MATHEMATICS OF COMPUTATION
Volume 68, Number 225, January 1999, Pages 307–320
S 0025-5718(99)01020-0

EXAMPLES OF GENUS TWO CM CURVES DEFINED OVER THE RATIONALS

PAUL VAN WAMELEN

Abstract. We present the results of a systematic numerical search for genus two curves defined over the rationals such that their Jacobians are simple and have endomorphism ring equal to the ring of integers of a quartic CM field. Including the well-known example $y^2 = x^5 - 1$ we find 19 non-isomorphic such curves. We believe that these are the only such curves.

1. Introduction

It is well known that there are only a finite number of elliptic curves defined over the rationals with Complex Multiplication. We would like to consider the analogous question for genus two curves. In particular we will look for examples of genus two curves defined over the rationals such that their Jacobians are simple and have endomorphism ring equal to the ring of integers of a quartic CM field. We believe that we have found all such examples. Note though that we did not consider the case of non-simple Jacobians, nor the case where the endomorphism ring is a non-maximal order in a CM field. The curves we found are correct to high precision, but we did not prove that they have Complex Multiplication.

We look for such curves as follows. We start out with a list of quartic CM fields ordered by discriminant. Then it is easy to construct a torus with endomorphism ring equal to the ring of integers of such a field (see section 2). Now we can make these tori into abelian varieties by finding a Riemann form on the torus. In section 3 we see how to find all distinct Riemann forms. This leads to an explicit algorithm for writing down all abelian varieties with endomorphism ring equal to the ring of integers in a given CM field. Most of the theory in these two sections can also be found in [4] or [11] (see also [12]).

Now we can use the theory of theta functions to compute (to high precision) an equation for a curve with Jacobian equal to a given abelian surface. This is explained in section 4. This curve is in a canonical form, and we must finally address the question of whether such a curve can be defined over the rationals. Mestre's solution to this problem is recalled in section 5. Section 6 contains some notes on the implementation of these ideas, and Section 7 briefly discusses the results.

Received by the editor June 13, 1996.

1991 *Mathematics Subject Classification.* Primary 14-04; Secondary 14K22.

This work was partially supported by grant LEQSF(1995-97)-RD-A-09 from the Louisiana Educational Quality Support Fund.

2. Constructing a torus

For the rest of this paper F will be a CM-field with $[F:\mathbb{Q}] = 2n$. That is, F is a totally imaginary quadratic extension of a totally real field F^+. Later we will set $n = 2$. By a CM type of F we mean a set Φ of one half of the embeddings of F into $\mathbb{C}$ such that no two of them are complex conjugate. Recall that if A is a complex torus of dimension n such that $F \subset \operatorname{End}(A)_{\mathbb{Q}}$, then the complex representation of $\operatorname{End}(A)_{\mathbb{Q}}$ is isomorphic to $\sum_{\phi_i \in \Phi} \phi_i$ for some CM type Φ. We say A is of type (F, Φ).

Theorem 1. 1. *If $\mathfrak{a}$ is a lattice in F and Φ is a type, then $\mathbb{C}^n/\Phi(\mathfrak{a})$ is a complex torus of type (F, Φ).*
2. *If A is a complex torus of type (F, Φ), then there exists a lattice $\mathfrak{a}$ in F such that A is complex isomorphic to $\mathbb{C}^n/\Phi(\mathfrak{a})$.*
3. *If Φ is a simple type and $\mathfrak{a}$ is a fractional ideal of F, then* $\operatorname{End}(\mathbb{C}^n/\Phi(\mathfrak{a})) \cong \mathcal{O}_F$.

Proof. 1 and 2 are just i) and ii) of [4, Thm 1.4.1]. For 3 recall that if the type is simple the torus is simple ([4, 1.3.5]), and if the torus is simple $\operatorname{End}(A)_{\mathbb{Q}} = F$ ([4, Thm 1.3.3.i]). Now [4, Thm 1.4.1.iii] says that the endomorphism ring is given by all α such that $\alpha\mathfrak{a} \subset \mathfrak{a}$. So if $\mathfrak{a}$ is a fractional ideal the endomorphism ring is the ring of integers. □

Theorem 2. *If $\mathfrak{a}$ and $\mathfrak{b}$ are two fractional ideals in F and Φ is a simple type, then the two tori $\mathbb{C}^n/\Phi(\mathfrak{a})$ and $\mathbb{C}^n/\Phi(\mathfrak{b})$ are isomorphic if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class.*

Proof. This follows directly from [4, Thm 1.4.2]. □

We are interested in the case $n = 2$. In this case we can easily decide whether a given type is simple or not. From the fact that in a CM field complex conjugation commutes with any other Galois element we see that the only possibilities for the Galois group of a degree 4 CM field are the cyclic group of order 4, the Klein 4-group and the dihedral group of order 8. If the Galois group is the Klein 4-group, then the field is biquadratic and we see that the type must be lifted from an imaginary quadratic subfield and is therefore not simple. In the other two cases the type is simple.

3. Finding a Riemann form

In the previous section we saw that for a given non-biquadratic quartic CM field F, there is a finite number of tori whose endomorphism ring is the ring of integers in F. For a torus to be an abelian variety it must admit a Riemann form. So we now need to decide which of these tori admit Riemann forms, and also whether there could be more than one Riemann form for a given torus.

Let $\mathfrak{D}_{F/\mathbb{Q}}$ be the different of F and $\mathfrak{d}_{F/\mathbb{Q}}$ its discriminant. Let a bar denote complex conjugation.

Theorem 3. 1. *If ξ is such that*
   (a) *$F = F^+(\xi)$, $\xi^2 \in F^+$ and $\operatorname{Im}(\phi_i(\xi)) > 0$ for all $\phi_i \in \Phi$, and*
   (b) *$\mathfrak{D}_{F/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}} = (\xi^{-1})$ for some fractional ideal $\mathfrak{a}$ of F,*

then

$$E(z,w) = \sum_{j=1}^{n} \phi_j(\xi)(\overline{z}_j w_j - z_j \overline{w}_j). \tag{1}$$

defines a principal polarization of type (F,Φ) *on* $\mathbb{C}^n/\Phi(\mathfrak{a})$.

