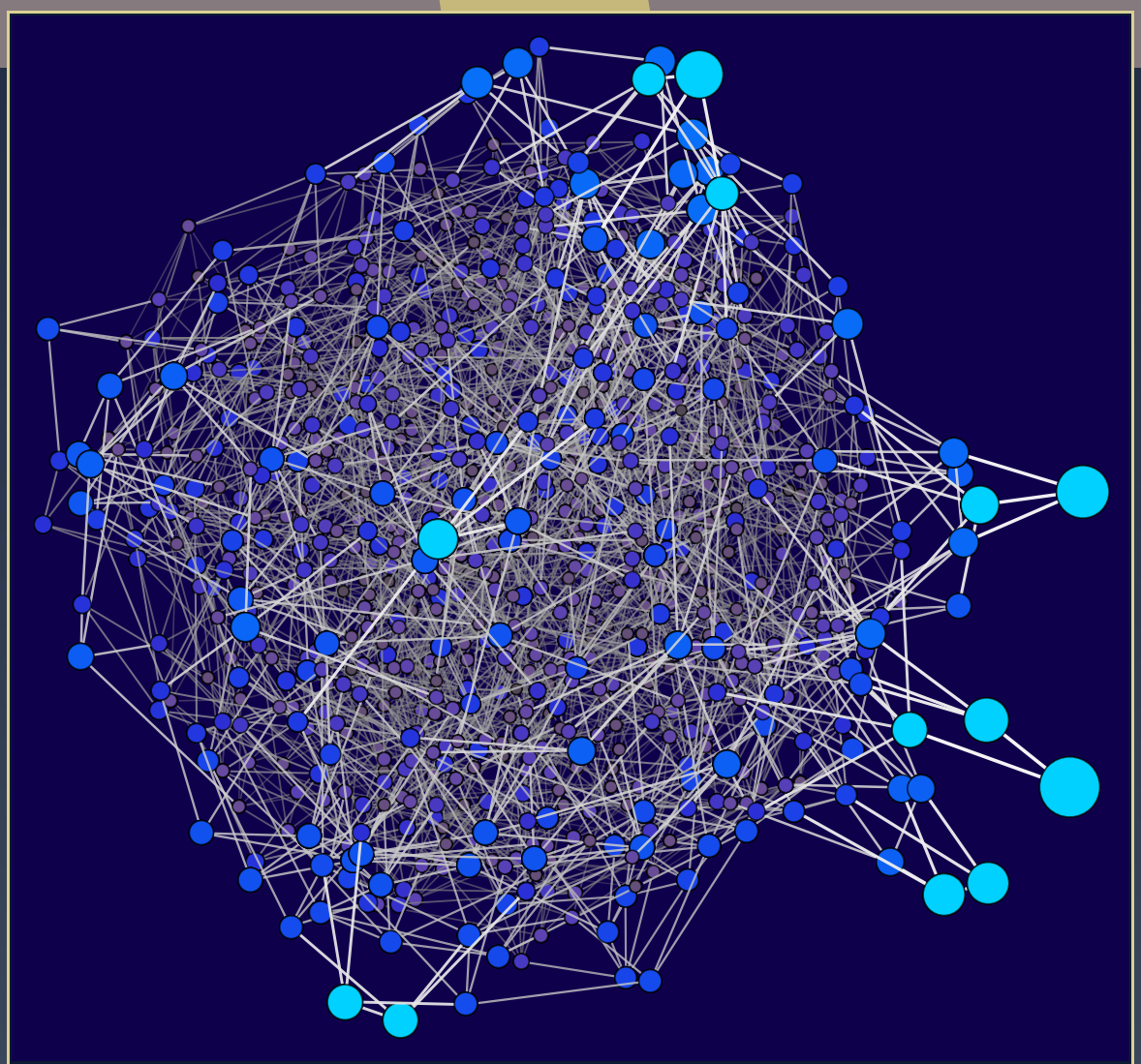
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Genus 3 hyperelliptic curves with CM via Shimura reciprocity

Bogdan Adrian Dina and Sorina Ionica



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.161

Genus 3 hyperelliptic curves with CM via Shimura reciprocity

Bogdan Adrian Dina and Sorina Ionica

Up to isomorphism, every three-dimensional simple principally polarized abelian variety over $\mathbb{C}$ is the Jacobian of a smooth projective curve of genus 3. Furthermore, this curve is either a hyperelliptic curve or a plane quartic. To define hyperelliptic class polynomials, we note that given a hyperelliptic Jacobian with CM, all principally polarized abelian varieties that are Galois conjugated to it are hyperelliptic. Using Shimura's reciprocity law, we then compute approximations of the invariants of the initial curve, as well as their Galois conjugates. We show examples of class polynomials computed using this method for the Shioda and Rosenhain invariants.

1. Introduction

Shimura and Taniyama's complex multiplication theory shows that it is possible to construct certain abelian extensions of CM fields by computing the values of Siegel modular functions evaluated at points with CM in the Siegel upper half-space. In addition, the effective computation of these modular forms makes it possible to compute models for CM curves, and also to effectively construct the related class fields.

For example, in genus one, the field of modular functions of level 1 is generated by the j-invariant. It is well known that the j-invariant of an elliptic curve with endomorphism ring isomorphic to the ring of integers of the CM field K generates the Hilbert class field of K. In the genus 2 case, the field of Siegel modular functions of level 1 is generated by the absolute Igusa invariants [11]. Similarly, when evaluated at CM points, their values give invariants of a hyperelliptic curve whose Jacobian has CM, and the class field equations, known as class polynomials, are recovered by computing these invariants for all curves with CM by the field [22; 8]. In genus 3, every simple principally polarized abelian variety (p.p.a.v.) over $\mathbb{C}$ of dimension 3 is isomorphic to the Jacobian of a complete smooth projective curve, which is either a hyperelliptic curve or a plane quartic. Since two different sets of invariants for both genus 3 hyperelliptic curves and plane quartics are known in the literature, it is more difficult to tackle the problem of computing class polynomials for genus 3.

MSC2010: 11G10, 11G15, 11G30.
Keywords: hyperelliptic curve, complex multiplication, theta constants, class field.

In [27, Lemma 4.5], Weng shows that a simple principally polarized abelian threefold with CM by a sextic CM field containing $\mathbb{Q}(i)$ is a hyperelliptic Jacobian. In the same paper, Weng gives an algorithm to compute hyperelliptic curves whose Jacobians have CM by a sextic field containing $\mathbb{Q}(i)$. In later work, Balakrishnan, Ionica, Lauter, and Vincent [1] give an algorithm which removes this restriction on the CM field, by performing a heuristic check. This heuristic relies on Mumford's Vanishing Criterion [16; 18], which states that a genus 3 curve is hyperelliptic if and only if one of the 36 even theta constants is 0. Given a period matrix with CM by a sextic CM field, the algorithm in [1] first computes the theta constants with enough precision to see if there is one which approximates zero, and then computes the Rosenhain invariants. These invariants generate a certain subfield of the ray class field of modulus 2 over the reflex field K^r of K and by approximating them with high precision, we can recognize them as algebraic numbers. This method has its limitations, since as soon as the degree of the class field over which the Rosenhains are defined is large (≥ 500), the complexity of the algebraic dependance computation becomes a bottleneck. From a concrete point of view, only examples of CM fields with class number 1 were considered in [1].

In this paper, we extend the work in [1; 2] by considering the action on a hyperelliptic CM point of the Galois group $\mathrm{Gal}(CM_{\mathfrak{m}}(K^r)/K^r)$, where $CM_{\mathfrak{m}}(K^r)$ is a subfield of the ray class field of a given modulus $\mathfrak{m}$.

Once we identify a hyperelliptic curve X by verifying computationally and heuristically the vanishing criterion condition, we compute the Galois conjugates of its invariants via Shimura's reciprocity law. With these in hand, we compute the Shioda and Rosenhain class polynomials given by

$$H^R_{K^r,i}(t) = \prod_{\sigma}(t - \lambda_i^{\sigma}) \quad \text{and} \quad H^S_{K^r,j}(t) = \prod_{\sigma}(t - \mathrm{Shi}_j^{\sigma}), \tag{1-1}$$

where λ_i $(1 \leq i \leq 5)$ and Shi_j $(1 \leq j \leq 9)$ denote the Rosenhain and Shioda invariants (introduced in Section 2) and $\sigma \in \mathrm{Gal}(CM_{\mathfrak{m}}(K^r)/K^r)$, with $\mathfrak{m} = (2)$ for the product in $H^R_{K^r,i}$ and $\mathfrak{m} = (1)$ for the product in $H^S_{K^r,j}$.

Aiming to implement our results in SageMath [25] and compute examples for the class polynomials of the Rosenhain and Shioda invariants, we also propose some methods to construct the reflex field associated to a given CM type, the typenorm, as well as the image of the typenorm as a subgroup in the Shimura class group.

2. Background

This section briefly recalls the necessary background and notation on complex abelian varieties, theta functions and the Vanishing Criterion which fully characterizes hyperelliptic principally polarized abelian varieties. We also define the invariants of hyperelliptic curves that we will be computing in the next sections.

