MATHEMATICS OF COMPUTATION
Volume 68, Number 228, Pages 1663–1677
S 0025-5718(99)01101-1
Article electronically published on May 17, 1999

PROVING THAT A GENUS 2 CURVE HAS COMPLEX MULTIPLICATION

PAUL VAN WAMELEN

Abstract. Recently examples of genus 2 curves defined over the rationals were found which, conjecturally, should have complex multiplication. We prove this conjecture. This involves computing an explicit representation of a rational map defining complex multiplication.

1. Introduction

In [5] 18 non-trivial genus 2 curves defined over the rationals are given, and it is conjectured that these curves have complex multiplication. In this paper we will prove this conjecture. The idea is to compute a CM-morphism explicitly. This will be achieved by computing such a morphism numerically to high precision and then guessing exact values for the coefficients of this morphism. It can then be checked that these exact functions do define complex multiplication. The morphism is computed numerically by going through the analytic representation of the Jacobian of the curve — we compute the necessary integrals to go from the abelian variety to the torus, multiply by the matrix giving the complex representation of the morphism, and then use theta functions to go back to the abelian variety.

2. Definitions

Recall that any genus two curve is hyperelliptic. Let C be the genus 2 hyperelliptic curve represented by

$$y^2 = \prod_{i=1}^{5}(x - a_i) = f(x),$$

where the a_i are distinct points in $\mathbb{C}$. We assume that the curve is defined over $\mathbb{Q}$, so $f(x) \in \mathbb{Q}[x]$.

If we regard C as a Riemann surface, the a_i are the branch points of the double cover of $\mathbb{P}$ by C. Let $\{A_1, A_2, B_1, B_2\}$ form a symplectic basis for the homology of C. Let A_1 be a clockwise path around a_1 and a_2, A_2 a clockwise path around a_3 and a_4, B_1 around a_2, a_3, a_4 and a_5 and B_2 around a_4 and a_5. The only intersections of these paths are A_i intersecting B_i, $i = 1, 2$, in one point and with intersection multiplicity one.

Received by the editor December 16, 1997.
1991 *Mathematics Subject Classification.* Primary 14-04; Secondary 14K22.
Key words and phrases. CM-curves, complex multiplication, genus 2 curves.
This work was partially supported by grant LEQSF(1995-97)-RD-A-09 from the Louisiana Educational Quality Support Fund.

Let $\phi_1 = dx/y$ and $\phi_2 = xdx/y$. Then $\{\phi_1, \phi_2\}$ forms a basis for the holomorphic 1-forms on C. We define the period matrix P by

$$P = \begin{pmatrix} \int_{B_1} \phi_1 & \int_{B_2} \phi_1 & \int_{A_1} \phi_1 & \int_{A_2} \phi_1 \\ \int_{B_1} \phi_2 & \int_{B_2} \phi_2 & \int_{A_1} \phi_2 & \int_{A_2} \phi_2 \end{pmatrix}.$$

Let ω_1 and ω_2 be the two 2×2 matrices such that $P = (\omega_1, \omega_2)$.

If we define τ to be the matrix $\omega_2^{-1}\omega_1$, then τ is in $\mathfrak{h}_2$, the Siegel upper half-space.

Let Λ be the free abelian group in $\mathbb{C}^2$ generated by the columns of P. Then Λ is a lattice in $\mathbb{C}^2$ and the Jacobian J of C is given by $\mathbb{C}^2/\Lambda$.

The Jacobian also has the structure of an abelian variety. Let α be an endomorphism of this abelian variety. We will assume that C has complex multiplication by the full ring of integers of a cyclic quartic CM-field, so we fix an isomorphism between $\mathrm{End}(J) \otimes \mathbb{Q}$ and a cyclic quartic CM-field K. We will denote the real subfield of index 2 by K^+. Let $\tilde{\alpha}$ be the algebraic integer in K corresponding to α under this isomorphism. We will assume that $\tilde{\alpha}$ is not in the real subfield K^+.

If we think of J as $\mathbb{C}^2/\Lambda$, then α induces a linear map from $\mathbb{C}^2$ to itself. We denote the 2×2 matrix giving this map by $\overline{\alpha}$. As $\overline{\alpha}$ represents an endomorphism of $\mathbb{C}^2/\Lambda$, there exists a 4×4 rational integer matrix M such that

$$\overline{\alpha}P = PM. \tag{1}$$

The minimum polynomial of M will now be an irreducible polynomial of degree 4 (defining the CM-field).

Recall that the Jacobian is the unique abelian variety birationally equivalent to the symmetric product of the curve with itself. For the rest of this paper we will denote by $P_1 + P_2$ the image of $P + \infty$ under the map induced on $C^{(2)}$ by α, where $P = (x, y)$, $P_i = (x_i, y_i)$, $i = 1, 2$.

Note that $x_1 + x_2$ and x_1x_2 can be considered as meromorphic functions on the curve. As these functions do not depend on the y-coordinate of P, we see that $x_1 + x_2$ and x_1x_2 are rational functions in x. As α is defined over K, we see that the coefficients of $x_1 + x_2$ and x_1x_2 as functions of x are in K.

