Genus 2 Curves with Quaternionic Multiplication

Srinath Baba, Håkan Granath*

March 17, 2005

Abstract

We explicitly construct the canonical rational models of Shimura curves, both analytically in terms of modular forms and algebraically in terms of coefficients of genus 2 curves, in the cases of quaternion algebras of discriminant 6 and 10. This emulates the classical construction in the elliptic curve case. We also give families of genus 2 QM curves, whose Jacobians are the corresponding abelian surfaces on the Shimura curve, and with coefficients that are modular forms of weight 12. We apply these results to show that our j-functions are supported exactly at those primes where the genus 2 curve does not admit potentially good reduction, and construct fields where this potentially good reduction is attained. Finally, using j, we construct the fields of moduli and definition for some moduli problems associated to the Atkin-Lehner group actions.

Key words: Shimura curve, canonical model, quaternionic multiplication, modular form, field of moduli
2000 Mathematics Subject Classification: 11G18, 14G35

1 Introduction

An abelian surface is said to have quaternionic multiplication, or QM for short, if its endomorphism ring admits an embedding by an order $\mathcal{O}$ in an indefinite non-split quaternion algebra over $\mathbb{Q}$. A genus 2 curve is said to have QM if its Jacobian does. Given $\mathcal{O}$, let $\mathcal{O}^1$ denote the elements in $\mathcal{O}$ with norm 1. This group acts, via an embedding of $\mathcal{O}$ into $M_2(\mathbb{R})$, naturally on the upper half plane $\mathcal{H}$, and the quotient $V = \mathcal{H}/\mathcal{O}^1$, which is a compact Riemann surface that we call a Shimura curve, is the moduli space of the natural moduli problem of classifying abelian surfaces with QM by $\mathcal{O}$. Shimura proved that this curve admits a model over $\mathbb{Q}$. Our main goal in this paper is to construct explicitly this canonical model of the Shimura curves of discriminants 6 and 10.

The complex multiplication points on V will play a big role for us. A QM abelian surface has complex multiplication if the center of the ring $\mathrm{End}(A)$ is

*Supported by a Marie Curie Intra-European Fellowship under the Sixth Framework Programme of the European Union.

a complex quadratic order $\mathfrak{O}$. Associated to every optimal embedding ι of a quadratic order $\mathfrak{O}$ into $\mathcal{O}$, is a fixed point $z_\iota \in \mathcal{H}$ such that the corresponding abelian surface has CM by $\mathcal{O}$. If $\mathrm{disc}(\mathfrak{O}) = D$, then we say that the resulting point on the Shimura curve has CM by D.

Also important is the so called the Atkin-Lehner group. The Shimura curve V comes equipped with a canonical group of involutions. Certain subgroups G of this group are distinguished by the fact that the quotient V/G is the moduli space that classifies principally polarized abelian surfaces A with an embedding of a certain subring of $\mathcal{O}$ into $\mathrm{End}(A)$ which extends to QM by $\mathcal{O}$.

The problem that we consider has two sides to it: On one side there are the abelian surfaces with QM considered as complex tori. There is a classical construction associating to a point z on the upper half plane $\mathcal{H}$ the period matrix of a QM abelian surface. On the other side, there are the genus 2 curves whose Jacobians have QM. Families of such curves have been constructed by Hashimoto and Murabayashi in the cases of discriminant 6 and 10. What is missing is an explicit way to link a genus 2 curve in such a family to the point z in the upper half plan giving its complex Jacobian. In addition, equations for Shimura curves have been computed by Kurihara and others. For example, it is known that in the case of $\mathcal{O}$ having discriminant 6, the Shimura curve has equation $x^2 + y^2 + 3 = 0$ defined over $\mathbb{Q}$. However, there is no explicit correspondence between points on this quadric and points $z \in \mathcal{H}$. In this paper, we construct such correspondences in the discriminant 6 and 10 cases, and derive complex uniformized family of genus 2 curves whose Jacobians are exactly those given by the classical construction.

The strategy in the paper is the following: On the one hand, there is a rational map of the Shimura curve into the moduli space $\mathcal{M}_2$ of genus 2 curves, factoring through the action of the Atkin-Lehner group. We compute equations for the image in $\mathcal{M}_2$ in terms of Igusa's invariants $J_2, \ldots, J_{10}$ using the work of Hashimoto and Murabayashi on families of genus 2 curves with QM in [9]. Then we solve these equations, and get a parametrization of the image curve. This is now given in terms of the coefficients of the sextics defining the genus 2 curves. On the other hand, we determine the ring of modular forms with respect to $\mathcal{O}^1$, and use this to construct a generator of the rational function field in terms of modular forms. Finally, we are able to find some CM points on the Shimura curve where we know both sides, i.e. both the genus 2 curve and the values of the modular forms. This information we then use to show that our two functions are equal. We denote the function we have constructed by j. This function is really defined on the quotient curve of the Shimura curve by the Atkin-Lehner involutions, so finally we construct functions on V which give the canonical structure by Shimura of V as a curve over $\mathbb{Q}$.

By using a construction of Mestre, we recover the genus 2 curve from its j-invariant. Using the analytic description of j, we are thus able to construct a sextic whose coefficients are modular forms of weight 12, such that at any point z in $\mathcal{H}$ the genus 2 curve C_z described by the sextic has Jacobian A_z. An important difference between our families and the ones given in [9], is that the former are families over V, while the latter factor via a cover of V.

The j-function that we define has many of the properties that its namesake in the elliptic curve case has. First, it follows immediately from our construction, that $j(C)$ generates the field of moduli of the genus 2 curve C. Contrary to the elliptic curve case, the genus 2 curve can in general not be defined over its field of moduli. We express the so called Mestre obstruction for this curve in terms of j, and hence we know in principle every possible field of definition. Furthermore, we show that the primes occurring on j are exactly those where the genus 2 curve do not have potentially good reduction. This shows that j is distinguished in the function field. Finally, using j, we construct the fields of moduli for the various moduli problems described by the Atkin-Lehner involutions.

One point in involving modular forms, is of course to be able to numerically compute values of our j-function. To calculate values of modular forms on a compact Shimura curve, one can embed the curve in a Hilbert modular surface. By restricting Hilbert modular forms on $\mathcal{H} \times \mathcal{H}$ to the embedded curve and putting in natural correction factors, one gets modular forms on the Shimura curve. We describe this in appendix A. In our cases, the curves can be embedded into the Hilbert modular surface corresponding to $\mathbb{Q}(\sqrt{5})$, and one can use the corresponding Eisenstein series on $\mathcal{H} \times \mathcal{H}$ to efficiently compute values of the modular forms occurring in this paper to arbitrary precision.

The obvious directions that should emerge from this work are extensions to higher discriminant and higher level. In the higher discriminant case, the difficulty lies in the absence of the Hashimoto-Murabayashi family. On the other hand, understanding the ring of modular forms may yield some success. In the cases that are considered here, better understanding of the behaviour of the j-invariant at algebraic points, and in particular singular moduli should prove useful in arithmetic applications.

The computations required in this paper were done using the computer algebra systems Macaulay 2 [6] and Pari/GP [18].

We thank the Max-Planck-Institut für Mathematik in Bonn, Germany, and the Departments of Mathematics at McGill University and Concordia university in Montreal, Canada, for their support.

2 Preliminaries

2.1 Shimura curves

Let $B = B_\Delta$ denote the indefinite quaternion algebra of discriminant Δ over $\mathbb{Q}$, where $\Delta = p_1 \dots p_{2n}$. Let $x \mapsto x^*$ be the canonical involution on B, so $\mathrm{nr}(x) = x^* x$, and let $\mathcal{O}$ be a maximal order in B_D. Following Rotger [21], we fix an element $\mu \in \mathcal{O}$ with $\mu^2 = -\Delta$ and we call the pair $(\mathcal{O}, \mu)$ a principally polarized maximal order in B. Define the positive anti-involution $a \mapsto a'$ on B by $a' = \mu^{-1} a^* \mu$ (i.e., the quadratic form $a \mapsto \mathrm{tr}(a'a)$ is positive definite). Let R be a maximally embedded subring of $\mathcal{O}$ invariant under $'$ (i.e, $R = \mathbb{Q}R \cap \mathcal{O}$ and $R' = R$). We call such rings *stable*.

Let $S_{(\mathcal{O},\mu)}$ be the set of triples $[A, \rho, \iota]$, where A is an abelian surface, ρ is a principal polarization on A, and $\iota : \mathcal{O} \to \mathrm{End}(A)$ is an embedding such that the Rosati involution defined by ρ on $\iota(\mathcal{O})$ is $'$. We recall how such triples are constructed. Fix an embedding $\theta : B \to M_2(\mathbb{R})$. For any point $z \in \mathcal{H}$, consider the lattice $\Lambda_z = \theta(\mathcal{O})v_z$ in $\mathbb{C}^2$, where $v = \begin{pmatrix} z & 1 \end{pmatrix}^t$. Define $A_z = \mathbb{C}^2/\Lambda_z$. On Λ_z, define the Riemann form

$$\begin{aligned} &E_z : \Lambda_z \times \Lambda_z \to \mathbb{Z} \\ &E_z(\theta(\lambda_1)v_z, \theta(\lambda_2)v_z) = \mathrm{tr}(\lambda_1^* \mu \lambda_2). \end{aligned}$$

E_z defines a principal polarization ρ_z on A_z such that the Rosati involution on $\mathrm{End}_{\mathbb{Q}}(A_z)$ corresponds to the positive anti-involution $a \mapsto a'$ on B. This defines a triple $[A_z, \rho_z, \iota_z]$, where A_z is an abelian surface, ρ_z a principal polarization on A_z and $\iota_z : \mathcal{O} \to \mathrm{End}(A_z)$ an injection.