2A. ***Principally polarized abelian varieties over*** $\mathbb{C}$ ***and period matrices.*** A principally polarized abelian variety defined over $\mathbb{C}$ is isomorphic to a complex torus admitting a Riemann form [3, Chapter 4]. Let

$g \geq 1$ and let $A = \mathbb{C}^g/\Lambda$, with Λ a full lattice in $\mathbb{C}^g$ and E a Riemann form for $(\mathbb{C}^g, \Lambda)$. We will write (A, E) to denote the g-dimensional p.p.a.v. over $\mathbb{C}$. We consider a *symplectic* basis for the lattice Λ, by which we mean the action of E on Λ with respect to this basis is given by the matrix

$$J_g = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}, \tag{2-1}$$

where I_g is the $g \times g$ identity matrix.

Let $\Omega = [\Omega_1 \mid \Omega_2]$ be the $g \times 2g$ matrix whose columns are the elements of this symplectic basis. By taking $Z = \Omega_2^{-1}\Omega_1$ we obtain a $g \times g$ matrix Z called a *period matrix*, i.e., an element of the Siegel upper half-space

$$\mathcal{H}_g = \{Z \in \mathcal{M}_g(\mathbb{C}) : Z^T = Z,\ \mathrm{Im}(Z) > 0\}.$$

We note that the lattice Λ can be written as $Z\mathbb{Z}^g + \mathbb{Z}^g$.

There is an action on $\mathcal{H}_g$ by the symplectic group

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \{M \in \mathrm{GL}_{2g}(\mathbb{Z}) : M^T J_g M = J_g\},$$

where J_g is as in equation (2-1), given by

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : Z \mapsto M.Z = (aZ + b)(cZ + d)^{-1}, \tag{2-2}$$

where on the right-hand side the multiplication of $g \times g$ matrices is the usual matrix multiplication.

The association of Z to $(\mathbb{C}^g/(Z\mathbb{Z}^g + \mathbb{Z}^g), E)$ gives a bijection between $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g$ and the moduli space of p.p.a.v. of dimension g over $\mathbb{C}$. In the remainder of this paper, we will denote this moduli space by $\mathcal{A}_g$.

2B. ***Theta functions.*** For $\omega = \binom{\omega_1}{\omega_2} \in \mathbb{R}^{2g}$ and $Z \in \mathcal{H}_g$, we define the following important theta series:

$$\vartheta(\omega, Z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i(\omega_1 + n)^t Z(\omega_1 + n) + 2\pi i(\omega_1 + n)^t \omega_2)). \tag{2-3}$$

Given a period matrix $Z \in \mathcal{H}_g$, we obtain a set of coordinates on the torus $A = \mathbb{C}^g/(Z\mathbb{Z}^g + \mathbb{Z}^g)$ in the following way: a vector $\binom{\omega_1}{\omega_2} \in \mathbb{R}^{2g}$ corresponds to the point $Z\omega_1 + \omega_2 \in \mathbb{C}^g/(Z\mathbb{Z}^g + \mathbb{Z}^g)$. Under this identification, points of the form $\xi = Z\xi_1 + \xi_2$ for $\xi = \binom{\xi_1}{\xi_2} \in \frac{1}{2}\mathbb{Z}^{2g}$ yield 2-torsion points on A. Using this notation we define

$$\vartheta[\xi](Z) = \exp(\pi i \xi_1^t Z \xi_1 + 2\pi i \xi_1^t \xi_2)\vartheta(\xi, Z). \tag{2-4}$$

In this context, ξ is called a *theta characteristic*, and the value $\vartheta[\xi](Z)$ is called a *theta constant*. We call ξ a *even* (*odd*) theta characteristic if $e_*(\xi) = 1$ ($e_*(\xi) = -1$ respectively), where $e_*(\xi) = \exp(4\pi i \xi_1^T \xi_2)$. If ξ is an even (odd) theta characteristic we call $\vartheta[\xi](Z)$ an *even (odd) theta constant*.

It can be easily shown that all odd theta constants are 0. We note that in the case where $g = 3$ there are exactly 36 even classes of theta characteristics in $\frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$. We recall there is an action of the symplectic

group $\mathrm{Sp}_{2g}(\mathbb{Z})$ on theta characteristics $\xi \in \frac{1}{2}\mathbb{Z}^{2g}$ defined by

$$M.\xi = M^*\xi + \tfrac{1}{2}\delta_0, \tag{2-5}$$

with $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$, $M^* = (M^{-1})^t$, and $\delta_0 = \left(\begin{smallmatrix} (c^t d)_0 \\ (a^t b)_0 \end{smallmatrix}\right)$ a column vector where $(c^t d)_0$ and $(a^t b)_0$ are the diagonal vectors of $c^t d$ and $a^t b$, respectively. In this context, given a period matrix $Z \in \mathcal{H}_g$, we briefly recall the transformation formula on the theta constants [3, Formula 8.6.1]

$$\vartheta[M.\xi](M.Z) = \zeta(M)\exp(k(M,\xi))\sqrt{\det(cZ+d)}\,\vartheta[\xi](Z), \tag{2-6}$$

where:

(1) $\zeta(M)$ is an eighth root of unity depending on M, having the same sign ambiguity as $\sqrt{\det(cZ+d)}$.

(2) $k(M,\xi) = \pi i (d\xi_1 - c\xi_2)^t(-b\xi_1 + a\xi_2 - (a^t b)_0) - \xi_1^t\xi_2$.

For more details on $\zeta(M)$, we refer the reader to [3, Exercice 8.11(9)].

2C. ***The Rosenhain invariants.*** Let $\mathcal{M}_g$ be the moduli space of smooth projective curves of genus g. By a theorem of Torelli [15, Theorem 12.1], there is an injective map $\mathcal{M}_g \hookrightarrow \mathcal{A}_g$. Inside $\mathcal{M}_g$ we further restrict our attention to the subspace of hyperelliptic curves $\mathcal{M}_g^{\mathrm{hyp}}$. We will be interested in the effective reconstruction of a moduli point in $\mathcal{M}_g^{\mathrm{hyp}}$ from a point in $\mathcal{A}_g$, whenever this point is in the image of $\mathcal{M}_g^{\mathrm{hyp}} \hookrightarrow \mathcal{A}_g$.

Let X be a hyperelliptic curve of genus g over $\mathbb{C}$ defined by an equation $y^2 = f(x)$, where f is a polynomial with $\deg(f) \in \{2g+1, 2g+2\}$. Let $(\lambda_i)_{1\le i\le 2g+2}$ be the distinct complex roots of f, with the convention that λ_{2g} is ∞ if $\deg(f)$ is odd. We identify these roots with the branch points for the covering map $\pi : X \to \mathbb{P}^1(\mathbb{C})$, that we denote by $P_1, \ldots, P_{2g+1}, P_\infty$. This motivates the following definition.

Definition 2.1. By a *marked* hyperelliptic curve X of genus g we understand a certain ordering of the branch points of the map π.

We will denote by $\mathcal{M}_g^{\mathrm{hyp}}[2]$ the moduli space of marked hyperelliptic curves. Let us introduce more terminology. We note that the action on $\mathcal{H}_g$ by the symplectic group of level 2

$$\Gamma_{2g}(2) = \{M \in \mathrm{Sp}_{2g}(\mathbb{Z}) : M \equiv I_{2g} \pmod 2\},$$

fixes 2-torsion points on the p.p.a.v. This leads to the following definition.

Definition 2.2. We define by $\mathcal{A}_g[2] = \Gamma_{2g}(2)\backslash\mathcal{H}_g$ *the moduli space of principally polarized abelian varieties of dimension* g *over* $\mathbb{C}$ *with a level* 2*-structure*.

We will identify the Jacobian of a marked hyperelliptic curve to a point in $\mathcal{A}_g[2]$ via the analytic construction. Let $H_1(X,\mathbb{Z})$ be the first homology group of X and let $H^0(\omega_X)$ be the group of 1-holomorphic forms on X. As explained in the literature, we view $H_1(X,\mathbb{Z})$ as a lattice in $H^0(\omega_X)^*$, the dual of $H^0(\omega_X)$ (see for example [3, Section 11.1]). As a consequence, we obtain the g-dimensional complex torus $J(X) = H^0(\omega_X)^*/H_1(X,\mathbb{Z})$. We choose a symplectic basis $\gamma_1, \ldots \gamma_{2g}$ for $H_1(X,\mathbb{Z})$ and

a basis $\omega_1, \ldots, \omega_g$ for $H^0(\omega_X)$. With the notation in Section 2A, the corresponding $g \times 2g$ matrix is $\Omega = \left(\int_{\gamma_j} \omega_i\right)_{1\le i\le g, 1\le j\le 2g}$ and $Z = \Omega_2^{-1}\Omega_1$.

Let $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\mathrm{Princ}(X)$ be the group of degree zero divisors on X modulo principal divisors. The Abel–Jacobi map yields a canonical isomorphism [3, Theorem 11.1.3]

$$AJ:\ \mathrm{Pic}^0(X) \to J(X). \tag{2-7}$$

Given a marked hyperelliptic curve X, we obtain a fixed set of 2-torsion points on $J(X)$. We take P_∞ as a base point and identify X with its image via the embedding $X \hookrightarrow \mathrm{Pic}^0(X)$. Then the branch points P_i, $i = 1, \ldots, 2g+2$, correspond to points of the form $e_i = [(P_i) - (P_\infty)]$ on $\mathrm{Pic}^0(X)$. This allows us to choose an indexed set of characteristics $\eta = (\eta_i)_{1\le i\le 2g+2}$ in $(1/2)\mathbb{Z}^{2g}$ such that

$$AJ(e_i) = Z(\eta_i)_1 + (\eta_i)_2 \ (\mathrm{mod}\ Z\mathbb{Z}^g + \mathbb{Z}^g). \tag{2-8}$$

This leads to the following definition.