2. *If* (F,Φ) *is a simple type, then all principal polarizations of type* (F,Φ) *on* $\mathbb{C}^n/\Phi(\mathfrak{a})$ *are given by such a* ξ.

Proof. Clearly $E(z,w) = -E(w,z)$ and

$$E(iz,w) = -i\sum_{j=1}^{n} \phi_j(\xi)(\overline{z}_j w_j + z_j \overline{w}_j)$$

is symmetric positive definite. Furthermore we have $E(\Phi(\alpha),\Phi(\beta)) = \mathrm{tr}_{F/\mathbb{Q}}(\xi\overline{\alpha}\beta)$, and so E will be integral valued on $\Phi(\mathfrak{a})$ if and only if $\xi\overline{\alpha}\beta \subset \mathfrak{D}^{-1}_{F/\mathbb{Q}}$. This proves that E is a non-degenerate Riemann form on $\mathbb{C}^n/\Phi(\mathfrak{a})$. Note that if $\{\alpha_i\}_{i=1}^{n}$ is a basis for the ideal $\mathfrak{a}$ then $\det(\mathrm{tr}_{F/\mathbb{Q}}(\xi\overline{\alpha_i}\alpha_j)) = N_{F/\mathbb{Q}}(\xi\mathfrak{a}\overline{\mathfrak{a}})\mathfrak{d}_{F/\mathbb{Q}}$; that is, if condition 1b holds, then $\det(E) = 1$ and E is a principal polarization.

For the converse, we see from [4, Thm 1.4.5] that every non-degenerate Riemann form E on $\mathbb{C}^n/\Phi(\mathfrak{a})$ is given by (1) for some ξ satisfying condition 1a. We have seen that, as E is integral valued, $\xi\mathfrak{a}\overline{\mathfrak{a}} \subset \mathfrak{D}$, and, as E defines a principal polarization, the norms of these two ideals are in fact equal. But then the ideals are equal. □

From now on (A,ξ) will denote an abelian variety with a principal polarization given by ξ as in the theorem.

We now address the question of whether we can find a ξ satisfying the conditions of the theorem for any $\mathbb{C}^n/\Phi(\mathfrak{a})$.

Theorem 4. *Let* $F = F^{+}(\sqrt{-m})$ *with* $m \in \mathcal{O}_{F^{+}}$. *Then we can find a fractional ideal* $\mathfrak{a} \subset F$ *and an element* $b \in \mathcal{O}_{F^{+}}$ *such that* $\mathfrak{D}_{F/\mathbb{Q}}/(\sqrt{-m}) = \mathfrak{a}\overline{\mathfrak{a}}b$.

Proof. Using the transitivity of the different, we will first consider the extension F/F^{+} and its different $\mathfrak{D}_{F/F^{+}}$. Let $\mathfrak{P}$ be a ramified (over F^{+}) prime of F. Assume that it occurs to an odd power, k, in the prime decomposition of $\mathfrak{D}_{F/F^{+}}/(\sqrt{-m})$. Then it occurs to the power $2k$ in the prime factorization of $\mathfrak{D}_{F/F^{+}}\overline{\mathfrak{D}_{F/F^{+}}}/(m)$. If $\mathfrak{p}$ is the prime of F^{+} such that $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}^2$, then recalling that $N(\mathfrak{D}_{F/F^{+}}) = \mathfrak{d}_{F/F^{+}}$, we see that $\mathfrak{p}$ occurs to the odd power k in the prime factorization of $\mathfrak{d}_{F/F^{+}}/m\mathcal{O}_{F^{+}}$. This, however, contradicts the fact that the discriminant $\mathfrak{d}_{F/F^{+}}$ differs by the square of an ideal from $m\mathcal{O}_{F^{+}}$. To see this recall that the discriminant is given by the greatest common divisor ideal of all discriminants of bases of F over F^{+} consisting of algebraic integers and it is easy to verify that

$$\mathrm{disc}(a_1 + b_1\sqrt{-m}, a_2 + b_2\sqrt{-m}) = 4(a_2b_1 - a_1b_2)^2 m.$$

So we can now write $\mathfrak{D}_{F/F^{+}}/(\sqrt{-m}) = \mathfrak{f}^2\mathfrak{g}\mathfrak{h}$, where $\mathfrak{f}$ consists of ramified primes, $\mathfrak{g}$ consists of split primes and $\mathfrak{h}$ of inert primes. Notice that as only ramified primes divide $\mathfrak{D}$, $\mathfrak{D}_{F/F^{+}}/(\sqrt{-m}) = \overline{\mathfrak{D}_{F/F^{+}}/(\sqrt{-m})}$. This implies that if $\mathfrak{P}$ is a prime in $\mathfrak{g}$ then $\mathfrak{P}\overline{\mathfrak{P}}$ must divide $\mathfrak{g}$, and we can write $\mathfrak{g} = \mathfrak{g}_1\overline{\mathfrak{g}_1}$ for some ideal $\mathfrak{g}_1$. The ideal $\mathfrak{h}$ consists of inert primes, so we see that we can write $\mathfrak{h} = \mathfrak{h}_0\mathcal{O}_F$ for some ideal $\mathfrak{h}_0 \subset F^{+}$. As the norm map from the ideal class group of F to that of F^{+}

is onto ([14, Theorem 10.1]), there exist an ideal $\mathfrak{h}_1 \subset F$ and $c_1 \in F^+$ such that $\mathfrak{h} = \mathfrak{h}_1\overline{\mathfrak{h}_1}c_1$. So we have

$$\mathfrak{D}_{F/F^+}/(\sqrt{-m}) = \mathfrak{f}\mathfrak{g}_1\mathfrak{h}_1\overline{\mathfrak{f}\mathfrak{g}_1\mathfrak{h}_1}c_1$$