Let R be a stable subring of $\mathcal{O}$. Define an equivalence relation $\sim_R$ on $S_{(\mathcal{O},\mu)}$ as follows: $[A_1, \rho_1, \iota_1] \sim_R [A_2, \rho_2, \iota_2]$ if and only if there exists an isomorphism $\phi : A_1 \to A_2$ such that $\phi^*(\rho_2) = \rho_1$, and for every $r \in R$, the following diagram commutes.

$$\begin{tikzcd} A_1 \arrow[r, "\phi"] \arrow[d, "\iota_1(r)"] & A_2 \arrow[d, "\iota_2(r)"] \\ A_1 \arrow[r, "\phi"] & A_2 \end{tikzcd}$$

Let V_R be the moduli space that classifies triples $[A, \rho, \iota]/\sim_R$.

The normalizer group $N_{B^+}(\mathcal{O})$ acts on $\mathcal{H}$ as fractional linear transformations through θ. This generates a subgroup of $\mathrm{Aut}(\mathcal{H})$ which we denote by $\tilde{\Gamma}$. The subgroup of $\tilde{\Gamma}$ generated by elements of $\mathcal{O}$ of norm 1 is denoted by Γ. Let $V = \mathcal{H}/\Gamma$, which is a compact Riemann surface. The group $\tilde{\Gamma}/\Gamma \cong (\mathbb{Z}/2)^{2n}$, the so called Atkin-Lehner group, acts on V. Any coset $w \in \tilde{\Gamma}/\Gamma$ is of the form $w = \gamma\Gamma$, where $\gamma \in \mathcal{O}$ with $\mathrm{nr}(\gamma) = d > 0$ and $d \mid \Delta$. We write $w = w_d$. For any subgroup G of $\tilde{\Gamma}/\Gamma$, we denote $V_G = V/G$. We also let $V_d = V/\langle w_d \rangle$ for any positive divisor d of Δ.

In [21], an element $\chi \in \mathcal{O} \cap N_{B^+}(\mathcal{O})$ is called *twisting* if $\mathrm{tr}(\chi) = 0$ and $\chi\mu + \mu\chi = 0$ (note that this implies that $\mathrm{nr}(\chi) < 0$). A quadratic stable ring R is called *twisting* if it is contains a twisting element. Not all pairs $(\mathcal{O}, \mu)$ have twisting subrings, and if they exist there are exactly 2 of them. From now on, we assume that this is the case (it holds for $\Delta = 6$, 10). The twisting rings naturally correspond to two elements w_m, $w_{m'}$ of the Atkin-Lehner group with $mm' = \Delta$. We denote the twisting rings by R_m and $R_{m'}$ respectively and let $R_\Delta = \mathbb{Z}[\mu]$. The subgroup of the Atkin-Lehner group generated by w_m and $w_{m'}$ has 4 elements and is denoted by W.

The following result shows how we can identify the moduli spaces above with quotients of V by appropriate subgroups of the Atkin-Lehner groups.

Theorem 1. *There are natural identifications $V_{\mathcal{O}} = V$, $V_{R_d} = V_d$ for $d \in \{m, m', \Delta\}$ and $V_{\mathbb{Z}} = V_W$. For any other stable quadratic ring R, we have $V_R = V$.*

This theorem is a reformulation of more general results proved in [21]. In fact, it holds that

$$[A_z, \rho_z, \iota_z] \sim_R [A_{z'}, \rho_{z'}, \iota_{z'}]$$

if and only if the points z and z' are related by $z' = \gamma z$, where $\gamma = w\varepsilon \in N_{B^+}(\mathcal{O})$, $w \in Z(R)$, $\varepsilon \in \mathcal{O}^*$ and $w\mu = \mathrm{nr}(\varepsilon)\mu w$. Here $Z(R)$ denotes the centraliser of R in $\mathcal{O}$. It is straightforward to verify that this claim is equivalent to theorem 1.

We recall some fundamental facts that will be used in this paper. First, the curve V has a canonical model defined over $\mathbb{Q}$ (see [24]). The Atkin-Lehner involutions are also defined over $\mathbb{Q}$, so all quotient curves V_G are defined over $\mathbb{Q}$. Second, for any imaginary quadratic order $\mathfrak{O}_D$ that embeds into $\mathcal{O}$, the coordinates of a point with complex multiplication by $\mathfrak{O}_D$ on any rational model of V are in the ring class field $H(\mathfrak{O}_D)$ of $\mathfrak{O}_D$ (see [25]). The number of points on V with given CM can be computed by Eichler's theory of optimal embeddings, see [26].

Define the field of moduli $k_{\mathbb{Z}}$ of $[A, \rho]/\bar{\mathbb{Q}}$ as the smallest extension of $\mathbb{Q}$ such that for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/k_{\mathbb{Z}})$, there is an isomorphism $\phi_\sigma : A \to A^\sigma$ such that $\phi_\sigma^*(\rho^\sigma) = \rho$. For any subring R of $\mathrm{End}(A)$, we define the field of moduli of k_R as the minimal number field containing $k_{\mathbb{Z}}$ such that such that for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/k_R)$, there is an isomorphism $\phi_\sigma : A \to A^\sigma, \phi_\sigma^*(\rho^\sigma) = \rho$ such that the following diagram commutes for each $r \in R$

$$\begin{tikzcd} A \arrow[r] \arrow[d, "r"] & A^\sigma \arrow[d, "r^\sigma"] \\ A \arrow[r] & A^\sigma \end{tikzcd}$$

Let $\mathcal{M}_2$ denote the moduli space of genus 2 curves, and $\mathcal{A}_2$ denote the moduli space of principally polarized abelian surfaces. The open Torelli map associates to a point $C \in \mathcal{M}_2$ the pair $(\mathrm{Pic}^0(C), \Theta)$, where Θ is the theta divisor that embeds C into $\mathrm{Pic}^0(C)$. Thus, $\mathcal{M}_2$ maps onto a Zariski open subset of $\mathcal{A}_2$, and so the general principally polarized abelian surface is a Jacobian. Let $\tilde{E}$ denote the image of the natural forgetful map $V \to \mathcal{A}_2$, and let E denote the intersection with $\mathcal{M}_2$. We have the following picture:

$$\begin{tikzcd} & \mathcal{A}_2 & \mathcal{M}_2 \arrow[l, hook'] \\ V \arrow[r, "4:1"] & \tilde{E} \arrow[u, hook] & E \arrow[l, hook'] \arrow[u, hook] \end{tikzcd}$$

2.2 Igusa invariants and Mestre's construction

Let C be a non-singular genus 2 curve, with a hyperelliptic model

$$C : z^2 = a_6x^6 + a_5x^5y + a_4x^4y^2 + a_3x^3y^3 + a_2x^2y^4 + a_1xy^5 + a_0y^6,$$

Igusa, in [12], defined invariants $J_i = J_i(C)$, for $i = 2, 4, 6, 10$, which are homogenous polynomials of degree i in the coefficients a_k having rational coefficients. Two curves are isomorphic if and only if they define the same point $p = [J_2(C), J_4(C), J_6(C), J_{10}(C)]$ in the weighted projective space $\mathbb{P}(2, 4, 6, 10)$. The minimal field k over which the point p is defined is called the field of moduli of C.

In [16], Mestre shows how to solve the inverse problem of constructing the genus 2 curve C from its Igusa invariants. He constructs a conic

$$L = \sum_{1 \leq i,j \leq 3} A_{ij} x_i x_j, \tag{1}$$

and a cubic

$$M = \sum_{1 \leq i,j,k \leq 3} a_{ijk} x_i x_j x_k, \tag{2}$$

where the coefficients A_{ij} and a_{ijk} can be expressed in terms of the J_i's. The conic L is degenerate if and only if the curve C has more automorphisms than just the hyperelliptic involution. In this case, we say that C has non-trivial involutions. If so, then it follows from [2] that C is defined over k. If not, then the curve C can in general not be defined over k. In this case, C can be defined over a field extension K/k if and only if L is isotropic over K. It is therefore natural to consider the even Clifford algebra over k associated to L, and we denote it H_C. The quaternion algebra H_C is called the Mestre obstruction of C, and it has the property that C can be defined over K if and only if K splits H_C. If k is a field and $a, b \in k^*$, then we use the notation $(a, b)_k$ for the quaternion algebra over k generated by elements i and j satisfying $i^2 = a$, $j^2 = b$ and $ij + ji = 0$.

One recovers a hyperelliptic model $z^2 = f(x, y)$ from the Igusa invariants by finding a parametrization $x_i = x_i(x, y)$ of the solutions to the equation $L = 0$ and setting

$$f(x, y) = \sum_{1 \leq i,j,k \leq 3} a_{ijk} x_i(x, y) x_j(x, y) x_k(x, y).$$

3 Discriminant 6 case

Let $B = \mathbb{Q}(i, j)$, where $i^2 = 2$, $j^2 = -3$ and $ij + ji = 0$, so $\Delta = \mathrm{disc}(B) = 6$. We choose a maximal order $\mathcal{O} = \mathbb{Z}[i, (j+1)/2]$ in B, and an element $\mu = 2j + ij \in \mathcal{O}$ with $\mu^2 = -6$. We let $R_6 = \mathbb{Z}[\mu] \cong \mathbb{Z}[\sqrt{-6}]$. There are two twisting rings in this case, namely $R_2 = \mathbb{Z}[i] \cong \mathbb{Z}[\sqrt{2}]$ and $R_3 = \mathbb{Z}[j + ij] \cong \mathbb{Z}[\sqrt{3}]$.