Definition 2.3. Let $V = \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ the vector space over $\mathbb{F}_2$. By an *azygetic system* we understand an indexed set $\eta = (\eta_1, \ldots, \eta_{2g+2})$ of $2g+2$ vectors in $\frac{1}{2}\mathbb{Z}^{2g}$ such that the images of η_i in V, denoted by $\bar{\eta}_i$, satisfy

$$V = \mathrm{span}(\bar{\eta}_i), \quad \sum_{i=1}^{2g+1} \bar{\eta}_i = 0, \quad \bar{\eta}_{2g+2} = 0, \quad \text{and} \quad \bar{\eta}_i^t \bar{\eta}_j \equiv 1 \ (\mathrm{mod}\ 2), \tag{2-9}$$

for i, j different from $2g+2$ and $i \neq j$.

Two azygetic sets η' and η'' are said to be in the same *equivalence class* if $\bar{\eta}'_i = \bar{\eta}''_i$, $i = 1, \ldots, 2g+2$. Following Poor [18], the indexed set $(\eta_1, \ldots, \eta_{2g+2})$ obtained in equation (2-8) is an azygetic system and we call it an azygetic system *associated to the period matrix* Z.

If we change the homology basis by taking $(\gamma'_1, \ldots, \gamma'_{2g}) = (\gamma_1, \ldots, \gamma_{2g})M^t$, with $M \in \mathrm{Sp}_{2g}(\mathbb{Z})$, the new period matrix obtained using the construction above is $Z' = M.Z$. The azygetic system associated to Z' is $\eta' = (M^*\eta_1, \ldots, M^*\eta_{2g+2})$. Since the map $\mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{F}_2) \cong \mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_{2g}(2)$ is surjective, we further derive an action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ on equivalence classes of azygetic systems, which was shown to be free an transitive [18, Lemma 1.4.13].

Let us introduce some further notations. Let $T = \{1, \ldots, 2g+1, \infty\}$. For a given azygetic system, Poor defines the set $\mathcal{U}_\eta$ to be the set of indexes $i \in T$ such that η_i is even. For any $S_1, S_2 \subseteq T$ we denote the symmetric difference $S_1 \circ S_2 = (S_1 \cup S_2)\backslash(S_1 \cap S_2)$. For an azygetic system η and $S \subseteq T$, we define $\eta_S = \sum_{s\in S} \eta_s$. The following theorem, which we refer to as the Vanishing Criterion, gives a characterization of hyperelliptic period matrices in terms of their associated azygetic system and theta constants. For simplicity, we recall this theorem for genus 3 as stated in [1, Proposition 5] and refer the reader to [16, Chapter III.9] and [18, Theorem 2.6.1] for the general result in genus $g \geq 1$.

Theorem 2.4 (The Vanishing Criterion). *Let $Z \in \mathcal{H}_3$ and let η be an azygetic system. The following two statements are equivalent*:

(1) *Z is the period matrix of a symplectically irreducible abelian variety and there is exactly one of even theta characteristic δ such that $\vartheta[\delta](Z) = 0$ and that $\delta = \eta_{\mathcal{U}_\eta}$.*[1]

(2) *There is a marked hyperelliptic curve of genus 3 whose Jacobian has period matrix Z and η is the azygetic system associated to Z.*

In other words, Theorem 2.4 shows that given a hyperelliptic period matrix $Z \in \mathcal{H}_3$, choosing one of its azygetic systems η such that $\vartheta[\eta_{\mathcal{U}_\eta}] = 0$ fixes a labeling of the branch points. We recover the point in $\mathcal{M}_g^{\mathrm{hyp}}[2]$ using Takase's formulae [1; 24], which we recall in the following theorem.

Theorem 2.5 [1, Theorem 3]. *Let $Z \in \Gamma_6(2)\backslash\mathcal{H}_3$ a period matrix and η be the azygetic system such that the Vanishing Criterion is satisfied. Then with notation as above, for any disjoint decomposition $T - \{\infty\} = \mathcal{V} \sqcup \mathcal{W} \sqcup \{k, l, m\}$ with $\#\mathcal{V} = \#\mathcal{W} = 2$, we have*

$$\frac{\lambda_m - \lambda_l}{\lambda_m - \lambda_k} = \exp(4\pi i(\eta_k + \eta_l)_1(\eta_m)_2)\left(\frac{\vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{V}\cup\{m,l\})}] \cdot \vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{W}\cup\{m,l\})}]}{\vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{V}\cup\{k,m\})}] \cdot \vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{W}\cup\{k,m\})}]}(Z)\right)^2. \tag{2-10}$$

Note that in [1] the sign before the quotient of theta constants in equation (2-10) is incorrect. We give here the correct formula, as stated in several sources [2; 13].

Finally, note that by considering an affine map of $\mathbb{C}$, we may assume without restricting the generality that $\lambda_6 = 0$ and $\lambda_7 = 1$, i.e., X is given by

$$X : y^2 = x(x-1)\prod_{i=1}^{5}(x - \lambda_i). \tag{2-11}$$

In this case, we say that X is in *normalized Rosenhain form*. The moduli space $\mathcal{M}_3^{\mathrm{hyp}}[2]$ writes as

$$\mathcal{M}_3^{\mathrm{hyp}}[2] \cong \{\lambda = (\lambda_1, \ldots, \lambda_5), \lambda_i \in \mathbb{C} - \{0, 1\}, \lambda_i \neq \lambda_j\}.$$

The coefficients $\lambda_i \in \mathbb{C} - \{0, 1\}$, are called *the Rosenhain invariants* of the curve and will be the focus of our work.

2D. ***Shioda invariants.*** Shioda [20] gave a set of generators for the algebra of invariants of binary octavics over the complex numbers, which are now called *Shioda invariants*. Following Shioda's notation (see [20, page 1025]), these are 9 weighted projective invariants $(J_2, J_3, J_4, J_5, J_6, J_7, J_8, J_9, J_{10})$, where

[1] Poor defines symplectically irreducible on page 831 of [18]. His condition is equivalent to requiring that the abelian variety is not isomorphic as a polarized abelian variety to a product of lower-dimensional polarized abelian varieties. In this work, our period matrices are constructed to be simple, i.e., not isogenous to a product of lower-dimensional polarized abelian varieties. Since isomorphism is stronger than isogeny, all of the period matrices we construct are symplectically irreducible, and we may apply the theorem.

J_i has degree i. The invariants $J_2, \ldots, J_7$ are algebraically independent, while J_8, J_9, J_{10} depend algebraically on them. Note that over the complex numbers Shioda invariants completely determine points in $\mathcal{M}_3^{\mathrm{hyp}}$.

Using Igusa's map between the graded ring of Siegel modular forms of degree 3, and the graded ring of invariants of binary octavics, Lorenzo García [9] proposes a set of invariants which can be written as quotients of modular forms. These invariants involve large powers of the modular form χ_{28} in the denominators and we do not use them for experiments since they would need too much precision to compute.

Starting from the projective invariants J_i, we consider the following absolute Shioda invariants:[2]

$$\mathrm{Shi} = \left(\frac{J_2^7}{\Delta}, \frac{J_2^4 J_3^2}{\Delta}, \frac{J_2^5 J_4}{\Delta}, \frac{J_5 J_9}{\Delta}, \frac{J_2^4 J_6}{\Delta}, \frac{J_7^2}{\Delta}, \frac{J_2^3 J_8}{\Delta}, \frac{J_2^5 J_9^2}{\Delta^2}, \frac{J_2^2 J_{10}}{\Delta} \right), \tag{2-12}$$

with Δ the discriminant of the binary octavic, which is an invariant of degree 14. They are optimal for computations in the sense that they involve invariants of small weight and the values of their denominators for a given curve are products of powers of the primes of bad reduction of the curve; see [12]. Note that a subset of this set was already used by Weng [27] for computing models of hyperelliptic curves with CM by a field which contains i.

Proposition 2.1. *The invariants in equation (2-12) are modular, i.e., they can be written as quotients of Siegel modular forms of level* 1.

Idea of the proof. In [26], Tsuyumine proposed a set of invariants for the algebra of binary octavics and also computed them in terms of Siegel modular forms (see for instance [9, Theorem 3.4]). Using relations between Tsuyumine's invariants and the Shioda projective invariants (given in [9, Theorem 4.1]), we were able to write each invariant in equation (2-12) as a quotient of Siegel modular forms. The full computation is given in the arxiv version of this paper [7].

3. Computing abelian varieties with CM

In this section, we review results from the theory of complex multiplication, with the goal of describing our implementation of algorithms for computing several notions, such as the reflex field and the typenorm. Finally, we state the effective version of Shimura's second main theorem of CM.