Again using the fact that the norm map on class groups is onto, we can find an ideal $\mathfrak{d}_1$ and an element $d_1 \in F^+$ such that $\mathfrak{D}_{F^+/\mathbb{Q}}\mathcal{O}_F = \mathfrak{d}_1\overline{\mathfrak{d}_1}d_1$. Setting $\mathfrak{a} = \mathfrak{f}\mathfrak{g}_1\mathfrak{h}_1\mathfrak{d}_1$ and $b = c_1d_1$, we get

$$\mathfrak{D}_{F/\mathbb{Q}}/(\sqrt{-m}) = \mathfrak{D}_{F/F^+}\mathfrak{D}_{F^+/\mathbb{Q}}/(\sqrt{-m}) = \mathfrak{a}\bar{\mathfrak{a}}b.$$

□

This shows that for a simple CM field F, if we take $\mathfrak{a}$, b and m as in the theorem and set $\xi = (\sqrt{-m}b)^{-1}$ and choose Φ in such a way that $\mathrm{Im}(\phi_i(\xi)) > 0$ for all $\phi_i \in \Phi$, then ξ defines a principal polarization of type Φ on $\mathbb{C}^n/\Phi(\mathfrak{a}^{-1})$. So we have at least one principally polarized abelian variety whose endomorphism ring equals $\mathcal{O}_F$.

Next we want to address the question of how many non-isomorphic abelian varieties with complex multiplication by $\mathcal{O}_F$ we can construct.

Theorem 5. *Two principally polarized simple abelian varieties $(\mathbb{C}^n/\Phi(\mathfrak{a}), \xi_1)$ and $(\mathbb{C}^n/\Phi(\mathfrak{b}), \xi_2)$ of the same type are isomorphic if and only if we can find an element $\gamma \in F$ such that*

1. *$\gamma\mathfrak{a} = \mathfrak{b}$ and*
2. *$\xi_1 = \gamma\bar{\gamma}\xi_2$.*

Proof. This follows directly from Theorem 2 and [4, Section 3.5.2]. See also [12, Theorem 3.19]. □

Corollary 1. *Two polarizations on $\mathbb{C}^n/\Phi(\mathfrak{a})$ of the same simple type given by ξ_1 and ξ_2 give isomorphic abelian varieties if and only if $\xi_1 = u\bar{u}\xi_2$ for some unit $u \in \mathcal{O}_F^*$.*

We have now shown enough to see that the following is a valid algorithm for finding all principally polarized abelian varieties with CM by the ring of integers of a given simple CM field.

Algorithm 1. *To find all non-isomorphic principally polarized abelian varieties with CM by $\mathcal{O}_F$:*

1. *Find all ideal classes $\mathfrak{A}$ such that $\mathfrak{A}\overline{\mathfrak{A}}$ is the ideal class of the codifferent$\mathfrak{D}_{F/\mathbb{Q}}^{-1}$.*
2. *Find a set of coset representatives of the units in $\mathcal{O}_{F^+}$ modulo norms of units of $\mathcal{O}_F$.*
3. *For each ideal class found in 1 pick an ideal $\mathfrak{a}$ and find a generator b of $\mathfrak{D}_{F/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}}$.*
4. *For each ideal class in step 3, if there exists a unit u in $\mathcal{O}_F$ such that $ub = -\overline{ub}$, set $\xi_0 = (ub)^{-1}$ and go to the next step.*
5. *For each unit u^+ found in 2, choose a type Φ such that if $\xi = u^+\xi_0$ then $\mathrm{Im}(\phi_i(\xi)) > 0$ for each $\phi_i \in \Phi$.*
6. *ξ now defines a principal polarization of type Φ on $\mathbb{C}^n/\Phi(\mathfrak{a})$, and we can compute the corresponding element τ of the Siegel upper half-space $\mathfrak{h}_n$.*

Proof. By Theorem 1 and Theorem 2 we see that any torus with CM by the ring of integers of F is given by $\mathbb{C}^n/\Phi(\mathfrak{a})$ for one $\mathfrak{a}$ from each ideal class $\mathfrak{A}$. By Theorem 3 only a torus coming from an ideal class $\mathfrak{A}$ such that $\mathfrak{A}\overline{\mathfrak{A}}$ is the ideal class of the codifferent can admit a Riemann form. This is not a sufficient condition, but if some $\mathfrak{a} \in \mathfrak{A}$ gives a torus admitting a Riemann form, then by Theorem 5 any $\mathfrak{a} \in \mathfrak{A}$ will (and they will give isomorphic polarized abelian varieties).

Step 4 now checks the sufficient condition of Theorem 3 for the ideal $\mathfrak{a}$. Notice that (for now, in the case of a degree 4 field) we can decide whether such a unit exists by a finite procedure. Indeed, let u_0 be a primitive root of unity in F and u_1 a fundamental unit. Find k and h such that $b/\overline{b} = u_0^k$ and $u_1/\overline{u_1} = u_0^h$, and set $u = u_0^{d_1} u_1^{d_2}$. Then finding u such that $ub = -\overline{ub}$ is the same as finding d_1 and d_2 such that

$$2d_1 + hd_2 \equiv m - k \bmod 2m,$$

where $2m$ is the number of roots of unity in F. The same idea will clearly also work for larger CM fields. Theorem 4 just says that we will be able to find such a unit for *some* ideal class $\mathfrak{A}$.

The unit found in step 4 is clearly only unique up to a unit in F^+. On the other hand Corollary 1 says that we need not change ξ by the norm of a unit from F. This shows that step 5 will produce all the principal polarizations on all tori with CM by the ring of integers in F. □

Note that this algorithm might find a single polarized abelian variety more than once. Indeed, it is not clear when two polarized abelian varieties of *different types* are isomorphic. In particular, if we change ξ by a unit that is not totally positive, we still get a principal polarization, but with a different type. We only consider the following case. Here, besides a bar, ρ also denotes complex conjugation.

