3 + 1560x^2 + 1560x + 1183$
	$3^{12} \cdot 53^{12}$	$2^{20} \cdot 5^{10} \cdot 13^5$	$-1323x^6 - 1161x^5 + 9360x^4 + 9590x^3 - 34755x^2 + 1091x + 32182$
$[29, 29, 29]$	5^{12}	$2^{20} \cdot 29^5$	$43x^6 - 216x^5 + 348x^4 - 348x^2 - 116x$
$[37, 37, 333]$	$3^{12} \cdot 11^{12}$	$2^{20} \cdot 37^5$	$-68x^6 + 57x^5 + 84x^4 - 680x^3 + 72x^2 - 1584x - 4536$
$[53, 53, 53]$	$17^{12} \cdot 29^{12}$	$2^{20} \cdot 53^5$	$-3800x^6 + 15337x^5 + 160303x^4 - 875462x^3 + 896582x^2 - 355411x + 50091$
$[61, 61, 549]$	$3^{24} \cdot 5^{12} \cdot 41^{12}$	$2^{20} \cdot 61^5$	$40824x^6 + 103680x^5 - 67608x^4 - 197944x^3 - 17574x^2 + 41271x + 103615$

TABLE 1B.

DAB	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[5, 15, 45]$	$(2)^{12} \cdot (3)^6$	$(2a+1)_5^{10}$	$-x^6 + (-3a-3)x^5 + (5a+15)x^3 + (-15a-3)x - 4a + 1$
	$(2)^{12} \cdot (3)^6 \cdot (5a+2)_{31}^{12}$	$(2a+1)_5^{10}$	$(-2a+3)x^6 + (-9a+18)x^5 + (15a-70)x^3 + (39a+54)x - 52a - 1$
$[5, 30, 180]$	$(3a+2)_{11}^{12} \cdot (2)^{18} \cdot (3)^6 \cdot (5a+2)_{31}^{12}$	$(2a+1)_5^{10}$	$684x^6 + (390a+90)x^5 + (24a-3138)x^4 + (217a+401)x^3$ $+ (96a+3918)x^2 + (-2112a-1698)x + 284a + 432$
	$(3a+1)_{11}^{12} \cdot (2a-11)_{139}^{12} \cdot (4a+3)_{19}^{12}$ $\cdot (2)^{18} \cdot (3)^6 \cdot (5a+2)_{31}^{12}$	$(2a+1)_5^{10}$	$(927a+2906)x^6 + (5541a+18822)x^5 + (-33535a-124380)x^3$ $+ (33417a+183726)x + 12641a - 31928$
$[5, 35, 245]$	$(3a+2)_{11}^{12} \cdot (2)^{12} \cdot (a+6)_{29}^{12}$ $\cdot (7)^6 \cdot (a+9)_{71}^{12}$	$(2a+1)_5^{10}$	$(-4527a-783)x^6 + (6392a+7811)x^5 + (-4500a-17085)x^3$ $+ (-6948a+9783)x - 1687a + 39$
	$(3a+1)_{11}^{12} \cdot (11a+5)_{151}^{12}$ $\cdot (2a+15)_{191}^{12} \cdot (2)^{12}$ $\cdot (a-5)_{29}^{12} \cdot (7)^6$	$(2a+1)_5^{10}$	$(-435a-521)x^6 + (353a+110)x^5 + (131927a+189531)x^4$ $+ (-696187a-952511)x^3 + (-10094248a-15393369)x^2$ $+ (94869598a+145990333)x - 210533420a - 329328479$
$[5, 105, 2205]$	$(3a+1)_{11}^{12} \cdot (3)^6 \cdot (7)^6$	$(2)^{20} \cdot (2a+1)_5^{10}$	$(-5a+4)x^6 + (-81a+30)x^5 + (-135a+210)x^4 + (450a-210)x^3$ $+ (360a-1785)x^2 + (600a+15)x - 950a + 5625$
	$(a+11)_{109}^{12} \cdot (3a+2)_{11}^{12} \cdot (3)^6$ $\cdot (7)^6 \cdot (8a+3)_{79}^{12}$	$(2)^{20} \cdot (2a+1)_5^{10}$	$(-3a-260)x^6 + (1032a+1389)x^5 + (19160a+8760)x^3$ $+ (-16224a+163200)x + 162976a + 114632$
$[8, 12, 18]$	$(a)_2^{12} \cdot (3)^6 \cdot (2a-1)_7^{12} \cdot (2a+1)_7^{12}$	$(a)_2^{30}$	$(24a-54)x^5 + (-66a+96)x^4 + (-32a+220)x^3 + (12a-312)x^2$ $+ (96a+21)x - 5a - 16$
$[17, 119, 3332]$	$(2a+15)_{179}^{12} \cdot (a+2)_2^{36}$ $\cdot (a-1)_2^{12} \cdot (4a+7)_{43}^{12} \cdot (7)^6$	$(2a+1)_{17}^{10}$	$(213a+1875)x^6 + (8071a+4059)x^5 + (-1045a+58039)x^4$ $+ (32898a+26657)x^3 + (-12585a+3550)x^2 + (-46889a$ $- 136176)x - 42057a - 104692$
$[17, 255, 15300]$	$(2a-5)_{19}^{12} \cdot (a+2)_2^{24}$ $\cdot (a-1)_2^{24} \cdot (3)^6 \cdot (2a+31)_{883}^{12}$	$(2a+1)_{17}^{10} \cdot (5)^{10}$	$(-4264a-13208)x^6 + (9516a-94116)x^5 + (331770a-503670)x^4$ $+ (-1195640a+1593625)x^3 + (1141785a-2476410)x^2$ $+ (-69927a+2540472)x - 301251a - 1280828$
	$(2a+3)_{13}^{12} \cdot (4a+17)_{157}^{12} \cdot (2a+7)_{19}^{12}$ $\cdot (a+2)_2^{12} \cdot (a-1)_2^{12} \cdot (3)^6 \cdot (4a+3)_{67}^{12}$ $\cdot (2a-9)_{83}^{12} \cdot (2a+11)_{83}^{12}$	$(2a+1)_{17}^{10} \cdot (5)^{10}$	$(3703196a+9037010)x^6 + (12666396a+36366348)x^5$ $+ (33133830a+56148570)x^4 + (35333760a+111063545)x^3$ $+ (71845845a+45282705)x^2 + (154100103a-105860229)x$ $+ 81081415a - 36366223$

Table 2b.