3A. ***Reflex field computation.*** Let $K/\mathbb{Q}$ be a CM field and let L be the Galois closure of K with Galois group $\mathrm{Gal}(L/\mathbb{Q})$. A *CM type* of K is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of g embeddings $K \hookrightarrow \mathbb{C}$ such that no two embeddings appearing in Φ are complex conjugates. We say that Φ is *induced* from a CM subfield K' of K if the set $\{\phi|_{K'} \mid \phi \in \Phi\}$ is a CM type of K'. A CM type of K is called *primitive* if it is not induced by a proper CM subfield $K' \subset K$. In this paper, we fix the tuple (K, Φ) and call it a *CM-pair*. Since L

[2] An absolute invariant is a ratio of homogeneous invariants of the same degree.

is a CM field [14, Corollary 1.5], Φ extends to a CM type Φ_L of L, namely by

$$\Phi_L = \{\phi : L \to \mathbb{C} \mid \phi|_K \in \Phi\}. \tag{3-1}$$

We fix once and for all an embedding $\iota_K : K \to L$ and an embedding $\pi : L \to \mathbb{C}$. With these in hand, we associate to every element in $\phi \in \Phi_L$ an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that the following diagram commutes:

$$\begin{array}{ccc} L & \overset{\sigma}{\dashrightarrow} & L \\ {\scriptstyle \iota_K}\uparrow & & \downarrow{\scriptstyle \pi} \\ K & \xrightarrow{\phi|_K} & \mathbb{C} \end{array} \tag{3-2}$$

Note that this identification is certainly dependent on the embeddings ι_K and π. Let $\Phi_L^{-1} = \{\pi \circ \sigma^{-1} \in \mathrm{Hom}(L, \mathbb{C}) \mid \phi = \pi \circ \sigma \text{ for } \phi \in \Phi_L\}$. One can easily check that Φ_L^{-1} is a CM type on L if and only if Φ_L is a CM type on L. We denote by H^r the subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ of the form

$$H^r = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \sigma\Phi_L = \Phi_L\}. \tag{3-3}$$

Definition 3.1. The subfield of L fixed by the group H^r in equation (3-3) is called the *reflex field* of (K, Φ). We denote it by K^r.

Note that, from a computational point of view, choosing K^r as the field fixed by H^r also means fixing the embedding $\iota_{K^r} : K^r \to L$. As shown for instance in [14, Proposition 1.18], K^r is also a CM field and the associated CM type to K^r is given by the following construction:

$$\Phi^r = \Phi_L^{-1}|_{K^r} = \{\phi|_{K^r} \mid \phi \in \Phi_L^{-1}\}. \tag{3-4}$$

We call the tuple (K^r, Φ^r) the *reflex CM-pair* of (K, Φ). We implemented a procedure for computing the CM-pair (K^r, Φ^r) based on Definition 3.1 (see Algorithm 1 in [7] for full details). Our approach is similar to the implementation of the reflex field in the code of [23].

3B. ***The reflex typenorm.*** Let (K, Φ) be a primitive CM-pair with Galois closure L of K and reflex CM-pair (K^r, Φ^r). The *reflex typenorm* is the map

$$N_{\Phi^r} : K^r \to K \subset L, \quad x \mapsto \prod_{\phi \in \Phi^r} \phi(x). \tag{3-5}$$

We denote by $I(K)$ and $I(K^r)$ the set of nonzero fractional ideals of $\mathcal{O}_K$ and $\mathcal{O}_{K^r}$, respectively.

Lemma 3.1 [19, Chapter 2, Proposition 29]. *The reflex typenorm in equation (3-5) induces a map between ideals*

$$N_{\Phi^r} : I(K^r) \to I(K), \quad \mathfrak{a} \mapsto \prod_{\phi \in \Phi^r} \phi(\mathfrak{a}),$$

which extends to a homomorphism between class groups $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$.

When computing the typenorm of an ideal $\mathfrak{a} \in I(K^r)$, the product $\prod_{\phi\in\Phi^r} \phi(\mathfrak{a})$ gives a priori an ideal in L. To identify the ideal in K lying below this ideal, we first compute the factorization of this ideal and rely on an algorithm in [5, Algorithm 2.5.3] to get the prime ideal lying below each of the ideals appearing in this factorization. Algorithm 2 in [7] gives the pseudocode of our method. We remark that an alternative implementation for computing the typenorm, based on the proof of Lemma 3.1, is given in the code of [23].

3C. ***Class field theory.*** For a number field K and a finite modulus $\mathfrak{m}$ (i.e., a product of prime ideals in K), let $I_{\mathfrak{m}}(K)$ be the group of all fractional $\mathcal{O}_K$ ideals coprime to $\mathfrak{m}$, and consider the subgroup

$$P_{\mathfrak{m}}(K) = \{\mathfrak{a} \in I_{\mathfrak{m}}(K) : \mathfrak{a} = \alpha\mathcal{O}_F, \alpha \equiv 1 \pmod{^*\mathfrak{m}}\},$$

where the congruence $\alpha \equiv 1 \pmod{^*\mathfrak{m}}$ means that for all primes $\mathfrak{p}$ appearing in the factorization of $\mathfrak{m}$ we have $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m})$. The *ray class group* of K for the modulus $\mathfrak{m}$ is defined as the quotient group $\mathrm{Cl}_{\mathfrak{m}}(K) = I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K)$.

For a modulus $\mathfrak{m}$ in K we denote by $\mathcal{H}_{\mathfrak{m}}$ the unique (up to isomorphism) abelian extension of K whose ramified primes divide $\mathfrak{m}$ and such that the kernel of the *Artin map*

$$\Phi_{\mathfrak{m}} : I_{\mathfrak{m}}(K) \to \mathrm{Gal}(\mathcal{H}_{\mathfrak{m}}/K)$$

is equal to $P_{\mathfrak{m}}(K)$. The field $\mathcal{H}_{\mathfrak{m}}$ is called the *ray class field* of K of modulus $\mathfrak{m}$; see for instance [6, Theorem 8.6].

Let (K, Φ) be a primitive CM-pair with reflex pair (K^r, Φ^r). Let $m \in \mathbb{Z}$ such that $m\mathbb{Z} = \mathfrak{m} \cap \mathbb{Z}$ and denote by $I_m(K^r)$ the group of fractional ideals in K^r coprime to m. Following Shimura [19, Chapter 16], we consider

$$H_{\mathfrak{m}}(K^r) = \{\mathfrak{a} \in I_m(K^r) : \exists \alpha \in K^* \text{ with } N_{\Phi^r}(\mathfrak{a}) = \alpha\mathcal{O}_K,\ N_{K^r/\mathbb{Q}}(\mathfrak{a}) = \alpha\bar{\alpha},\ \alpha \equiv 1 \pmod{^*\mathfrak{m}}\}. \quad (3\text{-}6)$$

Note that $P_m(K^r) \subset H_{\mathfrak{m}}(K^r)$. Then, after [6, Theorem 8.6], up to isomorphism there is a unique Abelian extension of K^r, denoted by $CM_{\mathfrak{m}}(K^r)$, such that

$$\mathrm{Gal}(CM_{\mathfrak{m}}(K^r)/K^r) \cong I_m(K^r)/H_{\mathfrak{m}}(K^r). \quad (3\text{-}7)$$

The effective construction of $CM_{\mathfrak{m}}(K)$ relies on Shimura's Main Theorem 2, that we state in Section 3D. In order to compute Galois conjugates of elements in this number field in Section 4, we will need to compute the group $I_m(K^r)/H_{\mathfrak{m}}(K^r)$. In order to do this, we will need the following group introduced by Shimura:

$$\mathfrak{C}_{\mathfrak{m}}(K) = \{(\mathfrak{a}, \alpha) : \mathfrak{a} \in I_{\mathfrak{m}}(K) \text{ such that } \mathfrak{a}\bar{\mathfrak{a}} = (\alpha),\ \alpha \in K_0 \text{ totally positive},\ \alpha \equiv 1 \pmod{^*\mathfrak{m}}\}/\simeq, \quad (3\text{-}8)$$

where $(\mathfrak{a}, \alpha) \simeq (\mathfrak{a}', \alpha')$ if and only if there exists $\mu \in K^*$ such that $\mathfrak{a} = \mu\mathfrak{a}'$ and $\alpha = \alpha'\mu\bar{\mu}$ and $\mu \equiv 1 \pmod{^*\mathfrak{m}}$. Given a pair $(\mathfrak{a}, \alpha)$ satisfying the conditions in equation (3-8), we denote by $(\mathfrak{a}, \alpha)_{\mathfrak{m}}$ the corresponding equivalence class.

Lemma 3.2. *We denote by* $T : \mathrm{Cl}_m(K^r) \to \mathfrak{C}_{\mathfrak{m}}(K)$ *the map given by* $\mathfrak{a} \to (N_{\Phi^r}(\mathfrak{a}), N_{K^r/\mathbb{Q}}(\mathfrak{a}))_{\mathfrak{m}}$. *Then*:

(a) *The kernel of this map is* $\ker T = H_{\mathfrak{m}}(K^r)/P_m(K^r)$.

(b) *The image of the map* T *is isomorphic to* $I_m(K^r)/H_{\mathfrak{m}}(K^r)$.