Proposition 1. *Let $\mathbb{C}^g/\Phi(\mathfrak{a})$ with polarization given by ξ be the canonically principally polarized Jacobian of a curve defined over a real number field. Then $\mathbb{C}^g/\rho\Phi(\mathfrak{a})$ with polarization given by $-\xi$ gives the same polarized abelian variety.*

Proof. The essential ingredient is [4, Proposition 3.5.4]. We use the notation there. First we show that if $(A, \mathcal{C})$ is of type $(K, \Phi, \mathfrak{a}, \xi)$ with respect to θ then $(A^\rho, \mathcal{C}^\rho)$ is of type $(K, \rho\Phi, \mathfrak{a}, -\xi)$ with respect to $\theta^\times$. Here $\theta^\times(z) = \overline{\theta(\overline{z})}$. Except for the polarization, this follows directly from the definitions. For the polarization, recall that by [4, Proposition 3.5.4] the Riemann form E_ρ on $\mathbb{C}^g/\rho\Phi(\mathfrak{a})$ that corresponds to $E(\Phi(\alpha), \Phi(\beta)) = \mathrm{tr}_{F/\mathbb{Q}}(\xi\overline{\alpha}\beta)$ on $\mathbb{C}^g/\Phi(\mathfrak{a})$ satisfies

$$\begin{aligned} E_\rho(\rho\Phi(\alpha), \rho\Phi(\beta)) &= -E(\Phi(\alpha), \Phi(\beta)) \\ &= \mathrm{tr}_{F/\mathbb{Q}}((-\xi)\overline{\alpha}\beta) \end{aligned}$$

This shows that $(A^\rho, \mathcal{C}^\rho)$ has the Riemann form given by $-\xi$. Note that this first part of the proposition is also a special case of [4, Theorem 7.3.1].

If A is the Jacobian of a curve C defined over a real number field, then A is defined over the same number field and therefore A is isomorphic to A^ρ. Recall that the canonical polarization of a Jacobian is defined by the theta divisor, which is $\{\sum_{i=1}^{g-1} P_i - (g-1)O | P_i \text{ in } C\}$ for some fixed $O \in C$ rational over the real number field. Complex conjugation clearly fixes this divisor, and so $(A, \mathcal{C})$ equals $(A^\rho, \mathcal{C}^\rho)$. □

4. Constructing a curve with a given Jacobian

In this section we want to find a genus two curve that has its Jacobian equal to one of the abelian varieties we found in the previous section.

The principally polarized abelian varieties we constructed in the previous section are 2 dimensional and simple. This means that the abelian surface is not isogenous (and in particular not isomorphic) to the product of two elliptic curves. This in turn means that the abelian surface is the Jacobian of a non-singular genus two curve (see [5, Corollary 11.8.2 a)]). Any non-singular genus two curve is hyperelliptic and can be put into Rosenhain normal form

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

This of course is rather abstract, but there is an explicit method for computing a Rosenhain normal form for a given element of the Siegel upper half-space. This is done with the use of theta functions and Thomae's identities. We will just give the relevant formulas, but the interested reader can consult [8], [13]. The higher dimensional theta function with characteristic is defined as follows.

For column vectors $c', c'' \in \mathbb{R}^{2g}$, $z \in \mathbb{C}^g$ and $\tau \in \mathfrak{h}_n$, the classical multi-variable theta function is

$$\theta[{}^tc'; {}^tc''](^tz, \tau) = \sum_{m \in \mathbb{Z}^g} \exp(\pi i\, {}^t(m+c')\tau(m+c') + 2\pi i\, {}^t(m+c')(z+c'')).$$

Thomae's identities relate the λ's in the Rosenhain normal form to theta functions evaluated at $z = 0$. There is some freedom in the choice of characteristics, but one possibility is the following. Set

$$\begin{aligned}
\vartheta_1 &= \theta([0,0;1/2,0],[0,0],\tau),\\
\vartheta_2 &= \theta([0,0;1/2,1/2],[0,0],\tau),\\
\vartheta_3 &= \theta([0,1/2;1/2,0],[0,0],\tau),\\
\vartheta_4 &= \theta([1/2,0;0,0],[0,0],\tau),\\
\vartheta_5 &= \theta([1/2,0;0,1/2],[0,0],\tau),\\
\vartheta_6 &= \theta([1/2,1/2;0,0],[0,0],\tau)],
\end{aligned}$$

where τ is an element of Siegel upper-half space found above. Then

$$\lambda_1 = \frac{-\vartheta_1^2\vartheta_3^2}{\vartheta_6^2\vartheta_4^2}, \qquad \lambda_2 = \frac{-\vartheta_2^2\vartheta_3^2}{\vartheta_6^2\vartheta_5^2}, \qquad \lambda_3 = \frac{-\vartheta_2^2\vartheta_1^2}{\vartheta_4^2\vartheta_5^2}.$$

Of course this curve is probably not defined over the rationals. Furthermore we can only compute numerical approximations to the λ's. If the curve can be defined over the rationals, the λ's will be algebraic numbers, and we might be able to recognize the numeric approximations as such. In that case we might then be able to find a linear transformation that results in a curve defined over the rationals. In some of the simpler cases this method works, but in general we need more sophisticated machinery.

5. When is a genus two curve defined over the rationals

An elliptic curve is defined over the rationals if and only if its j invariant is rational. We might ask whether a similar thing happens for genus two curves. Indeed this turns out to be the case, but the picture is somewhat more complicated. Igusa defined three absolute invariants i_1, i_2 and i_3 for genus two curves analogous to the j invariant for elliptic curves. They have the property that if these invariants agree for two curves, the curves must be isomorphic over $\mathbb{C}$. Unfortunately it is not true that if these invariants are rational the curve can be defined over the rationals. Recently Mestre showed how to decide whether a curve with given Igusa invariants can be defined over the rationals.