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[5, 11, 29]$	$[29, 7, 5]$	$\alpha^2 + 3$	$(2)^{12} \cdot (a-1)_5^{12} \cdot (a+1)_7^{12}$	$(a+2)_5^{10}$	$(18a+60)x^6+(-76a-246)x^5+(127a+329)x^4$ $+(-77a-209)x^3+(-30a+155)x^2+(29a-69)x$ $+ 71a - 156$
			$(2)^{12} \cdot (a+6)_{23}^{12} \cdot (a-1)_5^{12}$	$(a+2)_5^{10}$	$(2a+1)x^6 + (-a-26)x^5 + (9a+38)x^4$ $+(-40a-25)x^3+(-21a-37)x^2+(100a+218)x$ $+ 102a + 268$
$[5, 13, 41]$	$[41, 11, 20]$	$\alpha^2 + 5$	$(a-3)_2^{12}$	$(a+4)_2^{20} \cdot (2a-5)_5^{10}$	$(-a+3)x^6 + (4a-8)x^5 + 10x^4 + (-a+20)x^3$ $+ (4a+5)x^2 + (a+4)x + 1$
$[5, 17, 61]$	$[61, 9, 5]$	$\alpha^2 + 4$	$(a-3)_3^{12}$	$(2)^{20} \cdot (a-4)_5^{10}$	$(a+4)x^6 + (-8a-42)x^5 + (37a+117)x^4$ $+ (-20a-240)x^3 + (56a-9)x^2 + (22a-114)x$ $+ 9a - 28$
$[5, 21, 109]$	$[109, 17, 45]$	$\alpha^2 + 8$	$(a-5)_3^{12} \cdot (3a+17)_5^{12}$	$(2)^{20} \cdot (3a-14)_5^{10}$	$(-28a+53)x^6 + (-113a+913)x^5$ $+ (-495a+1890)x^4 + (-746a+3308)x^3$ $+ (-563a+3574)x^2 + (-378a+1069)x - 151a$ $- 227$
$[5, 26, 149]$	$[149, 13, 5]$	$\alpha^2 + 6$	$(a+7)_5^{12} \cdot (a-5)_7^{12}$	$(2)^{20} \cdot (a-6)_5^{10}$	$(-125a-875)x^6 + (-1375a-8575)x^5$ $+(-9090a-62160)x^4+(-38862a-251798)x^3$ $+(-73257a-489843)x^2+(-53235a-347403)x$ $- 12896a - 86314$
$[5, 33, 261]$	$[29, 21, 45]$	$\frac{1}{3}\alpha^2 + 3$	$(a+5)_{13}^{12} \cdot (3)^6$	$(2)^{20} \cdot (a+2)_5^{10}$	$(-27a-96)x^5+(-18a-51)x^4+(-34a-58)x^3$ $+ (-18a-36)x^2 - 15x - 9a - 27$
			$(3)^6 \cdot (a)_7^{12}$	$(2)^{20} \cdot (a+2)_5^{10}$	$(-3a+6)x^5 - 90x^4 + (-128a-136)x^3$ $+ (-72a-744)x^2 + (-240a-240)x - 216$
$[5, 34, 269]$	$[269, 17, 5]$	$\alpha^2 + 8$	$(a-7)_{11}^{12} \cdot (2a-15)_{13}^{12}$ $\cdot (a+9)_5^{12}$	$(2)^{20} \cdot (a-8)_5^{10}$	$(-283a+2246)x^6 + (-4563a+33800)x^5$ $+ (-11932a+103166)x^4 + (127408a$ $- 1032304)x^3 + (998576a-7558008)x^2$ $+ (2439792a-18969664)x + 2110776a$ $- 16149072$