Proof. (a) Let $\mathfrak{a} \in \ker T$, i.e., $(N_{\Phi^r}(\mathfrak{a}), N_{K^r/\mathbb{Q}}(\mathfrak{a}))_{\mathfrak{m}} = (\mathcal{O}_K, 1)_{\mathfrak{m}}$. Then there exists an element $\mu \in K^*$ such that $N_{\Phi^r}(\mathfrak{a}) = \mu\mathcal{O}_K$ and $N_{K^r/\mathbb{Q}}(\mathfrak{a}) = \mu\overline{\mu}$ and $\mu \equiv 1 \pmod{{}^*\mathfrak{m}}$. Conversely, by the definition of $H_{\mathfrak{m}}(K^r)$, any element in $H_{\mathfrak{m}}(K^r)/P_m(K^r)$ is in $\ker T$.

(b) It follows immediately from point (a) that

$$T(\mathrm{Cl}_m(K^r)) \cong \mathrm{Cl}_m(K^r)/\ker T \cong (I_m(K^r)/P_m(K^r))/(H_{\mathfrak{m}}(K^r)/P_m(K^r)) \cong I_m(K^r)/H_{\mathfrak{m}}(K^r). \quad \square$$

In our implementation we computed a set of generators for $\mathrm{Cl}_m(K^r)$ using Magma, and then implemented an algorithm for enumerating the elements in the set $T(\mathrm{Cl}_m(K^r))$. Due to Lemma 3.2, this allowed us to compute the group $I_m(K^r)/H_{\mathfrak{m}}(K^r)$ and enumerate Galois conjugates of a CM point (see Definition 4.1).

3D. ***CM abelian varieties.*** Before stating Shimura's second main theorem, we briefly set the notation and recall the terminology. Let A an abelian variety of dimension g defined over a field k. We say that A has *complex multiplication* (CM) by a number field K if there exists an embedding $\iota : K \to \mathrm{End}(A) \otimes \mathbb{Q}$. If $\mathcal{O}_K$ is the maximal order of K, then we say that A has CM by $\mathcal{O}_K$ if $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}_K$. Let $\mathfrak{D}_{K/\mathbb{Q}}$ be the different of K, and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Suppose that the ideal $(\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$ is principal and generated by $\xi \in K^\times$ such that $\mathrm{Im}(\phi(\xi)) > 0$ for all $\phi \in \Phi$. Then by tensoring the map

$$\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a}) \to \mathbb{Q}, \quad (\Phi(x), \Phi(y)) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\xi\bar{x}y)$$

with $\mathbb{R}$ we obtain a Riemann form $E_{\Phi,\xi} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$. Hence for any triple $(\Phi, \mathfrak{a}, \xi)$ as above, the pair $(\mathbb{C}^g/\Phi(\mathfrak{a}), E_{\Phi,\xi})$ is a p.p.a.v. of dimension g with CM by $\mathcal{O}_K$ and of CM type Φ. Conversely, every p.p.a.v. of dimension g with CM by $\mathcal{O}_K$ is isomorphic to a complex torus for some triple $(\Phi, \mathfrak{a}, \xi)$ as above. Note that to go from the triple $(\Phi, \mathfrak{a}, \xi)$ to a period matrix as described in Section 2A, it suffices to write a basis for the ideal $\mathfrak{a}$ that is symplectic with respect to the Riemann form $E_{\Phi,\xi}$. This basis gives the matrix Ω, and then the period matrix is simply $Z = \Omega_2^{-1}\Omega_1$.

Let (A, E) be a p.p.a.v. with CM by $\mathcal{O}_K$, G the automorphism group of A and let k_0 be its field of moduli. To state Shimura's second main theorem of CM, we consider the *normalized Kummer variety* [19, Theorem 3, Section 4.4] of A. This is given by a tuple (W, h), where W is the quotient of A by G, which is defined over k_0, and $h : A \to W$ is the corresponding surjective map. Moreover, given a modulus $\mathfrak{m}$, we denote by $A[\mathfrak{m}]$ the $\mathfrak{m}$-torsion points of A, i.e., $A[\mathfrak{m}] = \{x \in A | \iota(\alpha)x = 0, \forall \alpha \in \mathfrak{m}\}$. A point $t \in A[\mathfrak{m}]$ is called proper if for all $a \in \mathcal{O}_K$, we have that $\iota(a)t = 0$ if and only if $a \in \mathfrak{m}$.

Theorem 3.2 [19, Main Theorem 2]. *Let* (A, E) *be a principally polarized abelian variety with CM by* $\mathcal{O}_K$ *and CM type* Φ *and let be* (W, h) *its normalized Kummer variety. Let* $\mathfrak{m}$ *be an ideal of* $\mathcal{O}_K$ *and* t *be*

a proper $\mathfrak{m}$*-torsion point. Let* k_0 *be the field of moduli of* A, K^r *the reflex field of* K *and* $k_0^* = k_0K^r$. *Then* $k_0^*(h(t))$ *is the class field of* K^r *corresponding to the ideal group* $H_{\mathfrak{m}}(K^r)$.

4. Computing class polynomials

We turn our attention now to the computation of the Shioda and Rosenhain invariants of a hyperelliptic curve of genus 3 with CM by $\mathcal{O}_K$, and more precisely to obtaining their minimal polynomials over the reflex field.

Given a primitive CM-pair (K, Φ), we denote by $\mathrm{Princ}(K, \Phi, \mathfrak{m})$ the set of isomorphism classes of simple p.p.a.v. with CM by $\mathcal{O}_K$ together with a proper $\mathfrak{m}$-torsion point. We denote by $A(\Phi, \mathfrak{a}, \xi, t)$ the abelian variety given by the triple $(\Phi, \mathfrak{a}, \xi)$ and the proper $\mathfrak{m}$-torsion point t. When $\mathfrak{m} = (1)$, we simply denote it by $A(\Phi, \mathfrak{a}, \xi)$ and we take $\mathrm{Princ}(K, \Phi)$ to be the set of all such abelian varieties. In our computations of Galois conjugates, we will extensively use the following action of the class group $I_m(K^r)/H_{\mathfrak{m}}(K^r)$ on $\mathrm{Princ}(K, \Phi, \mathfrak{m})$ given by Shimura [19, Section 16.3].

Definition 4.1. Let $A = A(\Phi, \mathfrak{a}, \xi, t) \in \mathrm{Princ}(K, \Phi, \mathfrak{m})$. Then for any $[\mathfrak{c}] \in I_m(K^r)/H_{\mathfrak{m}}(K^r)$ the action of $[\mathfrak{c}]$ on A is given by the abelian variety

$$A(\Phi, N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi, t \pmod{N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}}).$$

We will denote by $A^{\mathfrak{c}}$ the p.p.a.v. obtained in this way.

Note that the action in Definition 4.1 yields in fact an isogeny between principally polarized abelian varieties $I_{\mathfrak{c}} : A \to A^{\mathfrak{c}}$. Since the ideal $\mathfrak{c}$ is coprime to m, we have that $\ker I_{\mathfrak{c}} \cap A[\mathfrak{m}] = 0$. In particular, when $\mathfrak{m} = (m)$ and we fix a level m structure on A, this isogeny fixes the level m structure on $A^{\mathfrak{c}}$.

Notation 4.2. In the remainder of this paper, we will restrict to $\mathfrak{m} = (m)$, where $m = 1$ or $m = 2$. For a given $\mathfrak{c} \in I_m(K^r)/H_{\mathfrak{m}}(K^r)$, we will denote by $\sigma_{\mathfrak{c}} \in \mathrm{Gal}(CM_{\mathfrak{m}}(K^r)/K^r)$ the image of $\mathfrak{c}$ via the isomorphism in equation (3-7). Let $A = A(\Phi, \mathfrak{a}, \xi, t)$ be a p.p.a.v. in $\mathrm{Princ}(K, \Phi, \mathfrak{m})$. Let $B = (B_1|B_2)$ be a (3×6) complex-valued matrix containing a symplectic basis for $\Phi(\mathfrak{a})$ with respect to $E_{\Phi,\xi}$, and let $Z = B_2^{-1}B_1 \in \mathcal{H}_3$ be the corresponding period matrix. The action of $\mathfrak{c}$ on A yields a new p.p.a.v. $A(\Phi, N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi, t \pmod{N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}})$. In a similar manner, let $C = (C_1|C_2)$ be the matrix containing a symplectic basis for $\Phi(N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a})$ with respect to $E_{\Phi, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi}$ and let $Z' = C_2^{-1}C_1 \in \mathcal{H}_3$. We express C in terms of B by taking a matrix M, such that $C = BM^T$. The matrix M is in $\mathrm{GSp}_{2g}(\mathbb{Q})$ and is m-integral and invertible $\pmod m$ with inverse $U \in \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$. We also denote by $\tilde{U} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ a lift of U. Such a lift can be computed for instance thanks to [17, Theorem VII.21].

This notation will be used all throughout this section. We detail the computation of these matrices on an example.