From [23] it follows that the curve V has genus 0 and that there are 2 classes of elliptic fixed points of order 2 and 3 respectively for the action of Γ on $\mathcal{H}$. The involutions w_d on V, for $d = 2, 3, 6$, each have 2 fixed points. In the cases of $d = 2$ and $d = 3$, these are exactly the elliptic points of order d. Let z_d, z'_d denote the fixed points of w_d on V. Let x_d and x'_d be a choice of points on the upper half plane that descend to the points z_d, z'_d, for $d = 2, 3, 6$. By abuse of notation, we denote also by z_d, z'_d the images of these points on quotient surfaces V_G, for any subgroup G of the Atkin-Lehner group.

Lemma 2. *The curve V_W is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and $z_2, z_3, z_6 \in V_W(\mathbb{Q})$.*

Proof. The points z_2, z'_2 are points with complex multiplication by $\mathbb{Q}(i)$, so $z_2, z'_2 \in V(H(\mathbb{Q}(i))) = V(\mathbb{Q}(i))$. These two points are transposed by w_3 and also by complex conjugation. We conclude that $z_2, z'_2 \in V_3(\mathbb{Q})$. In particular $z_2 \in E(\mathbb{Q})$ and we get that $V_W \cong \mathbb{P}^1_{\mathbb{Q}}$.

The same argument, using $z_3, z'_3 \in V(H(\mathbb{Q}(\sqrt{-3}))) = V(\mathbb{Q}(\sqrt{-3}))$, gives that $z_3 \in V_W(\mathbb{Q})$.

The fixed points of w_2 on V_3 are the two points z_2 and z_6. Since $V_3 \cong \mathbb{P}^1_{\mathbb{Q}}$, we conclude that z_2 and z_6 are defined over a common minimal field F at most quadratic over $\mathbb{Q}$. If $F \neq \mathbb{Q}$, then we would have that z_2 and z_6 are conjugates under the nontrivial element $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Hence the images are on V_W are also conjugates, but since $z_3 \in V_W(\mathbb{Q})$ we would get $z_3 = z_6$ on V_W, a contradiction. □

3.1 The ring of modular forms

For any group G acting on $\mathcal{H}$, we denote by $v_i(G)$ the number of elliptic fixed points of order i for G, and by $s_k(G)$ the dimension of the space of holomorphic weight k modular forms for G. Let $\Gamma_d = \Gamma \cup w_d\Gamma$. Using the formulae in [23], it follows that the degree of the divisor of a modular form of weight k is $k/6$ and that $s_k = 1 - k + 2\lfloor k/4 \rfloor + 2\lfloor k/3 \rfloor$ for k even and $k > 2$, and 0 otherwise. We compute the following table:

G	v_2	v_3	v_4	v_6	s_4	s_6	s_{12}
Γ	2	2	0	0	1	1	3
Γ_2	0	1	2	0	0	1	1
Γ_3	1	0	0	2	0	0	2
Γ_6	3	1	0	0	1	0	2
$\tilde{\Gamma}$	1	0	1	1	0	0	1

We conclude that $S_4(\Gamma)$ is generated by a form $h_4(z)$ which vanishes necessarily at x_3 and x'_3. Similarly, $S_6(\Gamma)$ is generated by a form $h_6(z)$ which vanishes necessarily at x_2 and x'_2. We assume h_6 is normalised so that $h_4^3/h_6^2(x_6) = \sqrt{3}i$. Fix a basis of $S_{12}(\Gamma)$ by the forms h_4^3, h_6^2, h_{12}, where h_{12} is chosen so that it vanishes at x_6 and y_6. We normalize h_{12} so that $h_{12}^2 + 3h_6^4 + h_4^6 = 0$. Finally, the action of the Atkin-Lehner group on the modular forms is given by

$$
\begin{aligned}
w_6(h_4) &= h_4 = -w_2(h_4) = -w_3(h_4),\\
w_2(h_6) &= h_6 = -w_3(h_6) = -w_6(h_6),\\
w_3(h_{12}) &= h_{12} = -w_2(h_{12}) = -w_6(h_{12}).
\end{aligned}
$$

Proposition 3. *The modular forms h_4 and h_6 are algebraically independent, and*

$$\bigoplus_{k=0}^{\infty} S_{2k}(\Gamma) = \mathbb{C}[h_4(z), h_6(z), h_{12}(z)] \cong \mathbb{C}[h_4, h_6, h_{12}]/(h_{12}^2 + 3h_6^4 + h_4^6)$$

as graded rings.

Proof. To see that $h_4(z)$ and $h_6(z)$ are algebraically independent, first note that any linear combination of modular forms that is identically 0 must have terms of the same weight, and so any polynomial in $h_4(z)$ and $h_6(z)$ that vanishes identically must be a linear combination of monomials of the same weight. Also, any polynomial in $h_4(z)$ and $h_6(z)$ that is identically zero is divisible by h_6, for if not, we could write it as $ch_4(z)^m + h_6(z)P(h_4(z), h_6(z))$ for some polynomial P and constant c, and this would vanish at x_2 but not at x_3. Thus, dividing by $h_6(z)$ would give an algebraic relation of lower degree, and so algebraic independence follows by induction on the degree of the polynomial.

To see that the whole ring of modular forms is generated by h_4, h_6 and h_{12}, we observe that for weights $k \leq 12$ it follows from the dimension formula that all forms are combinations of h_4, h_6 and h_{12}. It also follows that $\dim S_{k+12} = \dim S_k + 2$ for all k. The same recursion formula holds for the graded polynomial ring $\mathbb{C}[h_4, h_6, h_{12}]/(h_{12}^2 + 3h_6^4 + h_4^6)$, and we are done. □

Now, we define the weight 0 modular form j_m, invariant under the action of w_6, as

$$j_m = \frac{4h_6^2}{3h_4^3}.$$

Since the degree of the divisor of a modular form of weight 12 is 2, j_m defines a double cover $V \to \mathbb{P}^1$, and we get

Proposition 4. *The map $j_m : V_6 \to \mathbb{P}^1$ is an isomorphism. Furthermore $j_m(w_2(z)) = j_m(w_3(z)) = -j_m(z)$.*

3.2 Equations for E and the arithmetic j-function

Our goal is to give equations for E and construct an embedding of E into $\mathbb{P}^1$ in terms of the Igusa invariants J_n. Our starting point is the following important result from [9].

Theorem 5. *The following equations give a family of QM-curves with respect to $\mathcal{O}$:*

$$y^2 = x(x^4 - Px^3 + Qx^2 - Rx + 1)$$

with

$$4s^2t^2 - s^2 + t^2 + 2 = 0,$$

$$P = -2(s+t), \quad R = -2(s-t), \quad Q = \frac{(1+2t^2)(11-28t^2+8t^4)}{3(1-t^2)(1-4t^2)}.$$

We rewrite these equations in the coordinates on $\mathcal{M}_2$ given by the Igusa invariants as follows:

Proposition 6. *The equations for E are*

$$J_2^6-68J_2^4J_4+1296J_2^2J_4^2+216J_2^3J_6-4608J_4^3-6912J_2J_4J_6+15552J_6^2=0, \quad \text{(3a)}$$

$$J_2^5-60J_2^3J_4+864J_2J_4^2+216J_2^2J_6-5184J_4J_6+248832J_{10}=0. \quad \text{(3b)}$$

The map given by

$$\varphi(p)=[J_2(24J_4-J_2^2),432J_6-96J_4J_2+3J_2^3]\in\mathbb{P}^1,$$

for $p\in E$, gives an embedding $\varphi:E\to\mathbb{P}^1$.

Proof. A calculation gives that (3a) and (3b) are satisfied by the family of genus 2 curves given in theorem 5. Let

$$\begin{aligned} A&=J_2, & C&=432J_6-96J_4J_2+3J_2^3,\\ B&=J_2^2-24J_4, & D&=12^5J_{10}. \end{aligned}$$

In these variables, equations (3) become

$$(AB+C)(AB-C)=4B^3, \quad \text{(4a)}$$

$$2D=B(AB-C). \quad \text{(4b)}$$

These equations define an irreducible reduced rational curve E_0 in $\mathbb{P}(2,4,6,10)$ with a single simple node at $[A,B,C,D]=[1,0,0,0]$. Hence (3) generate all relations. It is easy to see that the map given by $p\mapsto[AB,C]$ induces an isomorphism from the non-singular resolution of this curve to $\mathbb{P}^1$. $\square$

With notations as in the proof of proposition 6, we define the following function on E

$$j=j_6=\frac{AB-C}{AB+C}=\frac{D^2}{B^5}. \quad \text{(5)}$$

where the second equality follows from (4). Since the image of E in $\mathbb{P}(2,4,6,10)$ is the non-singular locus of the curve given by (4), we get:

Proposition 7. *j defines an isomorphism $E\to\mathbb{P}^1\setminus\{0,\infty\}$.*

The inverse map is given by

$$[A,B,C,D]=[j+1,j,j(1-j),j^3],$$

or, equivalently, the Igusa invariants are given in terms of j by

$$[J_2,J_4,J_6,J_{10}]=[12(j+1),6(j^2+j+1),4(j^3-2j^2+1),j^3].$$

Since $\tilde{E}$ is the resolution of the nodal curve E_0, there are two points on $\tilde{E}$ which are not Jacobians of genus 2 curves. By [10], we know that these points correspond to the points on $\tilde{E}$ with CM by $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. What is happening in these cases, is that the abelian surfaces are products of elliptic curves with the product principal polarization.

Remark. The map from the family in theorem 5 to the curve E is of degree 24 and is given by

$$j = \frac{16(2t^2+1)^4(t^2-1)^2}{27(4t^2-1)^3}.$$

3.3 Some explicit points on E

To compare the algebraically and analytically defined functions, we will need to compute a few explicit points on E. In this section, we compute the curves with discriminant 6 QM and D CM for $D=-24$ and $D=-19$.