TABLE 2B. *Continued.*

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C: y^2 = f$
$[5, 41, 389]$	$[389, 37, 245]$	$\alpha^2 + 18$	$(2a+21)_{11}^{12} \cdot (8a+83)_{17}^{12} \cdot (5a+52)_{19}^{12} \cdot (3a-28)_{5}^{12}$	$(2)^{20} \cdot (3a+31)_{5}^{10}$	$(1248a - 11685)x^6 + (-16097a + 150611)x^5 + (37185a - 349530)x^4 + (250806a - 2359968)x^3 + (-972081a + 9046728)x^2 + (-942318a + 8701533)x + 4994791a - 46866753$
$[5, 66, 909]$	$[101, 33, 45]$	$\frac{1}{3}\alpha^2 + 5$	$(a-2)_{19}^{12} \cdot (3)^6 \cdot (2a+13)_{43}^{12} \cdot (a-4)_{5}^{12}$	$(2)^{20} \cdot (a+5)_{5}^{10}$	$(-340a - 1674)x^6 + (-4179a - 26820)x^5 + (-26433a - 118800)x^4 + (-38358a - 315240)x^3 + (-46686a - 41130)x^2 + (40761a - 15348)x - 13013a + 39100$
			$(3)^6 \cdot (a+8)_{31}^{12} \cdot (2a-7)_{37}^{12} \cdot (a-4)_{5}^{12}$	$(2)^{20} \cdot (a+5)_{5}^{10}$	$(-6120a - 36189)x^6 + (-22143a - 102375)x^5 + (-21378a - 184140)x^4 + (-31356a - 65810)x^3 + (765a - 81765)x^2 + (-3783a + 6192)x$
$[8, 10, 17]$	$[17, 5, 2]$	$\alpha^2 + 2$	$(a+2)_{2}^{6}$	$(a+2)_{2}^{45} \cdot (a-1)_{2}^{20}$	$x^6 + (2a+4)x^5 + (3a+14)x^4 + (10a+8)x^3 + (-9a+32)x^2 + (16a-16)x - 4a + 8$
$[8, 18, 73]$	$[73, 9, 2]$	$\alpha^2 + 4$	$(a-4)_{2}^{6} \cdot (a+5)_{2}^{12} \cdot (4a-15)_{3}^{12}$	$(a-4)_{2}^{45}$	$(a+5)x^6 + (28a+132)x^5 + (214a+1026)x^4 + (349a+1658)x^3 + (259a+1242)x^2 + (47a+222)x - 3a - 14$
$[8, 22, 89]$	$[89, 11, 8]$	$\alpha^2 + 5$	$(a-4)_{2}^{12} \cdot (a+5)_{2}^{6} \cdot (4a-17)_{5}^{12}$	$(a+5)_{2}^{45}$	$(a-4)x^6 + (8a-36)x^5 + (16a-62)x^4 + (-13a+57)x^3 + (-17a+73)x^2 + (13a-57)x - a + 5$
$[8, 34, 281]$	$[281, 17, 2]$	$\alpha^2 + 8$	$(42a-331)_{17}^{12} \cdot (a-8)_{2}^{6} \cdot (a+9)_{2}^{24} \cdot (76a+675)_{5}^{12} \cdot (8a-63)_{7}^{12}$	$(a-8)_{2}^{45}$	$(-15024a + 118185)x^6 + (310153a - 2435026)x^5 + (-2658057a + 20990488)x^4 + (12047831a - 97400942)x^3 + (-33280854a + 231380920)x^2 + (34989188a - 413796872)x - 37610304a + 81055944$
$[8, 38, 233]$	$[233, 19, 32]$	$\alpha^2 + 9$	$(38a-271)_{13}^{12} \cdot (a+8)_{2}^{12} \cdot (a-7)_{2}^{6} \cdot (8a+65)_{7}^{12} \cdot (8a-57)_{7}^{12}$	$(a-7)_{2}^{45}$	$(-166628a - 1355047)x^6 + (-354121a - 2879769)x^5 + (-318274a - 2588269)x^4 + (-153661a - 1249743)x^3 + (-41827a - 339754)x^2 + (-6158a - 48444)x - 441a - 2400$

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

Table 2b. *Continued.*

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[8, 50, 425]$	$[17, 25, 50]$	$\frac{1}{5}\alpha^2 + 2$	$(a+2)_2^6 \cdot (a-1)_2^{12} \cdot (5)^6$	$(a+2)_2^{45} \cdot (5)^{15}$	$(34a+80)x^6 + (140a+224)x^5 + (110a-220)x^4 + (-455a+220)x^3 + (-5a+190)x^2 + (91a-104)x + 254a - 395$
			$(2a+3)_{13}^{12} \cdot (2a-5)_{19}^{12} \cdot (a+2)_2^6 \cdot (a-1)_2^{24} \cdot (5)^6$	$(a+2)_2^{45} \cdot (5)^{15}$	$(-1455a+1511)x^6 + (-1004a-2656)x^5 + (-19100a+20290)x^4 + (-3805a-4380)x^3 + (-72745a+108600)x^2 + (-7451a+10748)x - 99295a + 155108$
$[8, 66, 1017]$	$[113, 33, 18]$	$\frac{1}{3}\alpha^2 + 5$	$(4a-19)_{11}^{12} \cdot (a+6)_2^{12} \cdot (a-5)_2^6 \cdot (3)^6 \cdot (8a+47)_{41}^{12} \cdot (6a+35)_7^{12} \cdot (6a-29)_7^{12}$	$(a-5)_2^{45}$	$(-4215a-14698)x^6 + (30036a+338652)x^5 + (-549576a-134610)x^4 + (-2945519a + 22716733)x^3 + (12849441a-76601511)x^2 + (234523575a-1115687637)x - 843111919a + 4054444133$
			$(a+6)_2^{12} \cdot (a-5)_2^6 \cdot (3)^6 \cdot (2a+13)_{31}^{12} \cdot (28a+163)_{53}^{12} \cdot (6a+35)_7^{12}$	$(a-5)_2^{45}$	$(-27a-2538)x^6 + (7230a+8412)x^5 + (-3867a-272622)x^4 + (121693a+458725)x^3 + (-1686144a+6014715)x^2 + (-5324007a + 27892107)x + 110392412a - 532554277$
$[13, 9, 17]$	$[17, 15, 52]$	$\alpha^2 + 7$	$(a+2)_2^{12}$	$(2a-1)_{13}^{10} \cdot (a-1)_2^{20}$	$(a-2)x^6 + (-8a+8)x^5 + (14a-32)x^4 + (-19a+27)x^3 + (6a-21)x^2 + (3a+9)x - 4a - 7$
$[13, 18, 29]$	$[29, 9, 13]$	$\alpha^2 + 4$	$(a-1)_5^{12}$	$(a-4)_{13}^{10} \cdot (2)^{20}$	$(9a-22)x^6 + (-19a+21)x^5 + (8a-95)x^4 + (-70a-6)x^3 + (-23a-148)x^2 + (-7a-127)x - 18a - 7$
$[13, 29, 181]$	$[181, 41, 13]$	$\frac{1}{3}\alpha^2 + \frac{19}{3}$	$(6a-37)_{29}^{12} \cdot (a-6)_3^{12} \cdot (a+7)_3^{12} \cdot (4a+29)_5^{12}$	$(3a-19)_{13}^{10} \cdot (2)^{20}$	$(-16581a-119826)x^6 + (-52472a - 379062)x^5 + (-67729a-508419)x^4 + (-78876a-162464)x^3 + (-44960a+21657)x^2 + (14402a-144114)x - 21885a + 131494$
$[13, 41, 157]$	$[157, 25, 117]$	$\alpha^2 + 12$	$(3a+20)_{11}^{12} \cdot (a-7)_{17}^{12} \cdot (a-6)_3^{12} \cdot (a+7)_3^{12}$	$(2a-11)_{13}^{10} \cdot (2)^{20}$	$(-1181a+7035)x^6 + (18395a-104353)x^5 + (-116071a+664673)x^4 + (386042a - 2282384)x^3 + (-742970a+4253365)x^2 + (784564a-4063679)x - 253294a + 2224205$