3. Choosing an element of K to be used as $\tilde{\alpha}$

We plan to compute $x_1 + x_2$ and x_1x_2 explicitly for some algebraic integer $\tilde{\alpha}$ in $K \backslash K^+$. To minimize our work we would like to pick an $\tilde{\alpha}$ that will minimize the degree of the rational functions $x_1 + x_2$ and x_1x_2. An upper bound for the degree of these functions can be found in the following way. We will find an upper bound for the degrees of these functions as functions on C, then because x has degree 2 as a function on C we just divide by 2 to get the degrees of these functions as rational functions of x. Let X_1 and X_2 be the x-coordinate functions in $C \times C$, then recall that both of the functions on J corresponding to $X_1 + X_2$ and X_1X_2 have polar divisor 2Θ (where Θ denotes the theta divisor). The image of the embedding of C into J that maps P to the divisor class $P - \infty$ is exactly the theta divisor Θ. The degrees of $x_1 + x_2$ and x_1x_2 are given by the number of poles of these functions, and this is therefore equal to the number of points at which the functions $X_1 + X_2$ and X_1X_2 are infinite on the divisor $\alpha(\Theta)$. An upper bound for this number is the intersection multiplicity of $\alpha(\Theta)$ and 2Θ (it's only an upper bound, because some of the intersection points might also be intersection points with the zero divisor of $X_1 + X_2$ or X_1X_2). This intersection number is given by [3, Theorem 17.3]. Using the well-known fact that $(\Theta^2) = 2$, we get that an upper bound for the degrees of

the rational functions $x_1 + x_2$ and $x_1 x_2$ as functions of x are given by $\mathrm{tr}_{K^+/\mathbb{Q}}(\tilde{\alpha}\overline{\tilde{\alpha}})$, where the bar denotes complex conjugation.

For each curve we used Pari's `polred` function to find a "small" polynomial (with integer coefficients) to define the CM-field. Let z be a root of this polynomial. It turned out that if we then compute $\mathrm{tr}_{K^+/\mathbb{Q}}(\tilde{\alpha}\overline{\tilde{\alpha}})$ for $\tilde{\alpha} = q_0 + q_1 z_1 + q_2 z_2 + q_3 z_3$ with $\{1, z_1, z_2, z_3\}$ an integral basis and the q_i's small integers, the minimum was attained by $\tilde{\alpha} = z$ for each of our CM-fields.

4. Computing an approximation to $\overline{\alpha}$

If we suspect that a curve has CM by a certain CM-field, we can use Algorithm 1 in [5] to write down a complex torus with CM by the given field. Let the period matrix of this torus be P'. For this torus, denote the matrix corresponding to complex multiplication by α by $\overline{\alpha}'$. It is given by the image of $\tilde{\alpha}$ under the diagonal embedding of K using the type. For $\overline{\alpha}'$ we can write down the corresponding M' such that $\overline{\alpha}' P' = P' M'$; we can also compute $\tau' \in \mathfrak{h}_2$ corresponding to P' . We can compute approximations to the period matrix and τ of our curve by doing the integrals involved numerically. Now τ' and τ should be related by a symplectic matrix; that is, there should exist a symplectic matrix $S = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ such that $(a\tau + b)(c\tau + d)^{-1} = \tau'$. We can go about finding this matrix in two ways. The first is to move both these τ's into a fundamental domain by symplectic matrices. This can be done for the fundamental domain given in [2, Theorem 1] in a way similar to the well-known method for moving an element of the complex upper half-plane into the usual fundamental domain. The other method is to use the observation that the equation relating τ and τ' can be rewritten as $(a\tau + b) = \tau'(c\tau + d)$ and each of the 4 equations corresponding to the four entries of these matrices then gives us an integral linear dependency between certain entries of τ, entries of τ', and certain products of two such entries. We can try to find these linear dependencies by using an algorithm for finding integral linear dependencies between the elements of a set of complex numbers. These algorithms are usually based on the LLL algorithm; see for instance [1, Algorithm 2.7.4]. The coefficients will then lead to the symplectic matrix S we are looking for.

Once we have S it is a simple matter to find $\overline{\alpha}$ and M, we get

$$\overline{\alpha} = (\omega_1 c^t + \omega_2 d^t)\omega_2'^{-1}\overline{\alpha}'\omega_2'(\omega_1 c^t + \omega_2 d^t)^{-1},$$
$$M = S^t M' S^{t^{-1}}.$$

5. From the analytic to the algebraic Jacobian

For a point $v \in \mathbb{C}^2/\Lambda$ we can find its representation as an element of $C^{(2)}$ by using theta functions. For column vectors $c', c'' \in \mathbb{R}^{2g}$, $z \in \mathbb{C}^g$ and $\tau \in \mathfrak{h}_g$ the classical multi-variable theta function is given by

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

By choosing $k = 1$ and $V = \{1, 2, 3\}$ in Theorem IIIa.7.6 of [4] we get

$$(x_1 - a_1)(x_2 - a_1) = (a_1 - a_2)(a_1 - a_3)\left(\frac{\theta[1,0;1,1/2](0,\tau)\theta[1,1/2;1,1/2](z,\tau)}{\theta[1/2,0;1,1/2](0,\tau)\theta[1/2,1/2;1,1/2](z,\tau)}\right)^2;$$

with the same V and $k = 2$ we get

$$(x_1 - a_2)(x_2 - a_2) \\ = (a_1 - a_2)(a_2 - a_3)\left(\frac{\theta[1,0;3/2,1/2](0,\tau)\theta[1,1/2;3/2,1/2](z,\tau)}{\theta[1/2,0;1,1/2](0,\tau)\theta[1/2,1/2;1,1/2](z,\tau)}\right)^2,$$

where the theta functions are evaluated at $\tau = \omega_2^{-1}\omega_1$ and $z = \omega_2^{-1}v$. From these two equations we can now solve for x_1 and x_2.