Example 4.3. Let K be the CM field defined by the polynomial $x^6 + 43x^4 + 451x^2 + 729$ and denote by a a generator for this field. We choose the first CM type given by the implementation [2] and we get that the tuple $(\mathfrak{a}, \xi) = \left(\mathcal{O}_K, \frac{16}{114939}a^5 + \frac{1313}{229878}a^3 + \frac{5857}{114939}a\right)$ yields a CM point. We compute the action

on this CM point by the ideal $\mathfrak{c} = \left(9, \frac{1}{48}a^5 + \frac{11}{24}a^3 + \frac{1}{2}a^2 - \frac{155}{48}a + \frac{15}{2}\right)$ and get a second CM point given by

$$(\mathfrak{b}, \xi') = \left(\left(9, \tfrac{1}{48}a^5 + \tfrac{11}{24}a^3 + \tfrac{1}{2}a^2 - \tfrac{155}{48}a + \tfrac{15}{2}\right), \tfrac{16}{114939}a^5 + \tfrac{1313}{229878}a^3 + \tfrac{5857}{114939}a\right).$$

The code in [2] gives symplectic bases for $(\mathfrak{a}, \xi)$ and $(\mathfrak{b}, \xi')$ and we compute

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

The following result gives an explicit version of Shimura's reciprocity law.

Theorem 4.4 [23, Theorem 2.4]. *Let $\mathfrak{c} \in I_m(K^r)/H_{\mathfrak{m}}(K^r)$, $\sigma_{\mathfrak{c}} \in \mathrm{Gal}(CM_{\mathfrak{m}}(K^r)/K^r)$, $Z, Z' \in \mathcal{H}_3$ and the matrix M as in Notation 4.2. For every Siegel modular function f of level m with Fourier expansion coefficients in $\mathbb{Q}(\xi_m)$, we have*

$$f(Z)^{\sigma_{\mathfrak{c}}} = f^U(Z'), \tag{4-1}$$

where we denote by $f^U(Z') = f(\tilde{U}.Z')$, for any $\tilde{U} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ a lift of U.

We will use Theorem 4.4 to compute the Galois conjugates of the Shioda invariants of a hyperelliptic curve whose period matrix is obtained via the complex multiplication construction.

Proposition 4.1. *Let $A \in \mathrm{Princ}(K, \Phi)$ and $Z \in \mathcal{H}_3$ a period matrix for it. Let $[\mathfrak{c}] \in \mathrm{Cl}(K^r)$ corresponding to $\sigma_{\mathfrak{c}} \in \mathrm{Gal}(CM_1(K^r)/K^r)$ and Z' obtained as in Notation 4.2. Then $A^{\mathfrak{c}}$ is isomorphic to a hyperelliptic Jacobian if and only if A is. Moreover, we have the following relation:*

$$S_j(Z)^{\sigma_{\mathfrak{c}}} = S_j(Z'), \tag{4-2}$$

where S_j denotes the Siegel modular function giving the j-th Shioda absolute invariant, for all $j = 1, \ldots, 9$.

Proof. Suppose that $A \cong \mathrm{Jac}(X)$, with X a hyperelliptic curve. Since $\mathrm{Jac}(X)^{\sigma_{\mathfrak{c}}} \cong \mathrm{Jac}(X^{\sigma_{\mathfrak{c}}})$, it follows that $A^{\mathfrak{c}}$ is isomorphic to the Jacobian of the hyperelliptic curve $X^{\sigma_{\mathfrak{c}}}$. To prove equation (4-2), we apply Theorem 4.4 on the Siegel modular functions S_i. □

We now restrict to the case of the modulus $\mathfrak{m} = (2)$. The following result allows us to compute the Galois conjugates of the Rosenhain invariants.

Theorem 4.5. *Let $A \in \mathrm{Princ}(K, \Phi)$ which is isomorphic to the Jacobian of a marked genus 3 hyperelliptic curve and $Z \in \Gamma_6(2)\backslash\mathcal{H}_3$ a period matrix for it. Let $[\mathfrak{c}] \in I_2(K^r)/P_2(K^r)$ corresponding to $\sigma_{\mathfrak{c}} \in \mathrm{Gal}(CM_2(K^r)/K^r)$ and Z' obtained as in Notation 4.2. We consider η the azygetic system*

associated to Z and let $(\lambda_l)_{1\le l\le 5}$ be the Rosenhain invariants in equation (2-11). Then for any lift $\tilde{U} = \left(\begin{smallmatrix}\tilde{A} & \tilde{B}\\ \tilde{C} & \tilde{D}\end{smallmatrix}\right) \in \mathrm{Sp}_6(\mathbb{Z})$ of the matrix U with $\delta_0 = \left(\begin{smallmatrix}(\tilde{C}^T\tilde{D})_0\\ (\tilde{A}^T\tilde{B})_0\end{smallmatrix}\right)$, we have that

$$\lambda_l^{\sigma_\mathfrak{c}} = \exp(4\pi i(\eta_l+\eta_7)_1(\eta_6)_2)\cdot\zeta_4(\tilde{U},\eta)\cdot\lambda_l', \tag{4-3}$$

where

$$\zeta_4(\tilde{U},\eta) = \exp\Big(2\Big(k\big(\tilde{U},\tilde{U}^T\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,l\})}-\tfrac{1}{2}\delta_0\big)\big)+k\big(\tilde{U},\tilde{U}^T\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,l\})}-\tfrac{1}{2}\delta_0\big)\big)$$
$$-k\big(\tilde{U},\tilde{U}^T\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,7\})}-\tfrac{1}{2}\delta_0\big)\big)-k\big(\tilde{U},\tilde{U}^T\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,7\})}-\tfrac{1}{2}\delta_0\big)\big)\Big)\Big),$$

and

$$\lambda_l' = \left(\frac{\vartheta\big[\tilde{U}^t\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,l\})}-\frac{1}{2}\delta_0\big)\big]\cdot\vartheta\big[\tilde{U}^t\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,l\})}-\frac{1}{2}\delta_0\big)\big]}{\vartheta\big[\tilde{U}^t\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,7\})}-\frac{1}{2}\delta_0\big)\big]\cdot\vartheta\big[\tilde{U}^t\big(\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,7\})}-\frac{1}{2}\delta_0\big)\big]}\right)^2(Z').$$

Proof. Using Theorem 2.5 when $\lambda_6=0$ and $\lambda_7=1$, the coefficients λ_l with $l=1,\dots 5$ can be computed as

$$\lambda_l = \exp(4\pi i(\eta_l+\eta_7)_1(\eta_6)_2)\left(\frac{\vartheta[\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,l\})]\cdot\vartheta[\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,l\})]}{\vartheta[\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,7\})]\cdot\vartheta[\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,7\})]}\right)^2(Z).$$

For the sake of simplicity let

$$c_1=\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,l\})},\quad c_2=\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,l\})},\quad c_3=\eta_{\mathcal{U}_\eta\circ(\mathcal{V}\cup\{6,7\})}\quad\text{and}\quad c_4=\eta_{\mathcal{U}_\eta\circ(\mathcal{W}\cup\{6,7\})}.$$

By using Theorem 4.4, we have that

$$\begin{aligned}\lambda_l^{\sigma_\mathfrak{c}} &= \left(\exp(4\pi i(\eta_l+\eta_7)_1(\eta_6)_2)\left(\frac{\vartheta[c_1]\cdot\vartheta[c_2]}{\vartheta[c_3]\cdot\vartheta[c_4]}\right)^2(Z)\right)^{\sigma_\mathfrak{c}}\\ &= \exp(4\pi i(\eta_l+\eta_7)_1(\eta_6)_2)\left(\left(\frac{\vartheta[c_1]\cdot\vartheta[c_2]}{\vartheta[c_3]\cdot\vartheta[c_4]}\right)^2\right)^U(Z').\end{aligned} \tag{4-4}$$

We denote by $c_j' = \tilde{U}^T\big(c_j-\frac{1}{2}\delta_0\big)$. By applying the theta transformation formula, we get that

$$\vartheta[c_j]^U(Z') = \vartheta[\tilde{U}.c_j'](\tilde{U}.Z') = \zeta(\tilde{U})\exp\left(k(\tilde{U},c_j')\right)\sqrt{\det(\tilde{C}Z'+\tilde{D})}\vartheta[c_j'](Z').$$

Hence equation (4-4) becomes

$$\lambda_l^{\sigma_\mathfrak{c}} = \exp(4\pi i(\eta_l+\eta_7)_1(\eta_6)_2)\exp(2(k(\tilde{U},c_1')+k(\tilde{U},c_2')-k(\tilde{U},c_3')-k(\tilde{U},c_4')))\left(\frac{\vartheta[c_1']\cdot\vartheta[c_2']}{\vartheta[c_3']\cdot\vartheta[c_4']}\right)^2(Z')$$

where one can easily see that $\zeta_4(\tilde{U},\eta)=\exp(2(k(\tilde{U},c_1')+k(\tilde{U},c_2')-k(\tilde{U},c_3')-k(\tilde{U},c_4')))^2$ is a fourth root of unity. □

We will now give a geometric interpretation to our results. Recall that the Rosenhain coefficients are invariants for the space $\mathcal{M}_3^{\mathrm{hyp}}[2]$. The Galois conjugates of the Rosenhain invariants are the Rosenhain invariants of another point in this moduli space and the following result gives a method to compute the corresponding $Z'\in\Gamma_6(2)\backslash\mathcal{H}_3$ and the associated azygetic system.