We consider first the case $D=-24$. Let $K=\mathbb{Q}(\sqrt{-6})$. We have that the class number is $h(K)=2$, and a non-trivial ideal class in $\mathfrak{O}=\mathbb{Z}[\sqrt{-6}]$ is given by the ideal $\mathfrak{a}=(2,\sqrt{-6})$. Hence, there are two isomorphism classes of elliptic curves with $\mathbb{Z}[\sqrt{-6}]$ CM, namely the curves $E_1=\mathbb{C}/\mathfrak{O}$ and $E_2=\mathbb{C}/\mathfrak{a}$ with j-invariants

$$j(E_1)=j(\sqrt{-6})=1728(1399+988\sqrt{2})$$

and

$$j(E_2)=j(\sqrt{-6}/2)=1728(1399-988\sqrt{2})$$

respectively. Consider the cubic

$$f(t)=(1+\sqrt{2})t^3-3(7-3\sqrt{2})t^2-3(7+3\sqrt{2})t+(1-\sqrt{2}),$$

and define a genus 2 curve $C_{(-24)}$ by

$$z^2=f(x^2).$$

By a direct computation of Igusa invariants, one gets that $C_{(-24)}$ corresponds to a point on E, and has invariant $j=-16/27$.

Proposition 8. *The Jacobian J of $C_{(-24)}$ is isomorphic to $E_1\times E_2$ and has endomorphism ring $\begin{pmatrix}\mathfrak{O} & \mathfrak{a}\\ \mathfrak{a}^{-1} & \mathfrak{O}\end{pmatrix}$. Furthermore, this curve defines a point on E with $j(C_{(-24)})=-16/27$.*

Proof. Consider the non-hyperelliptic involutions u and v on $C_{(-24)}$ given by $u(x,z)=(-x,z)$ and $v(x,z)=(-x,-z)$. The quotient $C_{(-24)}/u$ has equation $s^2=f(t)$ (let $s=z$ and $t=x^2$), which is an elliptic curve with j-invariant $1728(1399-988\sqrt{2})$. Hence

$$C_{(-24)}/u\cong E_2.$$

Similarly the quotient $C_{(-24)}/v$ has equation $s^2=tf(t)$ (where $s=xz$, $t=x^2$), which has j-invariant $1728(1399+988\sqrt{2})$, so

$$C_{(-24)}/v\cong E_1.$$

Let $f_i : C_{(-24)} \to E_i$, $i = 1, 2$, be the corresponding quotient maps. They induce a natural surjective homomorphism of abelian varieties

$$\varphi : J \to E_1 \times E_2,$$

given by

$$\varphi(\mathcal{O}(a - b)) = (f_1(a) - f_1(b), f_2(a) - f_2(b)),$$

where $a, b \in C_{(-24)}$ (the minus signs on the left hand side is given by the group laws of the elliptic curves). By a direct computation, one gets that $f_i(a) = f_i(b)$ for $i = 1, 2$ if and only if $a = b$. Hence φ is an isomorphism. The claim about the endomorphism ring follows immediately.

The final claim follows from by a direct computation. □

Remark. By proposition 8, the endomorphism ring is a maximal order in $M_2(K)$ which is not isomorphic to $M_2(\mathfrak{O})$ (since the class of $\mathfrak{a}$ is not a square in the class group of K). Hence one get in particular that the Jacobian of $C_{(-24)}$ cannot be isomorphic to the square $E \times E$ of an elliptic curve E.

We now consider the case $D = -19$. Let $K = \mathbb{Q}(\sqrt{-19})$ and $\mathfrak{O} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. The class number if K is one, so there is only one elliptic curve $E_3 = \mathbb{C}/\mathfrak{O}$ with CM by $\mathfrak{O}$. It has j-invariant $j(E_3) = -96^3$. Consider the cubic

$$f(t) = 2t^3 - 3(1 + 9\sqrt{-19})t^2 - 3(1 - 9\sqrt{-19})t + 2,$$

and define a genus 2 curve $C_{(-19)}$ by

$$z^2 = f(x^2).$$

This curve corresponds to a point on E with $j = 81/64$, and by an argument similar to the proof of proposition 8 one gets

Proposition 9. *The Jacobian J of $C_{(-19)}$ is isomorphic to $E_3 \times E_3$ and has endomorphism ring $M_2(\mathfrak{O})$. Furthermore, this curve defines a point on E with $j(C_{(-19)}) = 81/64$.*

3.4 The arithmetic function and the analytic function

The main results of this paper relates the arithmetically and the analytically defined functions and gives an explicit map from V to its rational model in terms of modular forms. The first step in this direction is:

Proposition 10. *We have*

$$j = j_m^2, \tag{6}$$

considered as functions on $\tilde{E}$.

Proof. It is clear, from propositions 4 and 7, that j and j_m^2 are related by a linear fractional transformation. We noted in section 3.2 that the points on V_W

corresponding to $J_{10} = 0$ on E are the points z_2 and z_3. These points are therefore the zeroes and poles of j. Furthermore, $j(z_6) = -16/27$ by proposition 8. Now, we have $j_m^2(z_2) = 0$, $j_m^2(z_3) = \infty$ and $j_m^2(z_6) = -16/27$ by our choices of normalization. Hence we conclude that $j = j_m^2$ or $j = \frac{16^2}{27^2 j_m^2}$.

To determine which possibility is the correct one, we use the -19 CM point. By proposition 9, we get that $j = 81/64$ in this point. Now we can numerically compute j_m^2 in the point $z_{(-19)}$, which is the fixed point attached to the order $\mathbb{Z}[i + (1 + 3j)/2]$. This calculation can be done with full control of the size of the error terms, and doing this shows that the first possibility is the correct one. $\square$

By proposition 10 and the identity $-27j - 16 = (4h_{12}/h_4^3)^2$, we have that $\sqrt{j}$ and $\sqrt{-27j - 16}$ lift to meromorphic functions on V.

Theorem 11. *The map $f : V \to X = \{x^2 + 3y^2 + z^2 = 0\}$ given by*

$$f(z) = [h_4^3(z), h_6^2(z), h_{12}(z)] = [4, 3\sqrt{j}, \sqrt{-27j - 16}]$$

is an isomorphism defined over $\mathbb{Q}$.

Proof. Let $K_1 = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$. By [23], we have that the two elliptic points z_2, z_2' of order 2 on V belongs to $V(H(\mathbb{Q}(\sqrt{-1}))) \subset V(K_1)$. Similarly, the two elliptic points z_3, z_3' of order 3 belongs to $V(K_1)$. Furthermore $j(z) = 0$, so $f(z) = [1, 0, \pm\sqrt{-1}]$ for $z = z_2, z_2'$, and similarly $f(z) = [0, 1, \pm\sqrt{-3}]$ for $z = z_3,\ z_3'$. Hence, f maps 4 points on $V(K_1)$ to 4 points on $X(K_1)$. We conclude that f is defined over K_1.

Let $K_2 = \mathbb{Q}(\sqrt{-19})$ and consider the 4 points $z \in V(K_2)$, with -19 CM. We have, by proposition 9 that $j(z) = 81/64$, so $f(z) = [32, \pm 27, \pm 13\sqrt{-19}] \in X(K_2)$ for these points z. Hence f is defined over K_2.

We conclude that f is defined over $K_1 \cap K_2 = \mathbb{Q}$. $\square$

Remark. The equation for V given in theorem 11 is of course known, see [14]. What is new with this result is the explicitly given isomorphism.

Corollary 12. *The Atkin-Lehner action on the curve X is given by $w_2(p) = [x, -y, z]$, $w_3(p) = [-x, y, z]$, where $p = [x, y, z] \in X$. In particular, we get $V_d \cong \mathbb{P}^1_{\mathbb{Q}}$ for $d = 2, 3, 6$, and the projection maps $\pi_d : V \to V_d$, $\pi_W : V \to V_W$ are given by $\pi_2(p) = [x, z]$, $\pi_3(p) = [y, z]$, $\pi_6(p) = [x, y]$, $\pi_W(p) = [x^2, y^2]$.*

Proof. This follows immediately from theorem 11, since we know the action of W on the modular forms. $\square$

3.5 Mestre's obstruction and a family over E

Let $L(j)$ be the matrix of the quadratic form (1) where we have made the substitutions $J_2 = 12(j + 1)$, $J_4 = 6(j^2 + j + 1)$, $J_6 = 4(j^3 - 2j^2 + 1)$ and $J_{10} = j^3$.

Proposition 13. *The only curves on E which have non-trivial automorphisms are the two curves with -24 and -19 CM respectively. In both these cases, the automorphism group is isomorphic to $C_2 \times C_2$.*

Proof. The curve C with $j(C) = j$ has non-trivial automorphisms if and only if the matrix $L(j)$ has vanishing determinant. Now we get

$$\det(L(j)) = -2^{33}3^{-18}5^{-20}j^7(64j-81)^2(27j+16),$$

so the first claim follows immediately from our computations in section 3.3.

It is well known, see [1], that any genus 2 curve with automorphism group other than C_2 or $C_2 \times C_2$ has a model of the form $y^2 = x^5 + tx^3 + x$ or $y^2 = x^6 + tx^3 + 1$ for some $t \in \mathbb{C}$, or is the exceptional curve $y^2 = x^5 - x$. By comparing Igusa invariants, one checks that neither of the curves $C_{(-24)}$ and $C_{(-19)}$ can be written in this form. □

Consider now the matrix $N(j) =$

$$3^2 \begin{pmatrix} -32(96j^3 - 76j^2 + 75j - 108) & 48(296j^3 - 13j^2 - 564j) & 16(2856j^3 - 2389j^2 + 684j + 864) \\ 1800(8j^2 - 6j - 9) & 38700(2j^2 - 3j) & 900(242j^2 - 65j - 72) \\ 16875(8j - 9) & 50625j & 16875(j - 36) \end{pmatrix}.$$

We have $\det(N(j)) = 2^7 3^{11} 5^{10} j^3 (64j-81)^2$, and get

$$N(j)^t L(j) N(j) = -2^{15}3j^4(64j-81)^2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6j & 0 \\ 0 & 0 & 2(27j+16) \end{pmatrix}. \qquad (7)$$

Hence we have:

Proposition 14. *If C is on E and has trivial automorphisms, then the Mestre obstruction H_C is the quaternion algebra*

$$(-6j, -2(27j+16))_{k_{\mathbb{Z}}}.$$

Now we can get explicit equations for the sextic in the case of trivial automorphism groups:

Theorem 15. *The curve C is defined over (for example) the field $K = \mathbb{Q}(\sqrt{-6j})$. An explicit equation is*

$$\begin{aligned} f(x) =& (-4+3s)x^6 + 6tx^5 + 3t(28+9s)x^4 - 4t^2x^3 \\ &+ 3t^2(28-9s)x^2 + 6t^3x - t^3(4+3s), \end{aligned}$$

where $t = -2(27j+16)$, $s = \sqrt{-6j}$, i.e. the corresponding genus 2 curve $C : y^2 = f(x)$ lies on E and $j(C) = j$.

Proof. We see immediately from (7) that the Mestre conic (1) is parametrised by

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = N(j) \begin{pmatrix} x^2 + ty^2 \\ x^2 - ty^2 \\ -2sxy \end{pmatrix}.$$

Plugging this into the Mestre cubic (2), we get the result after dehomogenisation and a slight simplification. □

Corollary 16. *For any point $z \in \mathcal{H}$, the curve $C_z : y^2 = g_z(x)$, where*

$$\begin{aligned} g_z(x) = & h_4^3(z)(x^6 - 21x^4 - 21x^2 + 1)+ \\ & + \sqrt{-6}h_6^2(z)(x^6 + 9x^4 - 9x^2 - 1)+ \\ & + 2\sqrt{2}h_{12}(z)x(3x^4 - 2x^2 + 3) \end{aligned}$$

is a point on E with $j(C_z) = j(z)$ and Jacobian isomorphic to (A_z, ρ_z).

Proof. Using theorem 11, we get that

$$s = \frac{4\sqrt{-6}h_2^6(z)}{3h_4^3} \quad \text{and} \quad t = \frac{32h_{12}^2(z)}{h_4^6(z)},$$

which gives the result in the case of trivial automorphism group. One can also verify that the model works also for the two points with -19 and -24 CM respectively. □

3.6 Arithmetic properties

Proposition 17. *The field of moduli of the curve C is $k_{\mathbb{Z}} = \mathbb{Q}[j(C)]$.*

Proof. If σ is an automorphism of $\mathbb{C}$, then $C^\sigma \cong C$ if and only if $j(C^\sigma) = j(C)$ if and only if $j(C)^\sigma = j(C)$. The claim follows. □

Theorem 18. *The diagram*

$$\begin{tikzcd} & k_{\mathcal{O}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ k_{R_2} \arrow[dr, dash] & k_{R_6} \arrow[d, dash] & k_{R_3} \arrow[dl, dash] \\ & k_{\mathbb{Z}} & \end{tikzcd}$$

is given by

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{j}, \sqrt{-(27j+16)}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{-(27j+16)}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{j}) \arrow[d, dash] & \mathbb{Q}(\sqrt{-(27j+16)/j}) \arrow[dl, dash] \\ & \mathbb{Q}(j) & \end{tikzcd}$$

Proof. That $k_{\mathcal{O}} = \mathbb{Q}(\sqrt{j}, \sqrt{-(27j+16)})$ follows from theorem 11. That $k_{\mathbb{Z}}$ is $\mathbb{Q}[j(C)]$ is proposition 17. By the moduli property of V_d and by the explicit descriptions of the maps given in theorem 11, we see that the two diagrams are the same. □

Proposition 19. *If K is a field of definition of C, then $L = K \cdot k_{\mathcal{O}}$ is a field of definition of the endomorphisms, i.e.* $\mathrm{End}_L(A) \cong \mathcal{O}$.

Proof. By theorem 1.1 in [13], it is enough to show that the field L splits B. Now we get

$$B \otimes_{\mathbb{Q}} k_{\mathcal{O}} \cong H_C \otimes_{k_{\mathbb{Z}}} k_{\mathcal{O}},$$

since $H_C \otimes_{k_{\mathbb{Z}}} k_{\mathcal{O}} \cong (-6j, -2(27j+16))_{k_{\mathcal{O}}} \cong (-6,2)_{k_{\mathcal{O}}} \cong B \otimes_{\mathbb{Q}} k_{\mathcal{O}}$. But

$$H_C \otimes_{k_{\mathbb{Z}}} K \cong M_2(K)$$

since K is a field of definition for C, so we get

$$B \otimes_{k_{\mathbb{Z}}} L \cong M_2(L). \qquad \square$$

Remark. It follows that the curve C is always defined over the field $k_{\mathcal{O}}[\sqrt{-6}]$.

The following results show that our choice of j function is reasonable from an arithmetic point of view.

Proposition 20. *Let C on E be such that $k_{\mathbb{Z}}$ is a number field. Then C has potentially good reduction at a prime p not dividing 6 if and only if*

$$v_p(j) = 0. \tag{8}$$

In fact, the curve attains good reduction over the field

$$K = k_{\mathbb{Z}}[\sqrt{-6j}, \sqrt{-2(27j+16)}] \subseteq k_{\mathcal{O}}[\sqrt{2}, \sqrt{-3}].$$

Proof. First we prove that (8) is necessary. Recall that, with notations as in the proof of proposition 6, we have $j = D^2/B^5$. Also, equations 4 show that $p \mid D$ if and only if $p \mid B$. If the curve has potentially good reduction at p, then there exists an integral model over some extension field such that D is a unit at p. Hence B is also a unit at p, so (8) follows.

To prove that (8) is sufficient, we use our model in theorem 15. If we let $u = \sqrt{t}$, the model simplifies to

$$y^2 = (-4+3s)x^6 + 6ux^5 + 3(28+9s)x^4 - 4ux^3 + 3(28-9s)x^2 + 6ux - (4+3s).$$

In this model, we have $j = -s^2/6$ and $J_{10} = 2^{27}3^{12}s^6$. Hence, if j is a unit in $\mathfrak{O}_p$, then so is the discriminant $2^{12}J_{10}$. $\square$

4 Discriminant 10 case

Now we want to do exactly the same thing in the discriminant 10 case as we have done for discriminant 6. The presentation will however be briefer this time, and we omit proofs in those cases where they are completely analogous to what we have already done.

Let $B = \mathbb{Q}(i,j)$, where $i^2 = 2$, $j^2 = 5$ and $ij + ji = 0$, so $\Delta = \operatorname{disc}(B) = 10$. We choose the maximal order $\mathcal{O} = \mathbb{Z}[i, (1+j)/2]$ in B, and the element $\mu = ij \in \mathcal{O}$ with $\mu^2 = -10$. We let $R_{10} = \mathbb{Z}[\mu] \cong \mathbb{Z}[\sqrt{-10}]$. There are two twisting rings in this case, namely $R_2 = \mathbb{Z}[i] \cong \mathbb{Z}[\sqrt{2}]$ and $R_5 = \mathbb{Z}[(1+j)/2] \cong \mathbb{Z}[(1+\sqrt{5})/2]$.

The ring of modular forms with respect to Γ is generated by one element $g(z)$ of weight 4 and three forms $a_2(z)$, $a_5(z)$ and $a_{10}(z)$ of weight 6. The ring of modular forms with respect to Γ_d is generated by $g(z)$ and $a_d(z)$, for $d = 2$, 5 and 10. The ring with respect to $\tilde{\Gamma}$ is generated by $g(z)$. We can normalise the forms such that

$$\begin{aligned} a_2^2 + 2a_5^2 + a_{10}^2 &= 0, \\ 4g^3 + 27a_5^2 + a_{10}^2 &= 0. \end{aligned}$$

Furthermore, we get a holomorphic isomorphism $j_m : V_W(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ by

$$j_m(z) = \frac{g^3(z)}{a_2^2(z)}.$$

It is clear from our choice of normalization, that

$$\begin{aligned} j_m(z_{(-3)}) &= 0, & j_m(z_{(-8)}) &= \infty, \\ j_m(z_{(-20)}) &= 1/4, & j_m(z_{(-40)}) &= 27/8. \end{aligned} \tag{9}$$

where $z_{(D)}$ denotes a point on $V_W(\mathbb{C})$ whose abelian surface have D CM (which is unique for the above values of D).

Theorem 21 ([9]). *The following equations give a family of QM-curves with respect to $\mathcal{O}_{10}$:*

$$y^2 = x(P^2x^4 + P^2(1+R)x^3 + PQx^2 + P(1-R)x + 1)$$

with

$$P = \frac{4(2t+1)(t^2-t-1)}{(t-1)^2}, \quad R = \frac{(t-1)s}{t(t+1)(2t+1)},$$
$$Q = \frac{(t^2+1)(t^4+8t^3-10t^2-8t+1)}{t(t-1)^2(t+1)^2},$$

where

$$s^2 - t(t-2)(2t+1) = 0.$$

The equations for E in terms of $J_2, \ldots, J_{10}$ are significantly more complicated in this case, so we do not write them here. Let E_0 be the closure of the image of E in $\mathbb{P}(2, 4, 6, 10)$. It turns out that E_0 has one singular point $[12, 6, 4, 0]$, where it has two cusps meeting with different tangent directions. This point is the only intersection point with E_0 and the curve $J_{10} = 0$. It also turns out, that E_0 is not a complete intersection, which of makes it more difficult to find nice equations as we had in the discriminant 6 case. We can however find a parametrisation of E:

Proposition 22. *We have an isomorphism $j : E \to \mathbb{P}^1 \setminus \{0, \infty\}$ which is given by*

$$j = \frac{23751C^2 - 501060ABC + 2641541A^2B^2 - 37046420B^3}{2169C^2 - 34404ABC - 16709A^2B^2 + 37046420B^3}$$

where

$$A = 5J_2, \quad B = J_2^2 - 24J_4, \quad C = 5(33J_2^3 - 992J_2J_4 + 3600J_6).$$

The inverse is map is given by $[J_2, J_4, J_6, J_{10}] = [J_2(j), J_4(j), J_6(j), J_{10}(j)]$, *where*

$$\begin{aligned} J_2(j) &= 12j^2 - 16j + 12, \\ J_4(j) &= 6j^4 - 16j^3 + 6j^2 - 16j + 6, \\ J_6(j) &= 4j^6 - 16j^5 + 32j^3 - 8j^2 - 16j + 4, \\ J_{10}(j) &= j^4. \end{aligned}$$

For future reference, we also note the formula

$$j^2 = \frac{(J_2^2 - 24J_4)^5}{20^{10}J_{10}^2}. \tag{10}$$

Remark. The map from the family in theorem 21 to the curve E is of degree 12 and is given by

$$j = \frac{(t^2-1)^3}{4t(t^2-2t-1)^2}.$$

Proposition 23. *The following curves $C_{(D)}$ have D CM:*

$$\begin{aligned} C_{(-20)} &: y^2 = x^5 - \sqrt{5}x^3 + x, \\ C_{(-40)} &: y^2 = (2-\sqrt{5})x^6 + (30+51\sqrt{5})x^4 + (30-51\sqrt{5})x^4 + (2+\sqrt{5}), \\ C_{(-27)} &: y^2 = x^6 - (189+64\sqrt{-3})x^4 - (189-64\sqrt{-3})x^2 + 1, \\ C_{(-35)} &: y^2 = (2-\sqrt{5})x^6 + (30+19\sqrt{5})x^4 + (30-19\sqrt{5})x^4 + (2+\sqrt{5}). \end{aligned}$$

Proof. The proof of the last three cases is analogous to the proof of proposition 8. In the first case one gets in a similar way that the Jacobian is isomorphic to $E \times E$, where $E = \mathbb{C}/\mathbb{Z}[\sqrt{-5}]$. A splitting map

$$C_{(-20)} \to \{Y^2 = (X+2)(X^2 - 2 - \sqrt{5})\} \cong E$$

is given by

$$X = \frac{x^2+1}{x}, \quad Y = \frac{y(x^3+1)}{x^2(x^2-x+1)}. \qquad \square$$

It is easy to verify that the curves $C_{(D)}$ from proposition 23 lies on E, and we have

$$\begin{aligned} j(C_{(-20)}) &= 1/4, & j(C_{(-40)}) &= 27/8, \\ j(C_{(-27)}) &= -24/25, & j(C_{(-35)}) &= 8/7. \end{aligned} \tag{11}$$

Now we consider then matrix $L(j)$ corresponding to (1). We get

$$\det(L(j)) = -2^{33}3^{-18}5^{-20}j^{10}(4j-1)^2(25j+24)^2(7j-8)^2(8j-27).$$

In this case, one can find a matrix $N(j)$ with coefficients in $\mathbb{Z}[j]$ such that

$$N(j)^t L(j) N(j) = \\ -2^{15} 5 j^6 (7j-8)^2 (25j+24)^2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10(1-4j) & 0 \\ 0 & 0 & -2(8j-27)(1-4j) \end{pmatrix}. \tag{12}$$

Hence we get

Proposition 24. *If C is on E and has trivial automorphisms, then the Mestre obstruction H_C is the quaternion algebra*

$$(-10(1-4j), 5(8j-27))_{k_{\mathbb{Z}}}.$$

Lemma 25. *The -3 and -8 CM surfaces on $\tilde{E}_{10}$ have the product polarizations, hence neither of them is a Jacobian of a genus 2 curve.*

Proof. In the -3 CM case, there are only the product polarization (see [10]), so there is nothing to prove.

In the -8 CM case, one can use the formulas for period the matrices given in [9], p. 290 and find a period matrix $Z = \Omega(z)$ of the abelian surface. It is then straightforward to find a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ such that

$$Z' = (AZ+B)(CZ+D)^{-1} = \begin{pmatrix} \sqrt{-2} & 0 \\ 0 & \sqrt{-2} \end{pmatrix}.$$

Now, Z' is clearly the period matrix of a split abelian surface with product principal polarization. □

Proposition 26. *We have $j = j_m$ on $\tilde{E}$.*

Proof. It is clear that j and j_m are related by a linear fractional transformation. We know the values of j_m in 4 points given in (9). Now it follows from lemma 25 that the set $\{j(z_{(-3)}), j(z_{(-8)})\}$ equals $\{0, \infty\}$, and we have $j(z_{(-20)}) = 1/4$ and $j(z_{(-40)}) = 27/8$ by proposition 23. The claim follows. □

Theorem 27. *The expressions $\sqrt{1-4j}$ and $\sqrt{8j-27}$ lift to meromorphic functions on V. Furthermore, the map $f : V \to X = \{x^2 + 2y^2 + z^2 = 0\}$ given by*

$$f(z) = [a_2(z), a_5(z), a_{10}(z)] = [5, \sqrt{1-4j}, \sqrt{8j-27}]$$

is an isomorphism defined over $\mathbb{Q}$.

Proof. The first claim follows from the identities $1-4j = (5a_5/a_2)^2$ and $8j-27 = (5a_{10}/a_2)^2$.

Let $K_1 = \mathbb{Q}(\sqrt{-2}, \sqrt{-3})$. The elliptic points z_3, z_3' and the fixed points $z_{(-8)}, z'_{(-8)}$ of w_2 belongs to $V(K_1)$, and maps to $[5, 1, \pm\sqrt{-3}]$ and $[0, 1, \pm\sqrt{-2}]$ respectively. Hence the map is defined over K_1.

Let $K_2 = H(\mathbb{Q}(\sqrt{-35})) = \mathbb{Q}(\sqrt{-7}, \sqrt{5})$. The 4 points with -35 CM are defined over K_2, and by proposition 23, we have that $j = 8/7$ for these point, so they map to $[\pm\sqrt{-7}, 1, \pm\sqrt{5}]$. Hence the map is also defined over K_2 and we are done. □

Theorem 28. *The curve C is defined over the field $K = \mathbb{Q}(\sqrt{-10(1-4j)})$. An explicit equation is*

$$
\begin{aligned}
f(x) =& t^3(s^2+2s-10)x^6 - 4t^3(3s+4)x^5 + 15t^2(3s^2+2s+2)x^4 - 40t^2sx^3 \\
&+ 15t(-3s^2+2s-2)x^2 - 4t(3s-4)x - (s^2-2s-10),
\end{aligned}
$$

where $s = \sqrt{-10(1-4j)}/5$, $t = (8j-27)/5$.

Corollary 29. *For any point $z \in \mathcal{H}$, the curve $C_z : y^2 = g_z(x)$, where*

$$
\begin{aligned}
g_z(x) =& 5a_2^2(z)(x^6 - 3x^4 + 3x^2 - 1) + \\
& a_5^2(z)(x^6 + 45x^4 - 45x^2 - 1) - \\
& \sqrt{-2}a_2(z)a_5(z)(x^6 + 15x^4 + 15x^2 + 1) + \\
& 8\sqrt{5}a_2(z)a_{10}(z)(x^5 - x) + \\
& 2\sqrt{-10}a_5(z)a_{10}(z)(3x^5 + 10x^3 + 3x)
\end{aligned}
$$

is a point on E with $j(C_z) = j(z)$ and Jacobian isomorphic to (A_z, ρ_z).

Theorem 30. *The diagram*

$$
\begin{tikzcd}
 & k_{\mathcal{O}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
k_{R_2} \arrow[dr, dash] & k_{R_{10}} \arrow[d, dash] & k_{R_5} \arrow[dl, dash] \\
 & k_{\mathbb{Z}} &
\end{tikzcd}
$$

is given by

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{1-4j}, \sqrt{8j-27}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{(1-4j)/(8j-27)}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{1-4j}) \arrow[d, dash] & \mathbb{Q}(\sqrt{8j-27}) \arrow[dl, dash] \\
 & \mathbb{Q}(j) &
\end{tikzcd}
$$

Proposition 19 holds also in this case, with an analogous proof. We conclude that the genus 2 curve is defined over $k_{\mathcal{O}}[\sqrt{-10}]$, exactly corresponding to the result for the $D = 6$ case.

Proposition 31. *The only curves on E which have non-trivial automorphisms groups are the -20 CM curve which has group D_4, and the curves with -40, -27 and -35 CM where the group is $C_2 \times C_2$.*

Proposition 32. *Let C on E be such that $k_{\mathbb{Z}}$ is a number field. Then C has potentially good reduction at a prime p not dividing 10 if and only if*

$$v_p(j) = 0. \tag{13}$$

In fact, the curve attains good reduction over the field

$$K = k_{\mathbb{Z}}[\sqrt{-10(1-4j)}, \sqrt{5(8j-27)}] \subseteq k_{\mathcal{O}}[\sqrt{-2}, \sqrt{5}].$$

Proof. First we prove that (13) is necessary. Assume that C has good reduction over a field K at a prime p, so there is an integral model over K whose discriminant $2^{12}J_{10}$ is not divisible by p. We introduce the variables

$$A = 5J_2, \qquad C = 5(33J_2^3 - 992J_2J_4 + 3600J_6),$$
$$B = J_2^2 - 24J_4, \quad D = 20^5 J_{10}.$$

One can verify that A, B, C and D are integral at any prime not dividing 10, and D is a unit at p. Now we have, by (10), that $j = D^2/B^5$, so it is sufficient to show that also B is a unit. Now, there is a relation

$$31D^2 = B(DC - 49B^4),$$

so we are done in case $p \nmid 31$. However, modulo 31 there is a relation

$$D^2 = B(11ABD - 7A^2B^3 + 13CD - 8AB^2C + 11BC^2),$$

so B is must be a unit in this case too.