6. Computing $x_1 + x_2$ and x_1x_2 numerically

Now suppose we have a genus two curve defined over the rationals and are given an approximation (to high precision) of $\overline{\alpha}$ as a 2×2 matrix. Then for a given point (x, y) on the curve C we can compute approximations for x_1 and x_2 as follows. The embedding of C in the (analytic) Jacobian is given by the vector of integrals

$$v = \begin{pmatrix} \int_x^\infty \frac{dx}{\sqrt{f(x)}} \\ \int_x^\infty \frac{xdx}{\sqrt{f(x)}} \end{pmatrix}.$$

We compute this numerically. To do so we use the value of y to give a choice for the sign of the square root, and then analytically continue this value along a path out to infinity. We now compute $z = \omega_2^{-1}(\overline{\alpha}v)$ and, using the method in the previous paragraph, compute x_1 and x_2.

7. The complex representation of α

The endomorphism α also induces an endomorphism of the holomorphic 1-forms on J, $\Gamma(J, \Omega^1_J)$. As $\Gamma(J, \Omega^1_J) \cong \Gamma(C, \Omega^1_C)$, we see that α induces a map from holomorphic 1-forms on C to holomorphic 1-forms on C. It can be shown that this map is given by

$$\begin{aligned} \frac{dx}{y} &\mapsto \frac{dx_1}{y_1} + \frac{dx_2}{y_2} = \frac{\alpha_{11} + \alpha_{12}x}{y}dx, \\ \frac{xdx}{y} &\mapsto \frac{x_1dx_1}{y_1} + \frac{x_2dx_2}{y_2} = \frac{\alpha_{21} + \alpha_{22}x}{y}dx. \end{aligned} \tag{2}$$

If we use this map as a change of variable in the integrals defining P, we see that we recover the expression (1). Indeed,

$$\overline{\alpha} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

We can get the columns of M by finding the images of each of A_1, A_2, B_1 and B_2 under the maps $P \mapsto P_1$ and $P \mapsto P_2$ and computing the linear combination of the basis elements homologous to the sum of these two images.

8. Guessing the exact values of $x_1 + x_2$ and x_1x_2

If we compute x_1 and x_2 at enough points x and to sufficient precision, we can solve a linear system in order to find approximations for the coefficients of the rational functions $x_1 + x_2$ and x_1x_2. If we have these coefficients to sufficient precision, we might be able to use an LLL type algorithm in order to recognize these approximate coefficients as exact elements of the CM-field.

In fact the following observation implies that we can get away with only having to recognize rational numbers.

The morphism α is defined over K. As the holomorphic 1-forms are defined over $\mathbb{Q}$ and as the matrix $\overline{\alpha}$ comes from the map induced on the holomorphic 1-forms of C by the morphism α, we see that the matrix $\overline{\alpha}$ has entries in K. As the curve is defined over $\mathbb{Q}$, we see that if σ is an element of the Galois group of K over $\mathbb{Q}$ then $\sigma(\alpha)$ is another endomorphism of the Jacobian, and that the corresponding matrix is just the matrix $\overline{\alpha}$ with σ applied to each of its entries. So if we know the coefficients of $\overline{\alpha}$ as exact elements of K, we can write down the 4 conjugates of $\overline{\alpha}$ and with the same procedure as in the previous paragraph we can compute the conjugates of the coefficients of the rational functions $x_1 + x_2$ and $x_1 x_2$.

Now let $\{1, \xi, \xi^2, \xi^3\}$ be a $\mathbb{Q}$-basis for K, σ_i, $i = 1, 2, 3, 4$, the elements of the Galois group, and let $\beta = q_1 + q_2\xi + q_3\xi^2 + q_4\xi^3$, for rational numbers q_i, be a variable element of K. Then we can write each of q_1, q_2, q_3 and q_4 as a rational linear combinations of the 16 expressions $\sigma_i(\beta)\xi^j$, $i = 1, 2, 3, 4$, $j = 0, 1, 2, 3$. So if we have approximations for all the conjugates of an element β of K (and ξ), we can compute approximations to the rational coefficients q_i. Now we guess exact values for these by using, say, continued fractions.

9. Proving that $x_1 + x_2$ and $x_1 x_2$ are correct

So we have now guessed an exact value for $x_1 + x_2$ and $x_1 x_2$. To prove that they are correct we will check whether they give the correct action on the holomorphic 1-forms. From the exact expressions found we can solve a quadratic equation to get exact expressions for x_1 and x_2 (where the order does not matter). We substitute these into $dx_1/\sqrt{f(x_1)} + dx_2/\sqrt{f(x_2)}$ and $x_1 dx_1/\sqrt{f(x_1)} + x_2 dx_2/\sqrt{f(x_2)}$, and check whether they simplify to give

$$\begin{aligned} \frac{dx_1}{\sqrt{f(x_1)}} + \frac{dx_2}{\sqrt{f(x_2)}} &= \frac{\alpha_{11} + \alpha_{12}x}{\sqrt{f(x)}}dx, \\ \frac{x_1 dx_1}{\sqrt{f(x_1)}} + \frac{x_2 dx_2}{\sqrt{f(x_2)}} &= \frac{\alpha_{21} + \alpha_{22}x}{\sqrt{f(x)}}dx, \end{aligned}$$

as in (2). The simplification involves nothing harder than computing greatest common divisors of polynomials over number fields. The KANT/KASH package does this very well. On the other hand, this package does not (yet) handle square roots of polynomials (as occur in the expressions for x_1 and x_2) symbolically, so we have to do some work "by hand". The hardest part of the simplification is to simplify the square root of $f(x_i)$; this involves finding a square root of the form $a\sqrt{d_1} + b\sqrt{d_2}$ for an expression of the form $c + d\sqrt{d_1 d_2}$, (where only $d_1 d_2$ is known, not d_1 and d_2 separately), where the variables are all polynomials over the CM-field. This can be done in the following way. We first find the square root, call it g, of the polynomial

$$(c + d\sqrt{d_1 d_2})(c - d\sqrt{d_1 d_2}) = c^2 - d^2 d_1 d_2$$

(by computing the gcd of the polynomial and its formal derivative); then we see that g equals $(a\sqrt{d_1} + b\sqrt{d_2})(a\sqrt{d_1} - b\sqrt{d_2}) = a^2 d_1 - b^2 d_2$, and, of course, $d = 2ab$ and $c = a^2 d_1 + b^2 d_2$. Assuming that c and d are relatively prime and $d_1 d_2$ square-free,

we then get

$$\begin{aligned} 2a &= \gcd(g+c,d), \\ d_1 &= \frac{g+c}{2a^2}, \\ b &= \frac{d}{2a}, \\ d_2 &= \frac{d_1 d_2}{d_1}. \end{aligned}$$