Corollary 4.1. *Assume that $A(\Phi, \mathfrak{a}, \xi)$ is isomorphic to the Jacobian of a marked hyperelliptic curve X and let $Z \in \Gamma_6(2)\backslash\mathcal{H}_3$ be the corresponding period matrix for A and η be an azygetic system associated to Z. Given $[\mathfrak{c}] \in I_2(K^r)/H_2(K^r)$, there exist Z', M and $\tilde{U}$ as in Notation 4.2 such that $\eta' = \tilde{U}^T\eta$ is an azygetic system associated to the period matrix Z' of the marked hyperelliptic curve with Rosenhain invariants $(\lambda_l^{\sigma_\mathfrak{c}})_{l=1,\dots,5}$.*

Proof. We first note that we can choose C and the period matrix Z' in Notation 4.2 such that $\tilde{U} \in \Gamma_6(2)$. Indeed, if this is not the case, we define $C' = BM^T\tilde{U}^T = BM'^T$ with $M' = \tilde{U}M \in \mathrm{GSp}_6(\mathbb{Q})$. Then C' is still a symplectic basis for of $\Phi(N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a})$ with respect to $E_{\Phi, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi}$. Let $\overline{M} \in \mathrm{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ the reduction of $M \pmod 2$. We get that $\overline{M'} = \overline{\tilde{U}}\,\overline{M} = U\overline{M} = I_6$. Then $(\overline{M'})^{-1} = I_6$ in $\mathrm{Sp}_6(\mathbb{Z}/2\mathbb{Z})$. Therefore, by letting $C = C'$ and Z' the period matrix obtained from this new symplectic basis, we ensure that $\tilde{U} \in \Gamma_6(2)$.

Recall that the action described in Definition 4.1 yields an isogeny between A and $A^\mathfrak{c}$ which is given by

$$I_\mathfrak{c} : \mathbb{C}^3/\Phi(\mathfrak{a}) \to \mathbb{C}^3/\Phi(N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}), \quad x \mapsto x.$$

For simplicity, we will work with $I_\mathfrak{c}$ as an isogeny between the nonnormalized tori, i.e., $I_\mathfrak{c}$:$\mathbb{C}^3/(B_1\mathbb{Z}^3+B_2\mathbb{Z}^3) \to \mathbb{C}^3/(C_1\mathbb{Z}^3+C_2\mathbb{Z}^3)$. We consider the image of the fixed points $B_1(\eta_i)_1+B_2(\eta_i)_2 \pmod{(B_1\mathbb{Z}^3+B_2\mathbb{Z}^3)}$ via $I_\mathfrak{c}$. We compute η_i' such that

$$B_1(\eta_i)_1 + B_2(\eta_i)_2 = C_1(\eta_i')_1 + C_2(\eta_i')_2 \pmod{(C_1\mathbb{Z}^3 + C_2\mathbb{Z}^3)}. \tag{4-5}$$

By writing $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and using that $C = BM^T$, the 2-torsion point in equation (4-5) writes as

$$(B_1a^t + B_2b^t)(\eta_i')_1 + (B_1c^t + B_2d^t)(\eta_i')_2 \pmod{(C_1\mathbb{Z}^3 + C_2\mathbb{Z}^3)} = \\ B_1(a^t(\eta_i')_1 + c^t(\eta_i')_2) + B_2(b^t(\eta_i')_1 + d^t(\eta_i')_2) \pmod{(C_1\mathbb{Z}^3 + C_2\mathbb{Z}^3)}.$$

Hence $\bar{\eta}_i = \overline{M}^T\bar{\eta}_i'$. Then it is easy to check that $\eta_i' = \tilde{U}^T\eta_i$ is in fact an azygetic system associated to Z'. The first three facts in Definition 2.3 are trivial to check, the fourth equality follows by applying [15, Proposition 13.2(b)] for the isogeny $I_\mathfrak{c}$, which has degree prime to 2.

To show that η' is associated to Z', we will use the Vanishing Criterion. We choose an even theta characteristic $u \in \frac{1}{2}\mathbb{Z}^6$ such that $\vartheta[u](Z) \neq 0$ and $\vartheta[u](Z') \neq 0$ and apply once more Shimura's reciprocity law [23] on the quotients of the type $\left(\frac{\vartheta[v](Z)}{\vartheta[u](Z)}\right)^2$, with $v \in \frac{1}{2}\mathbb{Z}^6$ even. We deduce that the unique even theta constant vanishing Z' is $\vartheta[\eta_{\mathcal{U}_{\eta'}}]$ (since $\eta_{\mathcal{U}_{\eta'}} = \eta_{\mathcal{U}_\eta}$).

Finally, by applying Theorem 4.5 we get that

$$\lambda_l^{\sigma_\mathfrak{c}} = \exp(4\pi i(\eta_l + \eta_7)_1(\eta_6)_2)\left(\frac{\vartheta[c_1]\cdot\vartheta[c_2]}{\vartheta[c_3]\cdot\vartheta[c_4]}\right)^2(M'.Z), \tag{4-6}$$

for $l = 1, \dots, 5$. Hence the right-hand side expressions in equation (4-6) are the Rosenhain invariants of a marked genus 3 hyperelliptic curve. □

Computing the Shioda and Rosenhain class polynomials. From a computational point view, if we simply aim at computing the Galois conjugates of the Rosenhain invariants and deriving class field equations, one can choose between the approach in Theorem 4.5 or the one in Corollary 4.1. One can pick any period matrix for $A^{\mathfrak{c}}$ and use the formula in Theorem 4.5, or construct the period matrix Z' and its associated azygetic system as explained in the proof of the Corollary 4.1 and compute the resulting Rosenhain invariants via Takase's formula.

Algorithm 1 in the Appendix gives all the steps of our computation of a list of approximations for the Galois conjugates of the Rosenhain invariants, that we use to get the polynomials $H^R_{K^r,i}$ in equation (1-1). The algorithm for computing $H^S_{K^r,j}$ is similar and relies on the computation of the Siegel modular functions S_j in Equation (4-2). Note that in applications, for $i, j \geq 2$, it is easier to use the Hecke representation as introduced by Gaudry et al [10]:

$$\hat{H}^R_{K^r,i}(t) = \sum_{\sigma} \lambda_i^{\sigma} \prod_{\sigma' \neq \sigma} (t - \lambda_1^{\sigma'}), \quad \hat{H}^S_{K^r,j}(t) = \sum_{\sigma} \mathrm{Shi}_j^{\sigma} \prod_{\sigma' \neq \sigma} (t - \mathrm{Shi}_1^{\sigma'}),$$

where $\sigma, \sigma' \in \mathrm{Gal}(CM_{\mathfrak{m}}(K^r)/K^r)$ with $\mathfrak{m} = (2)$ for the product in $H^R_{K^r,i}$ and $\mathfrak{m} = (1)$ for the product and sum in $H^S_{K^r,j}$.

5. Benchmarks and results

We implemented the algorithms described here using SageMath [25] and Magma [4] by building on an existing implementation [2]. The computation of primitive CM types for genus 3 in [2] is dependent on the group structure of $\mathrm{Gal}(L/\mathbb{Q})$. Our CM type computation is independent of this group isomorphism, and works for all genera. In this general setting, we also implemented the construction of the reflex field of K and of the typenorm, as explained in Section 3. Since SageMath [25] does not implement ray class groups, we used an interface to Magma [4] to compute the group $\mathrm{Cl}_m(K^r)$ and enumerate elements in $T(\mathrm{Cl}_m(K^r))$.

5A. ***Practical experiments.*** For space reasons, we reproduce here partially an example and give the full computation in [7]. Let K be the CM field defined by the polynomial $x^6 + 43x^4 + 451x^2 + 729$. Since the field contains i, all p.p.a.v. with CM by K are hyperelliptic. For one of its primitive CM types, our implementation yields the reflex field as the field of equation $x^6 + 1012x^4 + 262048x^2 + 3968064$. The subgroup $T(\mathrm{Cl}_m(K^r))$, for $\mathfrak{m} = (1), (2)$, has three elements, which means that the polynomials $H^R_{K^r,i}$ and $H^S_{K^r,j}$ have degree 3.