TABLE 2B. *Continued.*

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[17, 5, 2]$	$[8, 10, 17]$	$\frac{1}{2}\alpha^2 + \frac{5}{2}$	1	$(3a+1)_{17}^{10} \cdot (a)_2^{30}$	$(-3a+4)x^5 - x^4 + (6a-2)x^3 + (9a-5)x^2 + (-3a+8)x - 3a + 6$
$[17, 15, 52]$	$[13, 9, 17]$	$\alpha^2 + 4$	$(a)_3^{12}$	$(a-4)_{17}^{10} \cdot (2)^{20}$	$-x^6 - 2ax^5 + (3a-3)x^4 + (8a+4)x^3 + (-19a+39)x^2 + (16a-30)x + 3a - 36$
$[17, 25, 50]$	$[8, 50, 425]$	$\frac{1}{10}\alpha^2 + \frac{5}{2}$	$(a)_2^{24} \cdot (2a+1)_7^{12}$	$(3a+1)_{17}^{10} \cdot (5)^{10}$	$(6a-2)x^6 + (-50a-64)x^5 + (285a+485)x^4 + (-485a-435)x^3 + (-70a+90)x^2 + (244a+92)x + 70a - 166$
			$(a)_2^{36} \cdot (a+7)_{47}^{12} \cdot (2a+1)_7^{12}$	$(3a+1)_{17}^{10} \cdot (5)^{10}$	$(315a+422)x^6 + (1212a+1757)x^5 + (-2605a - 3240)x^4 + (-50a-625)x^3 + (1730a-570)x^2 + (864a-212)x + 72a + 456$
$[17, 46, 257]$	$[257, 23, 68]$	$\alpha^2 + 11$	$(11, a+5)^{12} \cdot (13, a+10)^{12} \cdot (2, a)^{12} \cdot (2, a+1)^{24} \cdot (59, a+14)^{12}$	$(17, a+6)^{10} \cdot (2, a+1)^{20}$	$(-22a-1802)x^6 + (3596a+11488)x^5 + (-30700a-354072)x^4 + (243927a + 1843299)x^3 + (-616892a-5576996)x^2 + (647768a+5283496)x - 198146a - 1755298$
$[17, 47, 548]$	$[137, 35, 272]$	$\alpha^2 + 17$	$(14a-75)_{11}^{12} \cdot (4a+25)_{19}^{12} \cdot (3a-16)_2^{12} \cdot (3a+19)_2^{24}$	$(8a+51)_{17}^{10}$	$(285a+1620)x^6 + (-2683a-19110)x^5 + (13341a+76698)x^4 + (-28642a-195577)x^3 + (40284a+245904)x^2 + (-27600a-177408)x + 8154a + 51670$
$[29, 7, 5]$	$[5, 11, 29]$	$\alpha^2 + 5$	$(2)^{12} \cdot (2a+1)_5^{12}$	$(a-5)_{29}^{10}$	$(-4a-5)x^6 + (11a+37)x^5 + (-65a-62)x^4 + (111a+104)x^3 + (-28a - 189)x^2 + (-28a+157)x - 19a - 76$
			$(2)^{12} \cdot (5a+3)_{31}^{12} \cdot (2a+1)_5^{12}$	$(a-5)_{29}^{10}$	$(18a+42)x^6 + (62a+194)x^5 + (-209a+31)x^4 + (-648a-471)x^3 + (116a+338)x^2 + (244a + 259)x - 65a - 159$
$[29, 9, 13]$	$[13, 18, 29]$	$\frac{1}{4}\alpha^2 + \frac{7}{4}$	$(a)_3^{12}$	$(2)^{20} \cdot (3a+2)_{29}^{10}$	$(-25a+56)x^6 + (172a-39)x^5 + (-39a+561)x^4 + (312a+234)x^3 + (73a+354)x^2 + (76a+141)x + 15a + 37$

TABLE 2B. *Continued.*

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[29, 21, 45]$	$[5, 33, 261]$	$\frac{1}{3}\alpha^2 + 5$	$(4a+1)_{19}^{12} \cdot (3)^6$	$(2)^{20} \cdot (a-5)_{29}^{10}$	$(-a+20)x^6 + (-87a-18)x^5 + (-48a+198)x^4 + (-8a-296)x^3 + (384a+360)x^2 + (-384a - 480)x + 144a + 216$
			$(3)^6$	$(2)^{20} \cdot (a-5)_{29}^{10}$	$(-102a - 165)x^5 + (45a + 72)x^4 + (-174a - 262)x^3 + (36a-66)x^2 + (69a-144)x + 5a - 107$
$[29, 26, 53]$	$[53, 13, 29]$	$\alpha^2 + 6$	$(a-1)_{11}^{12} \cdot (a+1)_{13}^{12} \cdot (a+6)_{17}^{12}$	$(2)^{20} \cdot (a-6)_{29}^{10}$	$(-790a + 1564)x^6 + (241a - 12431)x^5 + (-15139a - 14345)x^4 + (-2950a - 165614)x^3 + (-51588a - 116086)x^2 + (-58139a - 53507)x + 12653a - 123381$
$[41, 11, 20]$	$[5, 13, 41]$	$\alpha^2 + 6$	1	$(2)^{20} \cdot (a-6)_{41}^{10}$	$(a+4)x^6 + (6a-2)x^5 + 17x^4 + (-12a-16)x^3 + (24a-5)x^2 + (-54a-16)x + 33a + 9$
$[53, 13, 29]$	$[29, 26, 53]$	$\frac{1}{4}\alpha^2 + \frac{11}{4}$	$(a+6)_{23}^{12} \cdot (a-1)_5^{12} \cdot (a)_7^{12}$	$(2)^{20} \cdot (3a+5)_{53}^{10}$	$(-31a+70)x^6 + (151a - 322)x^5 + (-405a + 658)x^4 + (238a - 846)x^3 + (3288a + 2437)x^2 + (-3262a + 12157)x - 27420a - 58255$
$[61, 9, 5]$	$[5, 17, 61]$	$\frac{1}{3}\alpha^2 + \frac{7}{3}$	1	$(2)^{20} \cdot (7a+4)_{61}^{10}$	$(a+2)x^6 + (-2a-15)x^5 + (36a-4)x^4 + (72a + 24)x^3 + (8a-24)x^2 + (-48a-80)x - 24a - 40$
$[73, 9, 2]$	$[8, 18, 73]$	$\frac{1}{2}\alpha^2 + \frac{9}{2}$	$(a)_2^{24} \cdot (2a-1)_7^{12}$	$(2a-9)_{73}^{10}$	$(-12a-6)x^6 + (8a+82)x^5 + (-51a+92)x^4 + (-126a-1)x^3 + (-36a+35)x^2 + (32a+50)x + 10a + 8$
$[73, 47, 388]$	$[97, 94, 657]$	$\frac{1}{8}\alpha^2 + \frac{43}{8}$	$(20a+109)_{101}^{12} \cdot (7a+38)_2^{24} \cdot (7a-31)_2^{12} \cdot (2a-9)_3^{12} \cdot (2a+11)_3^{12} \cdot (30a+163)_{79}^{12}$	$(22a+119)_{73}^{10}$	$(23a-43)x^6 + (-149a - 1221)x^5 + (8675a + 44883)x^4 + (-128038a - 698079)x^3 + (928849a + 5037588)x^2 + (123515a + 671208)x + 4023a + 21640$
$[89, 11, 8]$	$[8, 22, 89]$	$\frac{1}{4}\alpha^2 + \frac{11}{4}$	$(a)_2^{24}$	$(7a+3)_{89}^{10}$	$-x^5 + (-4a+2)x^4 + 21x^3 + (-16a+64)x^2 - 160x + 142a - 190$

TABLE 2B. *Continued.*

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C: y^2 = f$
$[97, 94, 657]$	$[73, 47, 388]$	$\frac{1}{3}\alpha^2 + \frac{22}{3}$	$(a-4)_2^{12} \cdot (a+5)_2^{12} \cdot (14a-53)_{23}^{12} \cdot (4a-15)_3^{12} \cdot (4a+19)_3^{12} \cdot (30a+143)_{41}^{12} \cdot (10a+47)_{61}^{12}$	$(24a+115)_{97}^{10}$	$(-128252a - 611298)x^6 + (-984572a - 4709700)x^5 + (-3071730a - 15394554)x^4 + (-6889006a - 20077475)x^3 + (-39650571a + 105355350)x^2 + (174191751a - 679664106)x + 256866525a - 973717416$
$[101, 33, 45]$	$[5, 66, 909]$	$\frac{1}{12}\alpha^2 + \frac{9}{4}$	$(3)^6 \cdot (2a+1)_5^{12} \cdot (7a+3)_{61}^{12}$	$(9a+5)_{101}^{10} \cdot (2)^{20}$	$(-216a + 464)x^6 + (-2304a - 48)x^5 + (-3984a - 960)x^4 + (-864a + 3088)x^3 + (-720a + 1422)x^2 + (-4047a - 5322)x - 818a - 2423$
			$(4a+3)_{19}^{12} \cdot (4a+1)_{19}^{12} \cdot (3)^6 \cdot (5a+3)_{31}^{12} \cdot (2a+1)_5^{12}$	$(9a+5)_{101}^{10} \cdot (2)^{20}$	$(-5229a + 4019)x^6 + (-6132a - 6909)x^5 + (44637a - 2364)x^4 + (53094a + 58660)x^3 + (-39159a + 19266)x^2 + (-30363a - 55761)x - 16848a - 16911$
$[109, 17, 45]$	$[5, 21, 109]$	$\alpha^2 + 10$	$(2a+1)_5^{12}$	$(a-10)_{109}^{10} \cdot (2)^{20}$	$(-8a - 8)x^6 - 16x^5 + (8a + 72)x^4 + (152a + 184)x^3 + (6a + 84)x^2 + (-255a - 339)x - 319a - 524$
$[113, 33, 18]$	$[8, 66, 1017]$	$\frac{1}{6}\alpha^2 + \frac{11}{2}$	$(3a+11)_{103}^{12} \cdot (a)_2^{24} \cdot (3)^6 \cdot (4a-1)_{31}^{12} \cdot (2a-1)_7^{12} \cdot (2a+1)_7^{12}$	$(2a-11)_{113}^{10}$	$(122a + 800)x^6 + (-1509a - 909)x^5 + (36762a - 85470)x^4 + (-116871a + 265713)x^3 + (-467682a + 704460)x^2 + (-480528a + 365352)x - 7616a + 226442$
			$(a)_2^{24} \cdot (3)^6 \cdot (4a+1)_{31}^{12} \cdot (2a+1)_7^{12}$	$(2a-11)_{113}^{10}$	$(-418a - 190)x^6 + (1476a - 660)x^5 + (1146a + 6810)x^4 + (2145a + 2175)x^3 + (-1437a - 3489)x^2 + (-42a - 2736)x + 830a + 394$
$[137, 35, 272]$	$[17, 47, 548]$	$\alpha^2 + 23$	$(2a-5)_{19}^{12} \cdot (a+2)_2^{12} \cdot (a-1)_2^{12}$	$(6a-1)_{137}^{10}$	$(4a + 6)x^6 + (8a + 36)x^5 + (-4a + 42)x^4 + (586a + 1289)x^3 + (1066a + 2808)x^2 + 4ax + 25596a + 65566$

Table 2b. *Continued.*

DAB	DAB^r	a	Δ_{stable}	$\Delta(C)/\Delta_{\text{stable}}$	f, where $C : y^2 = f$
$[149, 13, 5]$	$[5, 26, 149]$	$\frac{1}{4}\alpha^2 + \frac{11}{4}$	$(3a+1)_{11}^{12}$	$(11a+7)_{149}^{10} \cdot (2)^{20}$	$8x^6 + 96x^5 + (-24a + 168)x^4 + (-576a - 808)x^3 + (66a - 132)x^2 + (292a + 47)x + 86a - 87$
$[157, 25, 117]$	$[13, 41, 157]$	$\frac{1}{9}\alpha^2 + \frac{16}{9}$	$(a-4)_{17}^{12} \cdot (3a-1)_{23}^{12} \cdot (a)_{3}^{24} \cdot (a+1)_{3}^{12}$	$(7a+5)_{157}^{10} \cdot (2)^{20}$	$(-3328a - 7633)x^6 + (-17510a - 39323)x^5 + (-32518a - 68044)x^4 + (-17960a - 66720)x^3 + (256a - 51704)x^2 + (5184a - 22864)x + 1432a - 5264$
$[181, 41, 13]$	$[13, 29, 181]$	$\frac{1}{3}\alpha^2 + \frac{13}{3}$	$(a+5)_{17}^{12} \cdot (3a+2)_{29}^{12} \cdot (a)_{3}^{24} \cdot (a+1)_{3}^{12}$	$(3a-13)_{181}^{10} \cdot (2)^{20}$	$(330a + 1417)x^6 + (11102a + 1701)x^5 + (1396a + 59742)x^4 + (24016a + 92792)x^3 + (74408a + 38064)x^2 + (35248a + 26160)x - 5784a + 21888$
$[233, 19, 32]$	$[8, 38, 233]$	$\frac{1}{8}\alpha^2 + \frac{19}{8}$	$(a)_{2}^{24} \cdot (a-5)_{23}^{12} \cdot (a+5)_{23}^{12} \cdot (2a+1)_{7}^{12}$	$(11a+3)_{233}^{10}$	$(2348a - 3554)x^6 + (11828a - 12348)x^5 + (4498a - 23598)x^4 + (12704a + 9133)x^3 + (-3151a - 14433)x^2 + (5344a - 1974)x + 18a - 604$
$[257, 23, 68]$	$[17, 46, 257]$	$\frac{1}{8}\alpha^2 + \frac{19}{8}$	$(2a+3)_{13}^{12} \cdot (a+2)_{2}^{12} \cdot (a-1)_{2}^{24} \cdot (4a-3)_{43}^{12} \cdot (2a+9)_{47}^{12} \cdot (4a+13)_{53}^{12}$	$(8a-19)_{257}^{10}$	$(-2809a - 7326)x^6 + (5069a + 3572)x^5 + (52427a - 51416)x^4 + (249518a + 105951)x^3 + (-311115a - 180355)x^2 + (156533a - 20215)x - 34657a + 19003$
$[269, 17, 5]$	$[5, 34, 269]$	$\frac{1}{4}\alpha^2 + \frac{15}{4}$	$(3a+1)_{11}^{12} \cdot (2a+1)_{5}^{12}$	$(2)^{20} \cdot (15a+11)_{269}^{10}$	$(-168a - 272)x^6 + (960a + 1696)x^5 + (472a - 1008)x^4 + (-4448a - 1552)x^3 + (358a + 904)x^2 + (945a + 1690)x$
$[281, 17, 2]$	$[8, 34, 281]$	$\frac{1}{2}\alpha^2 + \frac{17}{2}$	$(a)_{2}^{36} \cdot (4a+1)_{31}^{12} \cdot (2a-1)_{7}^{12} \cdot (2a+1)_{7}^{12}$	$(2a-17)_{281}^{10}$	$(-835a + 1960)x^6 + (1343a + 7589)x^5 + (19630a + 6428)x^4 + (26923a + 13601)x^3 + (-6743a + 44228)x^2 + (-5762a + 18262)x + 17138a - 23184$
$[389, 37, 245]$	$[5, 41, 389]$	$\frac{1}{5}\alpha^2 + \frac{18}{5}$	$(3a+1)_{11}^{12} \cdot (3a+2)_{11}^{12} \cdot (4a+3)_{19}^{12} \cdot (4a+1)_{19}^{12} \cdot (a+6)_{29}^{12} \cdot (2a+1)_{5}^{12}$	$(2)^{20} \cdot (18a+13)_{389}^{10}$	$(-22952a - 6848)x^6 + (162272a - 61136)x^5 + (296568a + 208208)x^4 + (-212600a - 959344)x^3 + (89874a + 1610270)x^2 + (-428348a - 1023457)x + 315516a + 343397$

TABLE 2C.

DAB	DAB reflex	a	Obstructions	Curves
$[8, 14, 41]$	$[41, 7, 2]$	$\alpha^2 + 3$	$(a + 4)_2, (a - 3)_2$	2
$[8, 26, 137]$	$[137, 13, 8]$	$\alpha^2 + 6$	$(3a - 16)_2, (3a + 19)_2$	2
$[8, 30, 153]$	$[17, 15, 18]$	$\frac{1}{3}\alpha^2 + 2$	$(a + 2)_2, (a - 1)_2$	4
$[12, 8, 13]$	$[13, 10, 12]$	$\frac{1}{2}\alpha^2 + 2$	$(a + 1)_3, (2)$	2
$[12, 10, 13]$	$[13, 5, 3]$	$\alpha^2 + 2$	$(a + 1)_3, (2)$	2
$[12, 14, 37]$	$[37, 7, 3]$	$\alpha^2 + 3$	$(a + 3)_3, (2)$	2
$[12, 26, 61]$	$[61, 13, 27]$	$\alpha^2 + 6$	$(a - 3)_3, (2)$	2
$[12, 26, 157]$	$[157, 13, 3]$	$\alpha^2 + 6$	$(a - 6)_3, (2)$	2
$[12, 50, 325]$	$[13, 25, 75]$	$\frac{1}{5}\alpha^2 + 2$	$(a + 1)_3, (2)$	4
$[44, 8, 5]$	$[5, 14, 44]$	$\frac{1}{2}\alpha^2 + 3$	$(2), (3a + 2)_{11}$	2
$[44, 14, 5]$	$[5, 7, 11]$	$\alpha^2 + 3$	$(2), (3a + 2)_{11}$	2
$[44, 42, 45]$	$[5, 21, 99]$	$\frac{1}{3}\alpha^2 + 3$	$(2), (3a + 2)_{11}$	4
$[76, 18, 5]$	$[5, 9, 19]$	$\alpha^2 + 4$	$(2), (4a + 3)_{19}$	2
$[172, 34, 117]$	$[13, 17, 43]$	$\frac{1}{3}\alpha^2 + \frac{7}{3}$	$(2), (4a + 5)_{43}$	2
$[236, 32, 20]$	$[5, 16, 59]$	$\frac{1}{2}\alpha^2 + \frac{7}{2}$	$(2), (7a + 5)_{59}$	2

6. *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 [**9**]).

(1) Compute the Igusa invariants $I_n(\widetilde{C})$ of a genus-two curve $\widetilde{C}$ with CM by an order $\mathcal{O}_K$ over a number field L.

(2) Reduce these invariants modulo a prime $\mathfrak{p}$ of L, which yields elements of the residue field $k = \mathcal{O}_L/\mathfrak{p}$.

(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, Φ) of $\widetilde{C}$ and the number of k-points in the Jacobian groups of C and its quadratic twist C'. So with a good choice of Φ and $\mathfrak{p}$, 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 $\widetilde{C}$ from our table, and let C be ($\widetilde{C}$ mod $\mathfrak{p}$). 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 [**15**, § 8, Example of Algorithm 3] a curve C is constructed following the recipe 1.,2.,3. with Φ a certain CM-type of $K = [5, 13, 41]$. This curve is defined over a finite

https://doi.org/10.1112/S1461157015000121 Published online by Cambridge University Press

field $k = \mathbf{F}_{p^2}$, where

$$p = 142003856595807482747635387048977088071520136032341569\\ 014612056864049709760143646636956724980664377491196079\\ 730519617723521029855649462172148699393958968638652107\\ 696147277436345811056227385195781997362304851932650270\\ 514293705125991379$$

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_6 small (either 1 or a small non-square in k) and ensure $a_5 = 0$. Then there are five coefficients $a_0, \ldots, a_4 \in \mathbf{F}_{p^2}$, 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 $X^2 + 1 - 10$ over $\mathbf{Q}$. We find that up to twist and up to conjugation of $K_0^r = \mathbf{Q}(a)/\mathbf{Q}$, we have $\widetilde{C} : y^2 = f(x)$, where

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

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

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. So one of these curves could take the place of the curve in [**15**].

REMARK 6.1. 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 $(\pi) = \mathfrak{p}_1^2\mathfrak{p}_2$, where $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ by [**15**, Lemma 21]. This fixes π 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 us 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 6.2. *Let K, K^{r}, f, and $\Delta(C)$ be as in an entry of Tables 1a, 1b, or 2b other than* DAB $= [5,5,5]$. *Let $\mathfrak{p} \nmid \Delta(C)$ be a prime of K_0^{r} that is not inert in $K^{\mathrm{r}}/K_0^{\mathrm{r}}$ and let $k_{\mathfrak{p}}$ be its residue field. Let $\overline{f} = (f \bmod \mathfrak{p})$ and let $b \in k_{\mathfrak{p}}^*$ be a non-square. Let C_1, C_2 be the curves $y^2 = \overline{f}$ and $y^2 = b\overline{f}$ over $k_{\mathfrak{p}}$.*

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

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 $\{\mathrm{Frob}_{C_i,N(\mathfrak{p})}\} = \{\pm\pi\}$. In particular, we have $\{\#J(C_i)(k_{\mathfrak{p}})\} = \{N_{K/\mathbf{Q}}(\pm\pi - 1)\}$.

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

Note that we have a surjective map $\mathcal{O}_{K_0} = \mathbf{Z}_p[X]/(X^2 + \epsilon X + (\epsilon - D^{\mathrm{r}})/4) \to k_{\mathfrak{p}}$, 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 6.2. Our assumptions imply $k_{\mathfrak{P}} = k_{\mathfrak{p}}$, and our Φ^{r} is the *reflex* of Φ as defined in [**27**]. Our curves have Jacobians with endomorphism ring $\mathcal{O}_K$ of type Φ over K^{r} by Theorem 5.1. Moreover, they have good reduction at $\mathfrak{P}$ by $\mathfrak{p} \nmid \Delta(C)$. Therefore, by the Shimura–Taniyama formula ([**27**, Theorem 1(ii) in § 13.1] or [**18**, Theorem 4.1.2]), we have $\mathrm{Frob}_{C_i,N(\mathfrak{p})}\mathcal{O}_K = N_{\Phi^{\mathrm{r}}}(\mathfrak{P})$. This proves that the latter ideal has a generator π with $\pi\overline{\pi} \in \mathbf{Q}$. Such a generator is unique up to roots of unity, of which $\mathcal{O}_K$ contains only ± 1. Since b is a non-square, twisting by it changes the root of unity, hence $\{\pm\pi\}$ occurs exactly for $\{\overline{f}, b\overline{f}\}$. $\square$

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, Kristin Lauter and Bianca Viray for help with their formulas [**19**], Christophe Ritzenthaler for the reference [**22**], and the anonymous referee for helpful suggestions for the improvement of the exposition.

References

1. G. Bisson and M. Streng, 'On polarised class groups of orders in quartic CM-fields', Preprint, 2013, arXiv:1302.3756.

2. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265; Computational algebra and number theory (London, 1993).

3. J. H. Bruinier and T. Yang, 'CM-values of Hilbert modular functions', *Invent. Math.* 163 (2006) no. 2, 229–288.

4. G. Cardona and J. Quer, 'Field of moduli and field of definition for curves of genus 2', *Computational aspects of algebraic curves*, Lecture Notes in Computer Science 13 (World Scientific, 2005) 71–83.

5. R. Carls, D. Kohel and D. Lubicz, 'Higher-dimensional 3-adic CM construction', *J. Algebra* 319 (2008) no. 3, 971–1006.

6. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, Vol. 230 (Cambridge University Press, 1996).

7. D. A. Cox, *Primes of the form $x^2 + ny^2$* (John Wiley & Sons, 1989).

8. K. Eisenträger and K. Lauter, 'A CRT algorithm for constructing genus 2 curves over finite fields', *Arithmetics, geometry, and coding theory (AGCT 2005)*, Séminaires et Congrès 21 (Société Mathématique de France, Paris, 2010) 161–176; arXiv:math/0405305.

9. G. Frey and T. Lange, 'Complex multiplication', *Handbook of elliptic and hyperelliptic curve cryptography* (eds H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren; Chapman & Hall/CRC, 2006) 455–473.

10. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng, 'The 2-adic CM method for genus 2 curves with application to cryptography', *Advances in cryptology – ASIACRYPT 2006*, Lecture Notes in Computer Science 4284 (Springer, 2006) 114–129.

11. 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/.

12. E. Z. Goren and K. Lauter, 'Class invariants for quartic CM fields', *Ann. Inst. Fourier (Grenoble)* 57 (2007) no. 2, 457–480.

13. E. Z. Goren and K. Lauter, 'Genus 2 curves with complex multiplication', *Int. Math. Res. Not. IMRN* 2012 (2012) no. 5, 1068–1142.

14. M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics 201 (Springer, New York, 2000).

15. L. Hitt, G. McGuire, M. Naehrig and M. Streng, 'A CM construction for curves of genus 2 with p-rank 1', *J. Number Theory* 131 (2011) no. 5, 920–935; arXiv:0811.3434.

16. J.-I. Igusa, 'Arithmetic variety of moduli for genus two', *Ann. of Math.* (2) 72 (1960) no. 3, 612–649.

17. D. Kohel *et al.*, 'ECHIDNA algorithms for algebra and geometry experimentation,' 2007, http://echidna.maths.usyd.edu.au/~kohel/dbs/complex_multiplication2.html.

18. S. Lang, *Complex multiplication*, Grundlehren der mathematischen Wissenschaften 255 (Springer, 1983).

19. K. Lauter and B. Viray, 'An arithmetic intersection formula for denominators of Igusa class polynomials', *Amer. J. Math.* 137 (2015) no. 2, 497–533; doi:10.1353/ajm.2015.0010; arXiv:1210.7841v1.

20. Q. Liu, 'Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète', *Trans. Amer. Math. Soc.* 348 (1996) no. 11, 4577–4610.
21. J.-F. Mestre, 'Construction de courbes de genre 2 à partir de leurs modules', *Effective methods in algebraic geometry (Castiglioncello, 1990)*, Progress in Mathematics 94 (Birkhäuser, Boston, 1991) 313–334.
22. J. S. Milne, 'Abelian varieties defined over their fields of moduli, I', *Bull. Lond. Math. Soc.* 4 (1972) 370–372.
23. N. Murabayashi and A. Umegaki, 'Determination of all **Q**-rational CM-points in the moduli space of principally polarized abelian surfaces', *J. Algebra* 235 (2001) no. 1, 267–274.
24. The PARI Group, Bordeaux, PARI/GP, version 2.4.3, 2011, http://pari.math.u-bordeaux.fr/.
25. G. Shimura, 'On the zeta function of an abelian variety with complex multiplication', *Ann. of Math.* (2) 94 (1971) no. 2, 504–533.
26. G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Princeton University Press, 1994).
27. G. Shimura, *Abelian varieties with complex multiplication and modular functions* (Princeton University Press, 1998); sections 1–16 essentially appeared before in [28].
28. G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan 6 (The Mathematical Society of Japan, Tokyo, 1961).
29. W. Stein *et al.*, Sage mathematics software 4.7.2, 2011, http://www.sagemath.org/.
30. M. Stoll and J. E. Cremona, 'On the reduction theory of binary forms', *J. Reine Angew. Math.* 565 (2003) 79–99.
31. M. Streng, Sage package for using Shimura's reciprocity law for Siegel modular functions, http://www.math.leidenuniv.nl/∼streng/recip/.
32. M. Streng, 'Complex multiplication of abelian surfaces', PhD Thesis, Universiteit Leiden, 2010, http://hdl.handle.net/1887/15572.
33. M. Streng, 'An explicit reciprocity law for Siegel modular functions', Preprint, 2011, arXiv:1201.0020.
34. M. Streng, 'Computing Igusa class polynomials', *Math. Comp.* 83 (2014) 275–309; arXiv:0903.4766.
35. M. Streng and F. Bouyer, 'Implementation of Mestre's algorithm in Sage', http://trac.sagemath.org/sage_trac/ticket/6341.
36. M. Streng and F. Bouyer, 'Sage code for reduction of hyperelliptic curves, and data files for "Examples of CM curves of genus two defined over the reflex field"', https://bitbucket.org/mstreng/reduce.
37. G. van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 16 (Springer, 1988).
38. P. van Wamelen, 'Examples of genus two CM curves defined over the rationals', *Math. Comp.* 68 (1999) no. 225, 307–320.
39. P. van Wamelen, 'Proving that a genus 2 curve has complex multiplication', *Math. Comp.* 68 (1999) no. 228, 1663–1677.
40. T. Yang, 'Arithmetic intersection on a Hilbert modular surface and the Faltings height', *Asian J. Math.* 17 (2013) no. 2, 335–381; doi:10.4310/AJM.2013.v17.n2.a4; arXiv:1008:1854.
41. P. Zimmermann *et al.*, GMP-ECM 6.4.2 (elliptic curve method for integer factorization), 2012, https://gforge.inria.fr/projects/ecm/.

Florian Bouyer
University of Warwick
United Kingdom

F.Bouyer@Warwick.ac.uk

Marco Streng
Universiteit Leiden
Netherlands

Marco.Streng@gmail.com