10. Notes on the implementation

Most of the work was done in Mathematica (version 2.2), although a special purpose integration program was written in C, using the Pari library (version 1.39), which could be called from Mathematica. Gausian quadrature with 150 points and adapted for the specific functions to be integrated was used. This allowed integrals to even 300 or more decimal places to be done in reasonable time.

Once the integrals around the elements of a basis for the homology of the curve are computed, it is relatively easy to compute the period matrix (corresponding to a symplectic basis) for different orderings of the branch points. In this way the imaginary part of τ can be maximized. This is important for the computation of theta functions. The larger the imaginary part, the faster the series defining the theta function converges (in particular, the minimum of the real parts of the eigenvalues of the imaginary part of τ needs to be maximized). To compute τ' and $\overline{\alpha}'$ (see Section 4) we used the package Pari/gp (see [5]). To find the symplectic matrix relating τ and τ' we implemented method one, as described in Section 4, in Mathematica. This still involved some guesswork, as the τ's tend to lie on the boundary of the fundamental domain.

Computation of theta function values was also implemented in C, using the Pari library, and made callable from Mathematica. For some of the curves (for which the imaginary part of τ is not particularly big) this was the most time-consuming part of the calculation.

Using Section 3, we can predict for how many points P we need to compute x_1 and x_2 in order to be able to solve for the coefficients of $x_1 + x_2$ and $x_1 x_2$. We picked the points P in a rectangle a bit bigger than the smallest rectangle that would contain all the branch points (except infinity) moved up to above the branch point with maximal imaginary part. Solving the linear system for finding the coefficients proved to be problematic, as a lot of precision was lost. This turned out to be Mathematica 2.2's fault, as Mathematica 3.0 does this without significant loss of precision.

The linear combinations needed to find the coefficients of an algebraic integer once the conjugates are known was found using Pari (see Section 8). To guess the exact rationals we simply used Mathematica's `Rationalize`.

As already mentioned, the 1-forms were simplified using KANT/KASH version 1.7.

11. The results

For all 18 curves in [5] we were able to find the functions $x_1 + x_2$ and $x_1 x_2$ and simplify (2) to find $\overline{\alpha}$. Unfortunately, for most of the curves these functions are very

big. For instance, for the last curve one of the coefficients of an algebraic number which is a coefficient in a polynomial of degree 22 is given by

$$\frac{3828292949895166374116919517614694495134714074692934068014078603412500 7}{1000432039015677358171226479013293691116564501672983169555664062500}$$

For this curve the simplification of the 1-forms took more than three days of computer time (and gave the relatively simple

$$\overline{\alpha} = \begin{pmatrix} \frac{-19\,z}{663} - \frac{121\,z^2}{663} - \frac{11\,z^3}{663} & \frac{-6820\,z}{11271} - \frac{1210\,z^2}{11271} - \frac{110\,z^3}{11271} \\ \frac{-62\,z}{65} - \frac{11\,z^2}{65} - \frac{z^3}{65} & \frac{97\,z}{221} - \frac{22\,z^2}{221} - \frac{2\,z^3}{221} \end{pmatrix},$$

where z is a root of $117 - 42\,z + 8\,z^2 - z^3 + z^4$). This kind of data is probably only useful in electronic form, so we will only give the data for a few of the curves here. The data for the other curves can be found on the LSU homepage (`http://math.lsu.edu`).

For each curve we give the following items. The curve, in the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 5. All the curves in [5] have a rational point with $y = 0$ and were therefore easy to change into this form. To make it easier to identify the curve we next give the Igusa invariants. The roots a_i of $f(x)$ follow. Here it is the order of the roots that is most important. For this particular order of the roots and the symplectic basis chosen as described above we get a τ with a large imaginary part. Next we give a polynomial defining the CM-field and a numerical approximation to a root z of this polynomial. Recall that in all cases we used $\tilde{\alpha} = z$. We use rational linear combinations of powers of z to give elements of the CM-field. Then we list τ (corresponding to the specific choices we have made) and the $\overline{\alpha}$ and M we get from the simplification of the 1-forms. Finally we give the polynomials s_1, s_2 and d such that

$$x_1 + x_2 = \frac{s_1}{d}, \tag{3}$$

$$x_1 x_2 = \frac{s_2}{d}. \tag{4}$$

Note that our computations do not prove that the τ we give is correct. They also do not prove that a given curve has complex multiplication by the full ring of integers of the CM-field. It should be possible to verify this as follows. Our computation does prove that $\tilde{\alpha} = z$ is in the endomorphism ring. There are only a finite number of orders in the CM-field containing $\tilde{\alpha}$. As in [5], we should be able to compute exact values for the finite number of $\tau \in \mathfrak{h}_2$ corresponding to the finite number of abelian varieties that have CM by each of these orders. We can assume these τ lie in the fundamental domain given by [2, Theorem 1]. This shows that if we compute τ of our curve with sufficient error bounds on the integrals involved, we will know its value exactly and we will also know the CM order.

The curves below are numbered in the order they appear in [5] (with curve 0 being $y^2 = x^5 - 1$).

11.1. **Curve 1.** The curve is

$$y^2 = -1 + 3\,x + 6\,x^2 - 2\,x^3 - 3\,x^4 + x^5.$$

Igusa invariants:

$$\begin{aligned} i_1 &= 2^7 3^{15}, \\ i_2 &= 2^5 3^{11} 5, \\ i_3 &= 2^4 3^9 31. \end{aligned}$$

Roots:

$$\begin{aligned} a_1 &= -1, \\ a_2 &= -0.8477590650225735123..., \\ a_3 &= 0.23463313526982045654..., \\ a_4 &= 1.7653668647301795435..., \\ a_5 &= 2.8477590650225735123... \end{aligned}$$

The CM-field is defined by the polynomial $p = 2 + 4\,z^2 + z^4$. Let z be the root of p closest to $-0.7653668647301795435i$. Then

$$\tau = \begin{pmatrix} -3\,z - z^3 & -z - \frac{z^3}{2} \\ -z - \frac{z^3}{2} & \frac{-3\,z}{2} - \frac{z^3}{2} \end{pmatrix},$$

$$\overline{\alpha} = \begin{pmatrix} -z & 0 \\ 0 & 3\,z + z^3 \end{pmatrix},$$

$$M = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 2 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}.$$

The functions $x_1 + x_2$ and $x_1 x_2$ are given by

$$s_1 = 4 + z^2 + \left(-2 - z^2\right) x,$$

$$s_2 = 2 + z^2 + \left(-4 - z^2\right) x + x^2,$$

$$d = 1.$$

11.2. **Curve 2.** The curve is

$$y^2 = -\frac{11}{52} + \frac{16\,x}{13} - 3\,x^2 + 4\,x^3 - 3\,x^4 + x^5.$$

Igusa invariants:

$$\begin{aligned} i_1 &= 2^{28}, \\ i_2 &= -2^{20} 5, \\ i_3 &= -2^{14} 3 \cdot 41. \end{aligned}$$

Roots:

$$\begin{aligned} a_1 &= 0.8028086394949853360..., \\ a_2 &= 0.4648957829735655525... - i \cdot 0.6631980437060379643..., \\ a_3 &= 0.6336998972789417795... + i \cdot 0.0110841998504514601..., \\ a_4 &= 0.4648957829735655525... + i \cdot 0.6631980437060379643..., \\ a_5 &= 0.6336998972789417795... - i \cdot 0.0110841998504514601.... \end{aligned}$$

The CM-field is given by the polynomial $p = 3 + 4\,z + 2\,z^2 - z^3 + z^4$. Let z be the root of p closest to $-0.6513878188659973233 - 0.5224158034564077150i$. Then

$$\tau = \begin{pmatrix} \frac{1}{3} - \frac{5\,z}{9} + \frac{4\,z^2}{9} - \frac{2\,z^3}{9} & \frac{4}{9} + \frac{4\,z}{27} + \frac{z^2}{27} + \frac{z^3}{27} \\ \frac{4}{9} + \frac{4\,z}{27} + \frac{z^2}{27} + \frac{z^3}{27} & -\frac{35}{27} - \frac{44\,z}{81} + \frac{16\,z^2}{81} - \frac{11\,z^3}{81} \end{pmatrix},$$

$$\overline{\alpha} = \begin{pmatrix} -4 - \frac{8\,z}{3} + z^2 - \frac{4\,z^3}{3} & 6 + 4\,z - 2\,z^2 + 2\,z^3 \\ -3 - 2\,z + z^2 - z^3 & 5 + \frac{10\,z}{3} - 2\,z^2 + \frac{5\,z^3}{3} \end{pmatrix},$$

$$M = \begin{pmatrix} -1 & 1 & -2 & -1 \\ -1 & -1 & -2 & 0 \\ 3 & -1 & 3 & 2 \\ 0 & -1 & -1 & 0 \end{pmatrix}.$$

The functions $x_1 + x_2$ and $x_1 x_2$ are given by

$$s_1 = \frac{344}{507} + \frac{311}{1014}z - \frac{395}{2028}z^2 + \frac{245}{2028}z^3 + \left(-\frac{1481}{468} - \frac{529}{468}z + \frac{83}{117}z^2 - \frac{53}{117}z^3\right)x + \left(\frac{301}{52} + \frac{19}{13}z - \frac{45}{52}z^2 + \frac{8}{13}z^3\right)x^2 + \left(-\frac{2345}{468} - \frac{173}{234}z + \frac{161}{468}z^2 - \frac{85}{234}z^3\right)x^3 + \left(\frac{68}{39} + \frac{1}{13}z + \frac{1}{39}z^2 + \frac{1}{13}z^3\right)x^4,$$

$$s_2 = \frac{341}{1014} + \frac{253}{2028}z - \frac{77}{1014}z^2 + \frac{55}{1014}z^3 + \left(-\frac{1007}{676} - \frac{425}{1014}z + \frac{167}{676}z^2 - \frac{395}{2028}z^3\right)x + \left(\frac{31}{12} + \frac{19}{39}z - \frac{10}{39}z^2 + \frac{41}{156}z^3\right)x^2 + \left(-\frac{337}{156} - \frac{19}{78}z + \frac{1}{12}z^2 - \frac{7}{39}z^3\right)x^3 + \left(\frac{88}{117} + \frac{23}{468}z + \frac{1}{234}z^2 + \frac{7}{117}z^3\right)x^4,$$

$$d = \frac{59}{234} + \frac{71}{468}z - \frac{1}{9}z^2 + \frac{25}{468}z^3 + \left(-\frac{55}{39} - \frac{17}{26}z + \frac{19}{39}z^2 - \frac{3}{13}z^3\right)x + \left(\frac{469}{156} + \frac{51}{52}z - \frac{115}{156}z^2 + \frac{9}{26}z^3\right)x^2 + \left(-\frac{37}{13} - \frac{20}{39}z + \frac{5}{13}z^2 - \frac{7}{39}z^3\right)x^3 + x^4.$$

11.3. **Curve 3.** The curve is

$$y^2 = -\frac{11}{2} + \frac{45\,x}{4} - \frac{15\,x^3}{2} + x^5.$$

Igusa invariants:

$$\begin{aligned} i_1 &= 2 \cdot 3^{10} 5^5 7^5, \\ i_2 &= 2 \cdot 3^{10} 5^5 7^3, \\ i_3 &= 2 \cdot 3^7 5^3 7^3 193. \end{aligned}$$

Roots:

$$\begin{aligned} a_1 &= -2, \\ a_2 &= -1.9630310126778095021..., \\ a_3 &= 0.7269630351780198057..., \\ a_4 &= 0.7867801131949879910..., \\ a_5 &= 2.4492878643048017054.... \end{aligned}$$

The CM-field is defined by the polynomial $p = 20 + 10\,z^2 + z^4$. Let z be the root of p closest to $-2.6899940478558293078i$. Then

$$\tau = \begin{pmatrix} 2\,z + \frac{2\,z^3}{5} & 2\,z + \frac{3\,z^3}{10} \\ 2\,z + \frac{3\,z^3}{10} & \frac{z^3}{10} \end{pmatrix},$$

$$\overline{\alpha} = \begin{pmatrix} z & 0 \\ 0 & 3\,z + \frac{z^3}{2} \end{pmatrix},$$

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ -2 & -4 & 0 & 0 \\ -4 & 2 & 0 & 0 \end{pmatrix}.$$

The functions $x_1 + x_2$ and $x_1 x_2$ are given by

$$\begin{aligned} s_1 = &-\frac{55}{2} - \frac{29}{4}z^2 + \left(\frac{187}{2} + \frac{237}{8}z^2\right)x + \left(-123 - 47z^2\right)x^2 + \left(\frac{159}{2} + 31z^2\right)x^3 \\ &+ \left(14 + 7z^2\right)x^4 + \left(-57 - \frac{39}{2}z^2\right)x^5 + \left(4 + 2z^2\right)x^6 + \left(8 + 3z^2\right)x^7, \end{aligned}$$

$$\begin{aligned} s_2 = &\ 19 + \frac{1}{2}z^2 + \left(-\frac{39}{2} + \frac{31}{4}z^2\right)x + \left(-\frac{535}{8} - \frac{451}{16}z^2\right)x^2 \\ &+ \left(115 + \frac{117}{4}z^2\right)x^3 + \left(-\frac{71}{4} - \frac{9}{4}z^2\right)x^4 + \left(-46 - 11z^2\right)x^5 + \left(\frac{21}{2} + \frac{9}{2}z^2\right)x^6 \\ &+ \left(-2 - 1z^2\right)x^7 + \left(-4 - \frac{3}{2}z^2\right)x^8, \end{aligned}$$

$$\begin{aligned} d = &-5 - \frac{25}{16}z^2 + \left(\frac{45}{2} + \frac{13}{2}z^2\right)x + \left(-\frac{111}{4} - \frac{61}{8}z^2\right)x^2 \\ &+ \left(-8 - z^2\right)x^3 + \left(\frac{33}{2} + \frac{15}{4}z^2\right)x^4 + \left(8 + z^2\right)x^5 + x^6. \end{aligned}$$

11.4. **Curve 4.** The curve is

$$y^2 = \frac{8}{121} - \frac{100\,x}{121} + \frac{380\,x^2}{121} - \frac{430\,x^3}{121} - \frac{10\,x^4}{11} + x^5.$$

Igusa invariants:

$$\begin{aligned} i_1 &= \frac{2\cdot 3^{10}5^5719^5}{11^{12}}, \\ i_2 &= \frac{2\cdot 3^{8}5^5719^3}{11^{8}}, \\ i_3 &= \frac{2\cdot 3^{7}5^5719^3}{11^{8}}. \end{aligned}$$

Roots:

$$\begin{aligned} a_1 &= -1.9184728707533167674..., \\ a_2 &= 0.15334488302615875118..., \\ a_3 &= 2, \\ a_4 &= 0.3727880704437805965..., \\ a_5 &= 0.30143082637428651060.... \end{aligned}$$

The CM-field is defined by the polynomial $p = 20 + 10\,z^2 + z^4$. Let z be the root of p closest to $-2.6899940478558293078i$. Then

$$\tau = \begin{pmatrix} \frac{10\,z}{11} + \frac{7\,z^3}{44} & -\frac{12}{11} - \frac{z^2}{11} \\ -\frac{12}{11} - \frac{z^2}{11} & \frac{-6\,z}{11} - \frac{z^3}{22} \end{pmatrix},$$

$$\overline{\alpha} = \begin{pmatrix} 3\,z + \frac{z^3}{2} & -2\,z - \frac{z^3}{2} \\ 0 & z \end{pmatrix},$$

$$M = \begin{pmatrix} 0 & -2 & 2 & 0 \\ 3 & 0 & 0 & -4 \\ 1 & 0 & 0 & -3 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

The functions $x_1 + x_2$ and x_1x_2 are given by

$$\begin{aligned} s_1 = {} & \frac{12128}{1771561} - \frac{7296}{1771561}z^2 + \left(-\frac{327072}{1771561} + \frac{134408}{1771561}z^2\right)x \\ & + \left(\frac{3834192}{1771561} - \frac{863384}{1771561}z^2\right)x^2 + \left(-\frac{23775816}{1771561} + \frac{1804164}{1771561}z^2\right)x^3 \\ & + \left(\frac{7036336}{161051} + \frac{201196}{161051}z^2\right)x^4 + \left(-\frac{90236}{1331} - \frac{102716}{14641}z^2\right)x^5 \\ & + \left(\frac{46000}{1331} + \frac{8502}{1331}z^2\right)x^6 + \left(\frac{116}{11} + \frac{61}{121}z^2\right)x^7 + \left(-6 - 1z^2\right)x^8, \end{aligned}$$

$$s_2 = -\frac{17984}{1771561} - \frac{8960}{1771561}z^2 + \left(\frac{187488}{1771561} + \frac{126784}{1771561}z^2\right)x + \left(-\frac{288312}{1771561} - \frac{672264}{1771561}z^2\right)x^2 + \left(-\frac{3384256}{1771561} + \frac{1502224}{1771561}z^2\right)x^3 + \left(\frac{1446036}{161051} - \frac{70938}{161051}z^2\right)x^4 + \left(-\frac{1400}{121} - \frac{10820}{14641}z^2\right)x^5 + \left(-\frac{3590}{1331} + \frac{9}{1331}z^2\right)x^6 + \left(8 + \frac{100}{121}z^2\right)x^7 + \left(4 + \frac{1}{2}z^2\right)x^8,$$

$$d = \frac{6096}{161051} + \frac{1220}{161051}z^2 + \left(-\frac{101456}{161051} - \frac{19320}{161051}z^2\right)x + \left(\frac{662284}{161051} + \frac{117944}{161051}z^2\right)x^2 + \left(-\frac{2223224}{161051} - \frac{370748}{161051}z^2\right)x^3 + \left(\frac{383154}{14641} + \frac{61038}{14641}z^2\right)x^4 + \left(-\frac{38976}{1331} - \frac{6038}{1331}z^2\right)x^5 + \left(\frac{2399}{121} + \frac{697}{242}z^2\right)x^6 + \left(-\frac{84}{11} - 1z^2\right)x^7 + x^8.$$

11.5. **Curve 7.** The curve is

$$y^2 = -\frac{289}{116} + \frac{373\,x}{29} - 25\,x^2 + 22\,x^3 - 8\,x^4 + x^5.$$

Igusa invariants:

$$\begin{aligned} i_1 &= \frac{2^{38}3^{10}11^5}{5^{12}}, \\ i_2 &= \frac{-2^{26}3^8 11^3}{5^6}, \\ i_3 &= \frac{-2^{18}3^7 11^2 2927}{5^6}. \end{aligned}$$

Roots:

$$\begin{aligned} a_1 &= 3.0819566193534462548... + i \cdot 0.0131280766434132556..., \\ a_2 &= 3.0819566193534462548... - i \cdot 0.0131280766434132556..., \\ a_3 &= 0.6417149087096116878... + i \cdot 0.2505935554765203618..., \\ a_4 &= 0.6417149087096116878... - i \cdot 0.2505935554765203618..., \\ a_5 &= 0.5526569438738841148.... \end{aligned}$$

The CM-field is defined by the polynomial $p = 23 - 20\,z + 4\,z^2 - z^3 + z^4$. Let z be the root of p closest to $-1.0962912017836260078 - 2.6439984879835058294i$. Then

$$\tau = \begin{pmatrix} -\frac{856}{203} + \frac{267\,z}{203} + \frac{121\,z^2}{203} + \frac{90\,z^3}{203} & \frac{228}{203} + \frac{19\,z}{203} - \frac{18\,z^2}{203} - \frac{5\,z^3}{203} \\ \frac{228}{203} + \frac{19\,z}{203} - \frac{18\,z^2}{203} - \frac{5\,z^3}{203} & -\frac{148}{203} - \frac{80\,z}{203} + \frac{z^2}{203} - \frac{11\,z^3}{203} \end{pmatrix},$$

$$\overline{\alpha} = \begin{pmatrix} -\frac{25}{7} + \frac{38\,z}{35} + \frac{6\,z^2}{35} + \frac{11\,z^3}{35} & \frac{22}{7} - \frac{34\,z}{35} + \frac{2\,z^2}{35} - \frac{8\,z^3}{35} \\ \frac{22}{7} - \frac{34\,z}{35} + \frac{2\,z^2}{35} - \frac{8\,z^3}{35} & \frac{8}{7} - \frac{13\,z}{35} + \frac{9\,z^2}{35} - \frac{z^3}{35} \end{pmatrix},$$

$$M = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ -13 & 4 & -3 & -5 \\ 4 & -3 & 1 & 4 \end{pmatrix}.$$

The functions $x_1 + x_2$ and $x_1 x_2$ are given by

$$\begin{aligned} s_1 =& \frac{26948305}{341446} + \frac{44357013}{682892}z - \frac{3269481}{23548}z^2 + \frac{17726257}{341446}z^3 \\ &+ \left(-\frac{322745683}{341446} - \frac{23853006}{170723}z + \frac{630910883}{682892}z^2 - \frac{18565001}{48778}z^3\right)x \\ &+ \left(\frac{1356012089}{341446} - \frac{315012797}{682892}z - \frac{439432730}{170723}z^2 + \frac{391640583}{341446}z^3\right)x^2 \\ &+ \left(-\frac{691613999}{82418} + \frac{158119701}{82418}z + \frac{47035831}{11774}z^2 - \frac{305968657}{164836}z^3\right)x^3 \\ &+ \left(\frac{120817119}{11774} - \frac{15721866}{5887}z - \frac{22911999}{5887}z^2 + \frac{10446323}{5887}z^3\right)x^4 \\ &+ \left(-\frac{26142277}{3364} + \frac{44105909}{23548}z + \frac{59425923}{23548}z^2 - \frac{12278149}{11774}z^3\right)x^5 \\ &+ \left(\frac{87499117}{23548} - \frac{2344311}{3364}z - \frac{6494574}{5887}z^2 + \frac{4521019}{11774}z^3\right)x^6 \\ &+ \left(-\frac{124187}{116} + \frac{20534}{203}z + \frac{256815}{812}z^2 - \frac{74563}{812}z^3\right)x^7 \\ &+ \left(\frac{8917}{58} + \frac{8069}{406}z - \frac{22387}{406}z^2 + \frac{3273}{203}z^3\right)x^8 \\ &+ \left(-\frac{7251}{2842} - \frac{28177}{2842}z + \frac{144}{29}z^2 - \frac{13273}{5684}z^3\right)x^9 \\ &+ \left(-\frac{258}{203} + \frac{225}{203}z - \frac{30}{203}z^2 + \frac{40}{203}z^3\right)x^{10}, \end{aligned}$$

$$\begin{aligned} s_2 =& \frac{3761624}{170723} + \frac{15879683}{341446}z - \frac{46239133}{682892}z^2 + \frac{15358327}{682892}z^3 \\ &+ \left(-\frac{95165633}{341446} - \frac{81018919}{341446}z + \frac{313621027}{682892}z^2 - \frac{54510685}{341446}z^3\right)x \\ &+ \left(\frac{772077995}{682892} + \frac{187607263}{341446}z - \frac{64931605}{48778}z^2 + \frac{315620153}{682892}z^3\right)x^2 \\ &+ \left(-\frac{1523647521}{682892} - \frac{624972003}{682892}z + \frac{752911063}{341446}z^2 - \frac{486124879}{682892}z^3\right)x^3 \\ &+ \left(\frac{4263015}{1682} + \frac{7243216}{5887}z - \frac{55046885}{23548}z^2 + \frac{7519875}{11774}z^3\right)x^4 \\ &+ \left(-\frac{21317263}{11774} - \frac{975759}{841}z + \frac{19453103}{11774}z^2 - \frac{4027587}{11774}z^3\right)x^5 \end{aligned}$$

$$+\left(\frac{9592091}{11774}+\frac{16647161}{23548}z-\frac{4597581}{5887}z^2+\frac{2544685}{23548}z^3\right)x^6$$
$$+\left(-\frac{1159990}{5887}-\frac{6553987}{23548}z+\frac{2840205}{11774}z^2-\frac{239573}{11774}z^3\right)x^7$$
$$+\left(\frac{1187}{203}+\frac{8287}{116}z-\frac{18689}{406}z^2+\frac{2587}{812}z^3\right)x^8$$
$$+\left(\frac{3235}{406}-\frac{4569}{406}z+\frac{1955}{406}z^2-\frac{265}{406}z^3\right)x^9$$
$$+\left(-\frac{1746}{1421}+\frac{1175}{1421}z-\frac{165}{812}z^2+\frac{110}{1421}z^3\right)x^{10},$$

$$d=\frac{937562}{24389}-\frac{201085}{97556}z-\frac{3030915}{97556}z^2+\frac{342253}{24389}z^3$$
$$+\left(-\frac{134192477}{341446}+\frac{37696245}{341446}z+\frac{70473043}{341446}z^2-\frac{35938141}{341446}z^3\right)x$$
$$+\left(\frac{128103501}{82418}-\frac{25144155}{41209}z-\frac{13370845}{23548}z^2+\frac{53325313}{164836}z^3\right)x^2$$
$$+\left(-\frac{19060694}{5887}+\frac{1196437}{841}z+\frac{5065170}{5887}z^2-\frac{6268697}{11774}z^3\right)x^3$$
$$+\left(\frac{23789566}{5887}-\frac{20920979}{11774}z-\frac{4776332}{5887}z^2+\frac{12119511}{23548}z^3\right)x^4$$
$$+\left(-\frac{5471057}{1682}+\frac{15483175}{11774}z+\frac{5977325}{11774}z^2-\frac{1770337}{5887}z^3\right)x^5$$
$$+\left(\frac{1429147}{812}-\frac{493705}{812}z-\frac{173483}{812}z^2+\frac{42283}{406}z^3\right)x^6$$
$$+\left(-\frac{130003}{203}+\frac{35745}{203}z+\frac{11815}{203}z^2-\frac{7909}{406}z^3\right)x^7$$
$$+\left(\frac{60091}{406}-\frac{11961}{406}z-\frac{7475}{812}z^2+\frac{1193}{812}z^3\right)x^8$$
$$+\left(-\frac{3867}{203}+\frac{439}{203}z+\frac{129}{203}z^2+\frac{2}{203}z^3\right)x^9+x^{10}.$$

Acknowledgment

I would like to thank Bjorn Poonen for his generous help, in particular for pointing out how one can compute the degrees of the functions x_1+x_2 and x_1x_2 (see Section 3).

References

[1] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics 138. Springer-Verlag, 1993. MR **94i:**11105

[2] E. Gottschling. Explizite bestimmung der randflächen des fundamentalbereiches der modulgruppe zweiten grades. *Math. Annalen*, 138:103–124, 1959. MR **21:**5748

[3] J. Milne. Jacobian varieties. In G. Cornell and J. Silverman, editors, *Arithmetic Geometry*. Springer-Verlag, 1986, pp. 167–212. MR **89b:**14029

[4] D. Mumford. *Tata Lectures on Theta II*, Progr. Math. 43, Birkhäuser, 1984. MR **86b:**14017

[5] P. van Wamelen. Examples of genus two CM curves defined over the raionals, *Math. Comp.* 68 (1999), 307–320. CMP 99:03

Department of Mathematics, University of South Africa, P. O. Box 392, Pretoria, 0003, South Africa

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

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