To prove that (13) is sufficient, we use the model in theorem 28 and argue exactly as in the proof of proposition 20. □

Proposition 33. *The intersection of E_6 and E_{10} in $\mathcal{M}_2$ is the single point corresponding to the curve with -43 CM.*

Proof. Plugging the parametrisation of E_{10} from proposition 22 into equations (3), we get the only solution $j = 216/1225$. Now, in table 2 we see that this j-value corresponds to the -43 CM curve. □

5 Examples and tables

In [5] Elkies found that there are 27 rational CM points on E_6 and 21 on E_{10}. We list them in tables 1 and 2 respectively, together with the additional information that we now can give about these points. The points are ordered after increasing height of j. The relations between our uniformization j and Elkies' t is $j = 16/27(t-1)$ in the discriminant 6 case, and $j = t/8$ in the discriminant 10 case. Unfortunately, the caveat in [5] that not all of these curves, for example the -163 curve on E_6, are proved to have the correct CM still applies. It should probably be easier to prove these cases now that we can give the explicit sextics, but it seems to the authors that these are still computationally difficult problems.

Example 1. Consider the curve

$$y^2 = (x^2+5)((-1/6+\sqrt{2})x^4 + 20x^3 - 490/6x^2 + 100x + 25(-1/6-\sqrt{2}))$$

studied in [4]. This has discriminant 6 QM with $j = -9/128$. We get $k_{R_6} = \mathbb{Q}(\sqrt{-2})$, $k_{R_2} = \mathbb{Q}(\sqrt{-10})$, $k_{R_3} = \mathbb{Q}(\sqrt{5})$ and $k_{\mathcal{O}} = \mathbb{Q}(\sqrt{5}, \sqrt{-2})$, which is consistent with and somewhat more precise than the results in [4].

D	j	k_{R_2}	k_{R_6}	k_{R_3}	$\mathrm{disc}(H_C)$
-3	∞	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3})$	no curve
-4	0	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}$	$\mathbb{Q}$	no curve
-24	$-2^4/3^3$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$	–
-19	$3^4/2^6$	$\mathbb{Q}(\sqrt{-19})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-19})$	–
-40	$2^4 3^4/5^3$	$\mathbb{Q}(\sqrt{-10})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-2})$	$2\cdot\infty$
-51	$-7^4/(2^6 3^3)$	$\mathbb{Q}(\sqrt{17})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-51})$	1
-84	$-2^6 7^2/3^6$	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$	$2\cdot 3$
-52	$-2^6 3^4/5^6$	$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{13})$	$2\cdot 13$
-120	$2^4 7^4/(3^6 5^3)$	$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-3})$	$3\cdot\infty$
-75	$11^4/(2^6 3^6 5^1)$	$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-3})$	$3\cdot\infty$
-132	$-2^8 11^2/(3^3 5^6)$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{3})$	1
-43	$3^4 7^4/(2^6 5^6)$	$\mathbb{Q}(\sqrt{-43})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-43})$	$43\cdot\infty$
-168	$-2^4 7^2 11^4/(3^3 5^6)$	$\mathbb{Q}(\sqrt{6})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-2})$	$2\cdot 3$
-88	$-2^4 3^4 7^4/(5^6 11^3)$	$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Q}(\sqrt{-11})$	$\mathbb{Q}(\sqrt{2})$	$2\cdot 11$
-100	$2^8 3^4 5^1 7^4/11^6$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-5})$	$5\cdot\infty$
-123	$-7^4 19^4/(2^6 3^3 5^6)$	$\mathbb{Q}(\sqrt{41})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-123})$	1
-228	$2^{10} 7^4 19^2/(3^9 5^6)$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{-3})$	$2\cdot\infty$
-67	$3^4 7^4 11^4/(2^{12} 5^6)$	$\mathbb{Q}(\sqrt{-67})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-67})$	$67\cdot\infty$
-147	$-11^4 23^4/(2^6 3^6 5^6 7^1)$	$\mathbb{Q}(\sqrt{21})$	$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Q}(\sqrt{-3})$	$3\cdot 7$
-148	$-2^6 3^4 7^4 11^4/(5^6 17^6)$	$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{37})$	$2\cdot 37$
-312	$-2^4 7^4 23^4/(3^3 5^6 11^6)$	$\mathbb{Q}(\sqrt{-39})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{13})$	$3\cdot 13$
-372	$-2^6 7^4 19^4 31^2/(3^6 5^6 11^6)$	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$	$2\cdot 3$
-408	$-2^4 7^4 11^4 31^4/(3^9 5^6 17^3)$	$\mathbb{Q}(\sqrt{17})$	$\mathbb{Q}(\sqrt{-51})$	$\mathbb{Q}(\sqrt{-3})$	1
-267	$-7^4 31^4 43^4/(2^{12} 3^3 5^6 11^6)$	$\mathbb{Q}(\sqrt{89})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-267})$	1
-232	$2^4 3^4 7^4 11^4 19^4/(5^6 23^6 29^3)$	$\mathbb{Q}(\sqrt{-58})$	$\mathbb{Q}(\sqrt{29})$	$\mathbb{Q}(\sqrt{-2})$	$2\cdot\infty$
-163	$3^8 7^4 19^4 23^4/(2^6 5^6 11^6 17^6)$	$\mathbb{Q}(\sqrt{-163})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-163})$	$163\cdot\infty$
-708	$-2^{12} 7^4 11^4 47^4 59^2/(3^3 5^6 17^6 29^6)$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{3})$	1

Table 1: Rational CM points on E_6

D	j	k_{R_2}	$k_{R_{10}}$	k_{R_5}	$\mathrm{disc}(H_C)$
-3	0	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3})$	no curve
-8	∞	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}$	$\mathbb{Q}$	no curve
-20	$1/2^2$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-1})$	–
-35	$2^3/7$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Q}(\sqrt{-35})$	–
-27	$-2^3 3/5^2$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3})$	–
-40	$3^3/2^3$	$\mathbb{Q}$	$\mathbb{Q}\sqrt{-2}$	$\mathbb{Q}$	–
-52	$-3^3/(2^2 5^2)$	$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Q}(\sqrt{13})$	$\mathbb{Q}(\sqrt{-1})$	$13 \cdot \infty$
-120	$-3^3/(2^3 7^2)$	$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Q}(\sqrt{10})$	$\mathbb{Q}(\sqrt{-6})$	$3 \cdot \infty$
-72	$5^3/(2^3 3^1 7^2)$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{6})$	$\mathbb{Q}(\sqrt{-3})$	$3 \cdot \infty$
-43	$2^3 3^3/(5^2 7^2)$	$\mathbb{Q}(\sqrt{-43})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-43})$	$43 \cdot \infty$
-180	$-11^3/(2^2 13^2)$	$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Q}(\sqrt{15})$	$\mathbb{Q}(\sqrt{-1})$	$2 \cdot \infty$
-88	$3^3 5^3/(2^4 7^2)$	$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Q}(\sqrt{-11})$	$\mathbb{Q}(\sqrt{2})$	$2 \cdot 11$
-115	$2^6 3^3/(13^2 23)$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-23})$	$\mathbb{Q}(\sqrt{-115})$	$5 \cdot 23$
-67	$-2^3 3^3 5^3/(7^2 13^2)$	$\mathbb{Q}(\sqrt{-67})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-67})$	$67 \cdot \infty$
-280	$3^3 11^3/(2^4 7^1 23^2)$	$\mathbb{Q}(\sqrt{10})$	$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Q}(\sqrt{-14})$	$2 \cdot 7$
-340	$3^3 23^3/(2^2 7^2 29^2)$	$\mathbb{Q}(\sqrt{17})$	$\mathbb{Q}(\sqrt{-17})$	$\mathbb{Q}(\sqrt{-1})$	$2 \cdot 17$
-148	$3^3 11^3/(2^2 5^2 7^2 13^2)$	$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Q}(\sqrt{37})$	$\mathbb{Q}(\sqrt{-1})$	$37 \cdot \infty$
-520	$3^3 29^3/(2^6 7^2 13^1 47^2)$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{13})$	$\mathbb{Q}(\sqrt{-26})$	$2 \cdot \infty$
-232	$3^3 11^3 17^3/(2^5 5^2 7^2 23^2)$	$\mathbb{Q}(\sqrt{-58})$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{29})$	1
-163	$-2^6 3^3 5^3 11^3/(7^2 13^2 29^2 31^2)$	$\mathbb{Q}(\sqrt{-163})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-163})$	$163 \cdot \infty$
-760	$3^3 17^3 47^3/(2^3 7^2 31^2 71^2)$	$\mathbb{Q}(\sqrt{-95})$	$\mathbb{Q}(\sqrt{-38})$	$\mathbb{Q}(\sqrt{10})$	$5 \cdot 19$

Table 2: Rational CM points on E_{10}

Example 2. The curve

$$y^2 = 1/48x(9075x^4 + 3025(3 + 2\sqrt{-3})x^3 - 6875x^2 + 220(-3 + 2\sqrt{-3}x + 48)),$$

which is studied in [3] and [22], has discriminant 10 QM. We have $j = -32/147$, and hence we get $k_{R_{10}} = \mathbb{Q}(\sqrt{33})$, $k_{R_2} = \mathbb{Q}(\sqrt{-11})$, $k_{R_5} = \mathbb{Q}(\sqrt{-3})$ and $k_{\mathcal{O}} = \mathbb{Q}(\sqrt{-3}, \sqrt{-11})$.

Example 3. From table 1, we see for example that the curve with -132 CM on E_6 is defined over $\mathbb{Q}$. An explicit equation is given by

$$y^2 = 73x^6 - 750x^5 + 966x^4 + 2000x^3 - 876x^2 - 3000x - 1288.$$

To find this explicit model from the invariants $J_2, \ldots, J_{10}$, we used the PARI/GP package of Paul B. van Wamelen for computations of genus 2 curves.

Example 4. We consider an example of CM points with non-rational j-value. There are two points with -91 CM points on E_6, which we denote $z_{(-91)}$ and $z'_{(-91)}$. The j-values of these points belong to $H(\mathbb{Q}(\sqrt{-91})) = \mathbb{Q}(\sqrt{-7}, \sqrt{13})$. Numerically (up to several hundred decimals) we get

$$j(z_{(-91)}) = \overline{j(z'_{(-91)})} = \frac{3^4 p_7^4 p_{11}^4}{p_2^6 \overline{p}_2^{12} \overline{p}_{11}^6},$$

where $p_2 = (1 + \sqrt{-7})/2$, $p_7 = \sqrt{-7}$ and $p_{11} = 2 + \sqrt{-7}$.

A Restriction of Hilbert modular forms

In this appendix, we describe how to construct modular forms with respect to a cocompact quaternionic groups over $\mathbb{Q}$ in a way that is suitable for numerical computations. We start by embedding the curve into a suitable Hilbert modular surface. Note that our description of this embedding is just a reformulation of the classical construction of Hirzebruch-Zagier cycles [11]. The key to constructing modular forms with respect to the quaternionic group is to introduce a certain factor such that restriction of modular forms on $\mathcal{H} \times \mathcal{H}$ times this factor gives modular forms with respect to the quaternionic group. A special case of this occurs in [8].

Let $k = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is a square free integer. Let D be the discriminant of the field k, $\mathfrak{O}$ the ring of integers in k and the nontrivial automorphisms of k is denoted by $x \mapsto \overline{x}$. Consider the algebra $A = M_2(k)$. The canonical involution on A is given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^* = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Let $\Lambda = M_2(\mathfrak{O})$. The Hilbert modular group $\Gamma = \mathrm{SL}_2(\mathfrak{O})$ acts on $\mathcal{H} \times \mathcal{H}$ by $\gamma(z_1, z_2) = (\gamma z_1, \overline{\gamma} z_2)$. Let $\beta \in \Lambda$ with $\overline{\beta}^* = \beta$, $\beta \in \mathbb{Z} + \sqrt{D}\Lambda$ and $\det(\beta) > 0$. We assume furthermore that β is primitive, i.e. if $\beta = n\beta_0$ where β_0 has the same properties and $n \in \mathbb{Z}$, then $n = \pm 1$. Consider

$$\Lambda_\beta = \{\lambda \in \Lambda \mid \beta\lambda = \overline{\lambda}\beta\},$$

which is an order in an indefinite quaternion algebra over $\mathbb{Q}$. The discriminant of the order Λ_β is $\det(\beta)$ (cf. [7]). Let

$$C_\beta = \{(z, \beta z) \mid z \in \mathcal{H}\} \subset \mathcal{H} \times \mathcal{H}.$$

The group $\Gamma_\beta = \{\gamma \in \Lambda^1 \mid \beta\gamma = \pm\overline{\gamma}\beta\} \supseteq \Lambda_\beta^1$ acts on $C_\beta \cong \mathcal{H}$.

Our aim is to construct modular forms with respect to the group Γ_β. Let F be a Hilbert modular form with respect to Γ of weight (k_1, k_2), i.e. $F : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ is holomorphic and satisfies

$$F(\gamma z_1, \overline{\gamma} z_2) = j(\gamma, z_1)^{k_1} j(\overline{\gamma}, z_2)^{k_2} F(z_1, z_2),$$

for all $\gamma \in \Gamma$. Here $j(\alpha, z) = cz + d$ for any real matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We define a function

$$f(z) = j(\beta, z)^{-k_2} F(z, \beta z), \quad z \in \mathcal{H}.$$

Now, for $\gamma \in \Gamma_\beta$, we get $j(\beta, \gamma z) j(\gamma, z) = j(\beta\gamma, z) = \pm j(\overline{\gamma}\beta, z) = \pm j(\overline{\gamma}, \beta z) j(\beta, z)$, so

$$\frac{j(\overline{\gamma}, \beta z)}{j(\beta, \gamma z)} = \pm \frac{j(\gamma, z)}{j(\beta, z)}, \tag{14}$$

where the sign is the same as the sign in the equation $\beta\gamma = \pm\overline{\gamma}\beta$.

Proposition 34. *The function f is a modular form with respect to Λ_β^1 of weight $k_1 + k_2$. If k_2 is even, then it is also a modular form with respect to Γ_β.*

Proof. The function f is obviously holomorphic. By (14), we get

$$\begin{aligned} f(\gamma z) =& j(\beta, \gamma z)^{-k_2} F(\gamma z, \beta\gamma z) \\ =& j(\beta, \gamma z)^{-k_2} F(\gamma z, \overline{\gamma}\beta z) \\ =& j(\beta, \gamma z)^{-k_2} j(\gamma, z)^{k_1} j(\overline{\gamma}, \beta z)^{k_2} F(z, \beta z) \\ =& j(\beta, z)^{-k_2} j(\gamma, z)^{k_1} j(\gamma, z)^{k_2} F(z, \beta z) \\ =& j(\gamma, z)^{k_1 + k_2} f(z), \end{aligned}$$

for any $z \in \mathcal{H}$ and $\gamma \in \Lambda_\beta^1$. The last statement is now clear. □

References

[1] O. Bolza, *On Binary Sextics with Linear Transformations onto themselves,* Am. J. Math. 10, 47–70 (1888)

[2] G. Cardona, J. Quer, *Field of moduli and field of definition for curves of genus* 2, preprint

[3] L. Dieulefait, V. Rotger, *The arithmetic of QM-abelian surfaces through their Galois representations*, to appear in j. Algebra

[4] L. Dieulefait, V. Rotger, *On abelian surfaces with potential quaternionic multiplication*,

[5] N.D. Elkies, *Shimura curve computations,* Lect. Notes in Comput. Sci. 1423, 1–47, (1998)

[6] D.R. Grayson, M.E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, Available at http://www.math.uiuc.edu/Macaulay2/

[7] G. van der Geer, *Hilbert Modular Surfaces,* Springer-Verlag, 1988

[8] T. Hiramatsu, *Eichler maps and hyperbolic Fourier expansion,* Nagoya Math. J. 40 (1970), p. 173–192

[9] K.-I. Hashimoto, N. Murabayashi, *Shimura Curves as Intersections of Humbert Surfaces and Defining Equations of QM-curves of Genus Two,* Tôhoku Math. J. 47 (1995), 272–296

[10] T. Hayashida, M. Nishi, *Existence of curves of genus two on a product of two elliptic curves,* J. Math. Soc. Japan 17, 1–16 (1965).

[11] F. Hirzebruch, D. Zagier, *Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus,* Inventiones math. 23, 1–29 (1974)

[12] J.-I. Igusa, *Arithmetic Variety of Moduli for Genus Two,* Annals of Mathematics, vol. 72, no. 3, p. 612–649 (1960)

[13] B.W. Jordan, *Points on Shimura curves rational over number fields,* J. Reine Angew. Math. 371, 92–114 (1986)

[14] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization,* J. Fac. Sci. Univ. Tokyo Sect. IA Math. 25 (1979), no. 3, 277–300.

[15] H. Lange, C. Birkenhake, *Complex Abelian Varieties,* Grundl. math. Wiss. 302, Springer, 1992

[16] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules,* Progr. Math., 94, 313–334, 1991

[17] A.P. Ogg, *Real points on Shimura curves,* Progr. Math., 35, 277–307 (1983)

[18] PARI/GP, version `2.1.5`, Bordeaux, 2004, Available at http://pari.math.u-bordeaux.fr/

[19] F. Rodriguez-Villegas, *Explicit models of Genus 2 Curves with split CM,* Lect. Notes in Comp. Sci. 1838, 505–514 (2000)

[20] V. Rotger, *Quaternions, polarizations and class numbers,* J. Reine Angew. Math. 561, 177–197 (2003)

[21] V. Rotger, *Modular Shimura varieties and forgetful maps,* Trans. Amer. Math. Soc. 356, 1535–1550 (2004)

[22] V. Rotger, *The field of moduli of quaternionic multiplication on abelian varieties*, to appear in Int. J. of Math. and Math. Sci.

[23] G. Shimura, *Introduction to the arithmetic theory of automorphic functions,* Publ. Math. Soc. Japan, no. 11, Princeton Univ. Press, 1971

[24] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains,*. Ann. of Math. 91, 144–222 (1970)

[25] G. Shimura, *Construction of class fields and zeta functions of algebraic curves,* Ann. of Math. 85, 58–159 (1967)

[26] M.-F. Vignéras, *Arithmétique des algèbres de quaternions,* Springer-Verlag, Berlin, 1980.

Srinath Baba: Department of Mathematics, McGill University, 800 Sherbrooke street West, Montreal, Quebec, Canada- H3A 2T5
E-mail address: sbaba@math.mcgill.ca

Håkan Granath: Max-Planck-Institut für Mathematik, Vivatsgasse 7, DE-53111 Bonn, Germany
E-mail address: granath@mpim-bonn.mpg.de