The Igusa invariants are defined for a hyperelliptic curve

$$y^2 = f(x),$$

where $f(x)$ is a sextic with roots α_i, $i = 1, 2, \ldots, 6$, and leading term a_6. We first define the so-called integral invariants. To simplify notation we write (ij) for $\alpha_{k_i} - \alpha_{k_j}$. The integral invariants are

$$\begin{aligned} I_2 &= a_6^2 \sum_{15} (12)^2(34)^2(56)^2, \\ I_4 &= a_6^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\ I_6 &= a_6^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \\ I_{10} &= a_6^{10} \prod_{i<j} (ij)^2. \end{aligned}$$

where the subscript on the sums gives the number of possible combinations to sum over. The (absolute) Igusa invariants are now defined by

$$\begin{aligned} i_1 &= I_2^5 / I_{10}, \\ i_2 &= I_2^3 I_4 / I_{10}, \\ i_3 &= I_2^2 I_6 / I_{10}. \end{aligned}$$

In case the hyperelliptic curve is given in the form $y^2 = f(x)$ where $f(x)$ is a quintic, we can think of it as a sextic with one root at infinity. Then, for purposes of computing the Igusa invariants, we follow the convention that in the definition of the integral invariants any term of the form $\alpha_i - \infty$ equals 1.

As already mentioned, these invariants agree for two curves if and only if the two curves are isomorphic [3, Corollary on p. 632]. Note that the integral invariants are symmetric functions of the roots and these invariants can therefore be expressed as rational functions of the coefficients of $f(x)$. In particular we see that the Igusa invariants are rational if the curve can be defined over the rationals. Unfortunately the converse is not true. By using the Igusa invariants and Proposition 1 we can reject some $\tau \in \mathfrak{h}$ as not belonging to curves defined over the rationals. Indeed if τ and τ' correspond to the same torus but with polarizations given by ξ and $-\xi$, then if their Igusa invariants are not equal the proposition says that they cannot come from a curve defined over the rationals. Of course in general we need better methods.

Mestre [7] gave a method for deciding whether a curve with given Igusa invariants can be defined over a particular field.

Mestre constructs a conic L and a cubic M in $\mathbb{P}^2$ with coefficients in terms of i_1, i_2 and i_3.

For $v \in \mathbb{P}^2$ the conic L is defined by

$${}^t v L v = 0,$$

where L is given by

$$\begin{pmatrix} x+6y & 6x^2+2y & 2z \\ 6x^2+2y & 2z & 9x^3+4xy+6y^2 \\ 2z & 9x^3+4xy+6y^2 & 6x^2y+2y^2+3xz \end{pmatrix}$$

and

$$\begin{aligned} x &= \frac{8}{225}\frac{20i_2+i_1}{i_1}, \\ y &= \frac{16}{3375}\frac{-600i_3+i_1+80i_2}{i_1}, \\ z &= \frac{-64}{253125}\frac{1}{i_1^2}(-10800000i_1-9i_1^2-700i_2i_1 \\ &\quad +3600i_3i_1+12400i_2^2-48000i_2i_3). \end{aligned}$$

Defining the cubic is somewhat more involved. First set

$$\begin{aligned} a &= \frac{-I_2}{120}, \\ b &= \frac{I_2^2+20I_4}{135000}, \\ c &= \frac{-I_2^3-80I_2I_4+600I_6}{121500000}, \\ d &= \frac{-9I_2^5-700I_2^3I_4+12400I_2I_4^2+3600I_2^2I_6-48000I_4I_6-10800000I_{10}}{49207500000000}. \end{aligned}$$

These are the Clebsch invariants. For $v \in \mathbb{P}^2$ set

$$\begin{aligned} x_1 &= a^6I_{10}^4v_1, \\ x_2 &= -\frac{I_{10}^5i_1v_2}{2^{15}3^55^5}, \\ x_3 &= \frac{2^{60}3^{20}5^{20}a^{24}v_3}{i_1^4}. \end{aligned}$$

Then Mestre's cubic is defined to be

$$M(v) = \sum_{1\le i,j,k\le 3} a_{ijk}x_ix_jx_k = 0,$$

where the a_{ijk} are given by

$$\begin{aligned} a_{111} &= 8(a^2c-6bc+9d), \\ a_{112} &= 4(2b^3+4abc+12c^2+3ad), \\ a_{113} &= 4(ab^3+\tfrac{4}{3}a^2bc+4b^2c+6ac^2+3bd), \\ a_{122} &= a_{113}, \\ a_{123} &= 2(2b^4+4ab^2c+\tfrac{4}{3}a^2c^2+4bc^2+3abd+12cd), \\ a_{133} &= 2(ab^4+\tfrac{4}{3}a^2b^2c+\tfrac{16}{3}b^3c+\tfrac{26}{3}abc^2+8c^3+3b^2d+2acd), \\ a_{222} &= 4(3b^4+6ab^2c+\tfrac{8}{3}a^2c^2+2bc^2-3cd), \\ a_{223} &= 2(-\tfrac{2}{3}b^3c-\tfrac{4}{3}abc^2-4c^3+9b^2d+8acd), \\ a_{233} &= 2(b^5+2ab^3c+\tfrac{8}{9}a^2bc^2+\tfrac{2}{3}b^2c^2-bcd+9d^2), \\ a_{333} &= -2b^4c-4ab^2c^2-\tfrac{16}{9}a^2c^3-\tfrac{4}{3}bc^3+9b^3d+12abcd+20c^2d. \end{aligned}$$

It can be checked that the cubic can be given entirely in terms of the Igusa invariants. Our definition of Mestre's cubic is a multiple of Mestre's definition, but as we only care about the zeros it doesn't matter.

Mestre showed that a genus 2 curve with Igusa invariants i_1, i_2 and i_3 is defined over the number field F if and only if the conic L has a F-rational point in $\mathbb{P}^2_F$. By the Hasse-Minkowski theorem (see [9]) it is easy to decide whether a conic has a rational point.

In fact, if the conic has a rational point we can find an explicit curve defined over the rationals with the given Igusa invariants. That is because Mestre showed that the Weierstrass points of such a curve are given by the points of intersection of the conic L and the cubic M. This means we can do the following. If there is a rational point on the conic there are infinitely many, and we can parametrize them by $v_1 = f_1(t)$, $v_2 = f_2(t)$ and $v_3 = f_3(t)$ where the f_i are quadratic polynomials with rational coefficients. If we substitute this into the cubic M we get a polynomial $f(t)$ of degree 6. Then $y^2 = f(t)$ is a rational equation for the curve.

6. Notes on implementation

The algorithm for finding elements of the Siegel upper half-space was implemented in the Pari-GP package. In particular the package allows one to find the ring of integers in a number field and to compute in such a ring, including finding prime ideal decompositions, units, Galois elements, etc. There are also tables of number fields available (anonymous ftp: `megrez.math.u-bordeaux.fr /pub/numberfields/`). The table of quartic CM fields we used was extracted from these tables.

To compute the Igusa invariants corresponding to a given element of the Siegel upper half-space, we used both Mathematica and Pari-GP. The computation of theta function values can be done by summing their defining series. As the terms are exponential, the series converges very quickly. Unfortunately, in some cases this was still not practical—many of the τ in the Siegel upper half-space had very small imaginary part, so even though the convergence is fast we still would have needed to sum a prohibitively large number of terms. To overcome this problem we first applied a symplectic matrix to the τ's in order to maximize the imaginary part. This can be done analogously to the well-known method of moving an element of the complex upper half-space into the fundamental domain. We simply applied a generator from [1, Theorem 1] for $\mathrm{Sp}_2(\mathbb{Z})$ that increases the imaginary part of τ. Then we moved τ back into the center strip and Minkowski-reduced τ. We repeated this procedure until none of the generators increased the imaginary part of τ.

The Igusa invariants were computed accurate to approximately 300 decimal places. If they were not complex we tried to recognize them as rational numbers by computing their continued fraction expansions and stopping as soon as at least the first 90% of the digits of the fraction agreed with those of the real number. If the corresponding rational had less than 125 digits in the numerator we assumed that the real number was rational. In fact the largest rational Igusa invariant we found had only 59 digits in the numerator.

To test whether a curve with rational Igusa invariants can be defined over the rationals (and then to find such a curve) we need to find points on Mestre's conic. This is easy in theory but in practice it can lead to hard problems, in particular the need to factor some large integers. Fortunately, for our examples the largest factorizations were right at the limit of what can be done in reasonable time.

All the curves that had rational Igusa invariants turned out to be definable over the rationals.

Once the point on the conic was found, it is an easy matter to substitute into Mestre's cubic to find a rational equation for the curve. Unfortunately the equation for the curve can be huge. The worst case for our examples gave a sextic with coefficients with more that 5000 digits. To reduce these equations to a reasonable size we used the following algorithm. First try to remove all powers of 30 from the discriminant. If $f(x) \equiv (x-a)^6 \bmod p$ for some prime p, then p^{30} divides the discriminant. In all our examples the converse was also true. It is easy to check that if $f(x) \equiv (x-a)^6 \bmod p$ then $f(px+a)/p^6$ has discriminant with the power of p reduced by 30 (and still has integral coefficients). In this way we were able to reduce all powers of primes to less than 30. After the discriminant is reduced we try to apply a rational linear fractional transformation to $f(x)$ in order to decrease the size of the coefficients. It was enough to repeatedly apply a translation $f(x) \to f(x \pm 1)$ or an inversion combined with a translation $f(x) \to f(1/(x \pm 1))(x \pm 1)^6$ to reduce the size of the coefficients.

As explained above, we searched only quartic CM fields that were either cyclic or dihedral. We searched for all cyclic quartic CM fields up to discriminant 10^6; there are 54 such fields. Note that the largest discriminant of a cyclic quartic CM field with class number 1 or 2 is 240737 ([10],[2]). We searched all dihedral quartic CM fields up to discriminant 79525 (307 fields) and those with 6 or less different polarized abelian varieties up to discriminant 830816 (147 more fields). At this point the computation just to check the number of polarizations became too lengthy, so we further restricted consideration to fields with class number at most 4. Nearly all fields with at most 6 polarizations up to this point satisfied this condition anyway. Under this further restriction we went up to discriminant 10^6 (14 more fields). Note that by [6] the largest discriminant of a dihedral quartic CM field with class number 1 is 756605.

7. The results

The results are contained in Table 1. Of these Spallek [12] has also found curves (with the same Igusa invariants as ours) corresponding to the fields $\mathbb{Q}(\sqrt{-2+\sqrt{2}})$ and $\mathbb{Q}(\sqrt{-5+\sqrt{5}})$.

A few things are worth pointing out.

1. Note that all the fields in the table have class number either 1 or 2.
2. The fields in the table are all cyclic.
3. There exist exactly 7 class number 1 quartic cyclic CM fields (see [10]). We find one and only one curve with CM by each of these fields. (Note that there are lots of dihedral CM fields with class number 1, but as noted none of them gave a curve defined over the rationals).
4. There exist exactly 8 class number 2 quartic cyclic CM fields (see [2]). We find exactly two (non-isomorphic) curves with CM by each of these fields except the two fields $\mathbb{Q}(\sqrt{-6+2\sqrt{2}})$ and $\mathbb{Q}(\sqrt{-119+28\sqrt{17}})$, for which we find no curve. For each of these fields we got two sets of Igusa invariants. We were able to recognize them as non-rational elements of a quadratic field (accurate to about 600 places). In the first case the one set of invariants was the conjugates in $\mathbb{Q}(\sqrt{2})$ of the other set. The same happened for the other pair of invariants, but in $\mathbb{Q}(\sqrt{17})$.

TABLE 1. Genus 2 CM curves defined over the rationals

<table>
<tr><th>CM-field</th><th>i_1</th><th>i_2</th><th>i_3</th></tr>
<tr><td>$\mathbb{Q}(\zeta_5)$</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td></td><td colspan="3">$y^2 = x^5 - 1$</td></tr>
<tr><td>$\mathbb{Q}(\sqrt{-2+\sqrt{2}})$</td><td>$2^7 3^{15}$</td><td>$2^5 3^{11} 5$</td><td>$2^4 3^9 31$</td></tr>
<tr><td></td><td colspan="3">$y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$</td></tr>
<tr><td>$\mathbb{Q}(\sqrt{-13+2\sqrt{13}})$</td><td>$2^{28}$</td><td>$-2^{20} 5$</td><td>$-2^{14} 3 \cdot 41$</td></tr>
<tr><td></td><td colspan="3">$y^2 = -11x^6 - 2x^5 - x^4 + 4x^3 + 7x^2 - 6x + 1$</td></tr>
<tr><td>$\mathbb{Q}(\sqrt{-5+\sqrt{5}})$</td><td>$2 \cdot 3^{10} 5^5 7^5$</td><td>$2 \cdot 3^{10} 5^5 7^3$</td><td>$2 \cdot 3^7 5^3 7^3 193$</td></tr>
<tr><td></td><td colspan="3">$y^2 = -4x^5 + 30x^3 - 45x + 22$</td></tr>
<tr><td></td><td>$\frac{2 \cdot 3^{10} 5^5 719^5}{11^{12}}$</td><td>$\frac{2 \cdot 3^8 5^5 719^3}{11^8}$</td><td>$\frac{2 \cdot 3^7 5^5 719^3}{11^8}$</td></tr>
<tr><td></td><td colspan="3">$y^2 = -8x^6 + 52x^5 - 250x^3 + 321x + 131$</td></tr>
<tr><td>$\mathbb{Q}(\sqrt{-65+26\sqrt{5}})$</td><td>$\frac{2^{28} 3^{10} 5^5 79^5}{11^{12}}$</td><td>$\frac{2^{20} 3^8 5^5 79^3}{11^6}$</td><td>$\frac{2^{14} 3^7 5^3 79^2 7457}{11^5}$</td></tr>
<tr><td></td><td colspan="3">$y^2 = -8x^6 - 64x^5 + 1120x^4 + 4760x^3 - 48400x^2 + 22627x - 91839$</td></tr>
<tr><td></td><td>$\frac{-2^{28} 3^{15} 5^5 54799^5}{31^{12} 41^{12}}$</td><td>$\frac{-2^{22} 3^{11} 5^5 54799^3}{31^8 41^8}$</td><td>$\frac{-2^{15} 3^9 5^4 54799^2 184370689}{31^8 41^8}$</td></tr>
<tr><td></td><td colspan="3">$y^2 = 79888x^6 + 293172x^5 - 348400x^3 - 29744x + 103259$</td></tr>
<tr><td>$\mathbb{Q}(\sqrt{-29+2\sqrt{29}})$</td><td>$\frac{2^{38} 3^{10} 11^5}{5^{12}}$</td><td>$\frac{-2^{26} 3^8 11^3}{5^6}$</td><td>$\frac{-2^{18} 3^7 11^2 2927}{5^6}$</td></tr>
<tr><td></td><td colspan="3">$y^2 = 289x^6 + 242x^5 - 225x^4 - 92x^3 + 87x^2 - 42x - 43$</td></tr>
</table>

Table 1. (Continued)

CM-field	i_1	i_2	i_3
$\mathbb{Q}(\sqrt{-85+34\sqrt{5}})$	$\frac{2^{33}3^{10}5^{5}19^{5}521^{5}}{71^{12}}$	$\frac{2^{23}3^{10}5^{5}19^{5}521^{3}}{71^{8}}$	$\frac{2^{16}3^{7}5^{4}19^{3}521^{2}755777339}{71^{8}}$
	$y^2 = -584x^6 - 4020x^5 + 28860x^4 + 130240x^3 - 514920x^2 - 190244x - 289455$		
	$\frac{-2^{28}3^{10}5^{5}19^{10}687061^{5}}{11^{12}41^{12}61^{12}}$	$\frac{-2^{20}3^{8}5^{5}19^{6}687061^{3}}{11^{6}41^{8}61^{8}}$	$\frac{-2^{14}3^{9}5^{3}19^{4}401\cdot 687061^{2}208218677}{11^{6}41^{8}61^{8}}$
	$y^2 = -444408x^6 + 6986711x^5 + 44310170x^4 - 582800x^3 + 2656360x^2 - 8866880x + 2160600$		
$\mathbb{Q}(\sqrt{-37+6\sqrt{37}})$	$\frac{-2^{33}1319^{5}}{3^{7}11^{12}}$	$\frac{-2^{23}5\cdot 1319^{3}}{3^{3}11^{7}}$	$\frac{-2^{16}1319^{2}716747}{3^{4}11^{7}}$
	$y^2 = -544x^6 - 228x^5 + 168x^4 + 680x^3 + 36x^2 + 396x - 567$		
$\mathbb{Q}(\sqrt{-10+5\sqrt{2}})$	$\frac{2^{7}3^{10}5^{10}491^{5}577^{5}}{7^{12}23^{12}}$	$\frac{2^{5}3^{8}5^{7}13\cdot 491^{3}577^{3}2293}{7^{8}23^{8}}$	$\frac{2^{4}3^{7}5^{5}31\cdot 491^{2}577^{2}10419950621}{7^{8}23^{8}}$
	$y^2 = 8x^6 - 530x^5 - 160x^4 + 64300x^3 + 265420x^2 - 529x$		
	$\frac{2^{7}3^{10}5^{5}11^{5}2687^{5}8699^{5}}{7^{12}17^{12}23^{12}}$	$\frac{2^{5}3^{8}5^{4}11^{3}449\cdot 2687^{3}8699^{3}}{7^{8}17^{7}23^{8}}$	$\frac{2^{4}3^{7}5^{3}11^{2}13\cdot 2687^{2}7451\cdot 8699^{2}9852653}{7^{8}17^{7}23^{8}}$
	$y^2 = -4116x^6 + 64582x^5 - 139790x^4 - 923200x^3 - 490750x^2 + 233309x + 9347$		
$\mathbb{Q}(\sqrt{-65+10\sqrt{13}})$	$\frac{2^{28}5^{5}7^{5}}{3^{7}}$	$\frac{2^{21}5^{4}7^{3}19}{3^{3}}$	$\frac{2^{15}5^{3}7^{3}19\cdot 239}{3^{4}}$
	$y^2 = 1183x^6 + 1560x^5 + 1560x^4 - 1040x^3 + 36x$		
	$\frac{2^{43}5^{10}11^{5}29^{5}}{3^{7}53^{12}}$	$\frac{-2^{29}5^{7}11^{3}29^{3}}{3^{3}53^{8}}$	$\frac{-2^{20}5^{5}11^{2}29^{2}2490497}{3^{4}53^{8}}$
	$y^2 = -10584x^6 - 5940x^5 + 18180x^4 + 3200x^3 - 18960x^2 - 6508x + 3465$		

Table 1. (Continued)

CM-field	i_1	i_2	i_3
$\mathbb{Q}(\sqrt{-13+3\sqrt{13}})$	$\frac{2\cdot 7^{10}11^{5}21059^{5}}{3^{7}23^{12}}$	$\frac{2\cdot 5\cdot 7^{7}11^{3}8387\cdot 21059^{3}}{3^{3}23^{8}}$	$\frac{2\cdot 7^{6}11^{2}21059^{2}71347\cdot 739363}{3^{4}23^{8}}$
	$y^2=-243x^6+2223x^5-1566x^4-19012x^3+903x^2+19041x-5882$		
	$\frac{2\cdot 11^{5}53^{5}6719^{5}30113^{5}}{3^{7}23^{12}131^{12}}$	$\frac{2\cdot 5\cdot 11^{3}53^{3}6719^{3}7229\cdot 30113^{3}}{3^{3}23^{8}131^{8}}$	$\frac{2\cdot 11^{2}19\cdot 53^{2}6719^{2}30113^{2}237589628623651}{3^{4}23^{8}131^{8}}$
	$y^2=-70399443x^6+36128207x^5+262678342x^4-48855486x^3-112312588x^2+36312676x$		
$\mathbb{Q}(\sqrt{-53+2\sqrt{53}})$	$\frac{2^{28}3^{15}5805193^{5}}{17^{12}29^{12}}$	$\frac{-2^{23}3^{11}5\cdot 19\cdot 5805193^{3}}{17^{7}29^{8}}$	$\frac{-2^{15}3^{9}19\cdot 331\cdot 5805193^{2}68436029}{17^{7}29^{8}}$
	$y^2=50091x^6-54865x^5-129108x^4+158576x^3+110664x^2-180624x-112360$		
$\mathbb{Q}(\sqrt{-61+6\sqrt{61}})$	$\frac{-2^{28}7^{15}39079^{5}}{3^{19}5^{12}41^{12}}$	$\frac{-2^{24}7^{9}39079^{3}}{3^{11}5^{6}41^{8}}$	$\frac{-2^{15}7^{7}79\cdot 39079^{2}19530317}{3^{12}5^{6}41^{8}}$
	$y^2=-103615x^6-41271x^5+17574x^4+197944x^3+67608x^2-103680x-40824$		

Acknowledgments

I would like to thank Eyal Goren and Xiangdong Wang for some helpful discussions.

Added in proof

After this paper was accepted, Bjorn Poonen pointed out to me that it is a theorem that a genus 2 curve with CM by a quartic CM field with a dihedral Galois group of order 8 cannot be defined over the rationals. See Proposition 5.17 in G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* (Publications of the Mathematical Society of Japan, 11, Kann Memorial Lectures, 1), Princeton University Press, Princeton, NJ, 1994. MR **95e:**11048

References

1. E. Gottschling. Explizite bestimmung der randflächen des fundamentalbereiches der modulgruppe zweiten grades. *Math. Annalen*, 138:103–124, 1959. MR **21:**5748
2. K. Hardy, R. H. Hudson, D. Richman, and K. S. Williams. The determination of all imaginary cyclic quartic fields with class number 2. *Trans. Amer. Math. Soc.*, 311(1):1–55, 1989. MR **89f:**11148
3. J. I. Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math.*, 72(3):612–649, 1960. MR **22:**5637
4. S. Lang. *Complex Multiplication*. Springer-Verlag, 1983. MR **85f:**10042
5. H. Lange and C. Birkenhake. *Complex Abelian Varieties*. Springer-Verlag, 1992. MR **94j:**14001
6. S. Louboutin and R. Okazaki. Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one. *Acta Arith.*, 67(1):47–62, 1994. MR **95g:**11107
7. J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective Methods in Algebraic Geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.* Birkhäuser, 1991, pp. 313–334. MR **92g:**14022
8. D. Mumford. *Tata Lectures on Theta II*, volume 43 of *Progr. Math.* Birkhäuser, 1984. MR **86b:**14017
9. J.-P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1973. MR **49:**8956
10. B. Setzer. The determination of all imaginary, quartic, abelian number fields with class number 1. *Math. Comp.*, 35(152):1383–1386, 1980. MR **81k:**12005
11. G. Shimura and Y. Taniyama. *Complex Multiplication of Abelian Varieties*. The Mathematical Society of Japan, 1961. MR **23:**A2419
12. A.-M. Spallek. Kurven vom geschlecht 2 und ihre anwendung in public-key-kryptosystemen. Preprint 18, Universität GH Essen, Ellernstraße 29, 45326 Essen, Germany, 1994.
13. P. B. van Wamelen. Equations for the algebraic Jacobian of a hyperelliptic curve. *Submitted to Trans. Amer. Math. Soc.*
14. L. C. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, 1982. MR **85g:**11001

Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803-4918

E-mail address: `wamelen@math.lsu.edu`