For most computations on the Rosenhains 500 bits of precision were enough, whereas for the Shiodas we used 5000 bits of precision. Indeed, the Siegel modular forms appearing in the expressions of the Shiodas have much larger weight, which results into much more precision needed when computing with the Shiodas. To compute the Shiodas, we first computed the Rosenhain coefficients and got an approximation of the equation of the curve, and afterwards computed the Shiodas from this equation. All computations were performed on a single core of a Intel Core i7-4790 CPU 3.60GHz and took

polynomial	t^3	t^2	t	1
$H_{K^r,1}$	1	$\frac{1}{16}\alpha^2 - \frac{19}{8}\alpha + \frac{181}{16}$	$\frac{1}{48}\alpha^2 - \frac{49}{24}\alpha + \frac{875}{16}$	$\frac{1}{6}\alpha^2 - \frac{16}{3}\alpha + \frac{19}{2}$
$\hat{H}_{K^r,2}$	1	$-\frac{7}{144}\alpha^2 + \frac{149}{72}\alpha - \frac{3331}{144}$	$\frac{3}{16}\alpha^2 - \frac{65}{8}\alpha + \frac{1295}{16}$	$-\frac{11}{4}8\alpha^2 + \frac{239}{24}\alpha - \frac{1521}{16}$
$\hat{H}_{K^r,3}$	1	$-\frac{1}{16}\alpha^2 + \frac{19}{8}\alpha - \frac{277}{16}$	$\frac{13}{48}\alpha^2 - \frac{277}{24}\alpha + \frac{1791}{16}$	$-\frac{11}{24}\alpha^2 + \frac{227}{12}\alpha - \frac{1377}{8}$
$\hat{H}_{K^r,4}$	1	$\frac{7}{144}\alpha^2 - \frac{149}{72}\alpha + \frac{2467}{144}$	$-\frac{1}{144}\alpha^2 + \frac{11}{72}\alpha + \frac{59}{144}$	$\frac{7}{144}\alpha^2 - \frac{143}{72}\alpha + \frac{2551}{144}$
$\hat{H}_{K^r,5}$	1	-6	12	-8

Table 1. Coefficients of polynomials $H^R_{K^r,i}$ for the field of equation $x^6 + 43x^4 + 451x^2 + 729$.

approximately 5 minutes at 500 bits of precision and less than 2 hours for 5000 bits. Most time is spent on the theta constants computation, which is performed using the naive implementation in [2]. To compute the coefficients of the class polynomials $H^R_{K^r,i}$ and $H^S_{K^r,i}$ as algebraic integers, we use the algebraic dependence testing algorithm [5], implemented in PARI/GP by the function *algdep*. This algorithm gives us a conjectured minimal polynomial for each coefficient of the class polynomials.

Since $\mathrm{Princ}(K, \Phi)$ is stable under complex conjugation, it can be shown by using similar arguments as in [21, Section III.2] that the coefficients of the Shioda class polynomials are in fact in the field K_0^r, the real multiplication subfield of K^r. We conjecture that a similar result holds for the Rosenhain class polynomials. For the chosen example, K and K^r are equal, so we take K_0^r to be the field given by the equation

$$x^3 - 43x^2 + 451x^2 - 729$$

and we denote by α a generator for this field. Tables 1 and 2 give the coefficients of Rosenhain and Shioda class polynomials, respectively. Table 2 gives the Shioda class polynomials for the first Shioda invariant, and the full example is given in [7]. As expected, the polynomials for the Shiodas have larger coefficients, which is due again to the shape of the modular forms in their expression.

In order to heuristically check the correctness of these computations, we use a well known approach in the literature which consists in choosing a prime number p such that the abelian varieties with CM by $\mathcal{O}_K$ have good reduction, compute the roots of class polynomials $\pmod p$ and check that the Jacobians of the curves obtained in this way have the right number of points; see for instance [1] for details.

	coefficients
t^3	1
t^2	$\frac{-150499810389818442869289571906287699141437 5}{110603005123701223605415218816743955330378310 3}\alpha^2 + \frac{576021917913534128335758291802230916493406 30}{110603005123701223605415218816743955330378310 3}\alpha - \frac{182610135152410817952949427128063513960980968701}{247750731477090740876130090149506459940047415072}$
t	$\frac{271537582048409045934259507591982005281201875}{867127560169817593066455315523272609790165952752}\alpha^2 - \frac{171559472382027900944379509650789590018494955535}{130069134025472638959968297328490891468524892912 8}\alpha + \frac{189221715181445169536136728129202262948355511744769}{116541944086823484508131594406327838755798304049868 8}$
1	$\frac{-4970183343949242284467452261947818401413441768 75}{244738082582329317467076348253288461387176438504724 48}\alpha^2 + \frac{114442556401918903153013990970527856060706070221 15}{122369041291164658735358174126644230693588821925236224}\alpha - \frac{191953650625925394207069308222518633622840220848155861}{164463991495325301337875306062609846052182566675174850 56}$

Table 2. Coefficients of the polynomial $H^S_{K^r,1}$ for the field of equation $x^6 + 43x^4 + 451x^2 + 729$.

Appendix

Algorithm 1: Computing the Galois action using Shimura's reciprocity law

Input: A CM-pair (K, Φ), where K is a sextic CM field and Φ is a CM type, and precision prec.

Output: Lists containing the Galois conjugates of the Rosenhain invariants of hyperelliptic curves with CM by (K, Φ), if such curves exist.

Let $\mathcal{R}_l$, $1 \leq l \leq 5$ be an empty list.
Compute the Galois closure L of $K/\mathbb{Q}$.
Compute the reflex CM-pair (K^r, Φ^r) and the fixed embedding $\iota_{K^r} : K^r \to L$.
Determine the ray class group $\mathrm{Cl}_m(K^r)$ for the modulus $\mathfrak{m} = (2)$.
Compute and store elements of $T(\mathrm{Cl}_m(K^r))$ in a list $\mathfrak{H}(K^r, \Phi^r)$.
Choose a p.p.a.v. A with CM by $\mathcal{O}_K$ given by the triple $(\Phi, \mathfrak{a}, \xi)$ and construct period matrix Z with [1, Algorithm 2].
if exactly one of the theta constants $\vartheta[c](Z)$, with c even, is zero **then**
    Compute the Rosenhain invariants λ_l with precision prec using Takase's formula (2-10).
    for all $(N_{\Phi^r}(\mathfrak{c}), N_{K^r/\mathbb{Q}}(\mathfrak{c})) \in \mathfrak{H}(K^r, \Phi^r)$ **do**
        Compute the p.p.a.v. $A(\Phi, N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi)$ and the corresponding Z'.
        Compute $\lambda_l^{\sigma_\mathfrak{c}}$ using the formula in Theorem 4.5 and add it to the list $\mathcal{R}_l$.
return $\mathcal{R}_l$, $1 \leq l \leq 5$.

Acknowledgements

The first author is grateful to Jeroen Sijsling for many helpful discussions. The second author thanks Christelle Vincent for preliminary discussions which led to this research. We thank Andreas Enge for his remarks on an early version of this manuscript and the ANTS conference reviewers for their numerous comments. The authors acknowledge financial support from the FACE foundation.

References

[1] J.S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent, *Constructing genus-3 hyperelliptic Jacobians with CM*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 283–300.

[2] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent, *Genus 3*, https://github.com/christellevincent/genus3, 2016.

[3] C. Birkenhake and H. Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

[5] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 1991.

[6] D. A. Cox, *Primes of the form $x^2 + ny^2$*, vol. 2, Wiley, 2012.

[7] B. Dina and S. Ionica, *Genus 3 hyperelliptic curves with CM via Shimura reciprocity*, preprint, 2020. arXiv 2003.06386

[8] A. Enge and E. Thomé, *Computing class polynomials for abelian surfaces*, Experimental Mathematics **23** (2014), no. 2, 129–145.

[9] E. Lorenzo García, *On different expressions for invariants of hyperelliptic curves of genus* 3, preprint, 2019. arXiv 1907.05776

[10] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, ASIACRYPT, 2006, pp. 114–129.

[11] J. Igusa, *On Siegel modular forms of genus two*, American Journal of Mathematics **84** (1962), no. 1, 175–200.

[12] S. Ionica, P. Kiliçer, K. E. Lauter, E. Lorenzo García, A. Mânzăţeanu, M. Massierer, and C. Vincent, *Modular invariants for genus 3 hyperelliptic curves*, Research in Number Theory **5** (2018), 1–22.

[13] J.-C. Lario and A. Somoza (appendix by C. Vincent), *An inverse Jacobian algorithm for Picard curves*, preprint, 2020. arXiv 1611.02582

[14] J. S. Milne, *Complex Multiplication*, http://www.jmilne.org/math/CourseNotes/cm.html, 2006.

[15] J. S. Milne, *Abelian varieties*, www.jmilne.org/math/, 2008, pp. 166+vi.

[16] David Mumford, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007.

[17] M. Newman, *Integral matrices*, Pure and Applied Mathematics, vol. 45, Academic Press, 1972.

[18] C. Poor, *The hyperelliptic locus*, Duke Math. J. **76** (1994), no. 3, 809–884.

[19] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998. MR 1492449

[20] T. Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR 0220738

[21] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Leiden University, 2010.

[22] M. Streng, *Computing Igusa class polynomials*, Math. Comp. **83** (2014), no. 285, 275–309. MR 3120590

[23] M. Streng, *An explicit version of Shimura's reciprocity law for Siegel modular functions*, preprint, 2018. arXiv 1201.0020

[24] K. Takase, *A generalization of Rosenhain's normal form for hyperelliptic curves with an application*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), no. 7, 162–165.

[25] The Sage developers, *SageMath, the Sage mathematics software system*, 2016, http://www.sagemath.org.

[26] S. Tsuyumine, *On the Siegel modular field of degree 3*, Compos. Math. **63** (1987), no. 1, 83–98.

[27] A. Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372. MR 1877806

Received 28 Feb 2020. Revised 1 Aug 2020.

BOGDAN ADRIAN DINA: bogdan.dina@uni-ulm.de
Institute of Theoretical Computer Science, Ulm University, Ulm, Germany

SORINA IONICA: sorina.ionica@u-picardie.fr
Laboratoire Modélisation, Information & Systèmes, Université de Picardie Jules Verne, Amiens, France

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS