COMPUTING IGUSA CLASS POLYNOMIALS

MARCO STRENG

Abstract. We give an algorithm that computes the genus-two class polynomials of a primitive quartic CM-field K, and we give a running time bound and a proof of correctness of this algorithm. This is the first proof of correctness and the first running time bound of any algorithm that computes these polynomials. Our algorithm is based on the complex analytic method of Spallek and van Wamelen and runs in time $\widetilde{O}(\Delta^{7/2})$, where Δ is the discriminant of K.

1. Introduction

The *Hilbert class polynomial* $H_K \in \mathbf{Z}[X]$ of an imaginary quadratic number field K has as roots the j-invariants of complex elliptic curves having complex multiplication (CM) by the ring of integers of K. These roots generate the Hilbert class field of K, and Weber [41] computed H_K for many small K. The *CM method* uses the reduction of H_K modulo large primes to construct elliptic curves over $\mathbf{F}_p$ with a prescribed number of points, for example for cryptography. The bit size of H_K grows exponentially with the bit size of K: it grows like the discriminant Δ of K, and, conditionally, so does the running time of the algorithms that compute it ([14, 1]).

If we go from elliptic curves (genus 1) to genus-2 curves, we get the *Igusa class polynomials* $H_{K,n} \in \mathbf{Q}[X]$ $(n = 1, 2, 3)$ of a *quartic CM-field* K. Their roots are the Igusa invariants of all complex genus-2 curves having CM by the ring of integers of K. As in the case of genus 1, these roots generate class fields and the reduction of Igusa class polynomials modulo large primes p yields cryptographically interesting curves of genus 2. Computing Igusa class polynomials is considerably more complicated than computing Hilbert class polynomials, in part because of their denominators. Recently, various algorithms have been developed: a complex analytic method by Spallek [35] and van Wamelen [38], a p-adic method [17, 7, 8] and a Chinese remainder method [13], but no running time or precision bounds were available.

This paper describes a complete and correct algorithm that computes Igusa class polynomials $H_{K,n} \in \mathbf{Q}[X]$ of *quartic CM-fields* $K = \mathbf{Q}(\sqrt{\Delta_0}, \sqrt{-a + b\sqrt{\Delta_0}})$, where Δ_0 is a real quadratic fundamental discriminant and $a, b \in \mathbf{Z}$ are such that $-a+b\sqrt{\Delta_0}$ is totally negative. Our algorithm is based on the complex analytic method of Spallek and van Wamelen. The discriminant Δ of K is of the form $\Delta = \Delta_1\Delta_0^2$ for a positive integer Δ_1. We may and will assume $0 < a < \Delta$, as Lemma 10.9 below shows that each quartic CM-field has such a representation. We disregard the degenerate case of *non-primitive* quartic CM-fields, i.e., those that can be given with $b = 0$, as abelian varieties with CM by non-primitive quartic CM-fields are isogenous to products of CM elliptic curves, which can be obtained already using Hilbert class polynomials. We prove the

Date: 9 February 2011 (first version online: 19 September 2008). See also `http://arxiv.org/abs/0903.4766`.
2010 *Mathematics Subject Classification.* Primary 11G15, Secondary 14K22, 11Y40.

The results in this paper were part of my PhD thesis at Universiteit Leiden, and I would like to express my gratitude to my advisor, Peter Stevenhagen. I am grateful also to Eyal Goren and Kristin Lauter for providing me with preliminary versions of their denominator bounds, which enabled me to start the work on this project without waiting for their publication. Thanks also to Dan Bernstein for providing the reference for Section 11.1. Finally, thanks to David Freeman and members of my PhD committee for suggesting various improvements to the exposition.

following unconditional running time bound for our algorithm. We use $\widetilde{O}(g)$ to mean "at most g times a polynomial in $\log g$".

Main Theorem. *Algorithm 12.1 computes $H_{K,n}$ ($n = 1, 2, 3$) for any primitive quartic CM-field K. It has a running time of $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ and the bit size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.*

An essential part of the proof is the denominator bound, as provided by Goren and Lauter [19, 20]. We do not claim that the bound on our running time is optimal, but an exponential running time is unavoidable, because the degree of the Igusa class polynomials (as with Hilbert class polynomials) is already bounded from below by a power of the discriminant.

Overview. Section 2 provides a precise definition of the Igusa class polynomials that we will work with, and mentions other definitions occurring in the literature. Our main theorem is valid for all types of Igusa class polynomials.

Instead of enumerating curves, it is easier to enumerate their Jacobians, which are principally polarized abelian varieties (see Section 3). Van Wamelen [38] gave a method for enumerating all isomorphism classes of principally polarized abelian varieties with CM by a given order. We give an improvement of his results in Section 4.

Section 5 shows how principally polarized abelian varieties give rise to points in the *Siegel upper half space* $\mathcal{H}_2$. These points are matrices known as *period matrices*. Two period matrices correspond to isomorphic principally polarized abelian varieties if and only if they are in the same orbit under the action of the *symplectic group* $\mathrm{Sp}_4(\mathbf{Z})$. In Section 6, we analyze a reduction algorithm that replaces period matrices by $\mathrm{Sp}_4(\mathbf{Z})$-equivalent ones in a *fundamental domain* $\mathcal{F}_2 \subset \mathcal{H}_2$.

In Section 7, we give an upper bound on the entries of the reduced period matrices computed in Section 6.

Absolute Igusa invariants can be computed from period matrices by means of modular forms known as *(Riemann) theta constants*. Section 8 introduces theta constants and gives formulas that express Igusa invariants in terms of theta constants. The formulas that we give are much simpler than those that appear in [35, 43] or the textbook [16], reducing the formulas from more than a full page to only a few lines. We then give bounds on the absolute values of theta constants and Igusa invariants in terms of the entries of the reduced period matrices.

Section 9 bounds the degree of Igusa class polynomials and Section 10 gives the bounds of Goren and Lauter [19, 20] on the denominators. Section 11 explains how to reconstruct a rational polynomial from its complex roots.

Finally, Section 12 puts all the results together into a single algorithm and a proof of the main theorem.

Remark 1.1. Our methods can also be applied to the case of elliptic curves, though most steps are then overly complicated or unnecessary. In fact, Theorem 11.1 below, together with the main results of Dupont [10], forms exactly the missing rounding error analysis of Enge [14]. This shows that the main result of [14], which bounds the running time of computing Hilbert class polynomials, is valid also without its heuristic assumption. This is the first unconditional bound on the running time of the computation of Hilbert class polynomials.

2. Igusa class polynomials

The *Hilbert class polynomial* of an imaginary quadratic number field K is the polynomial of which the roots in $\mathbf{C}$ are the *j-invariants* of the elliptic curves over $\mathbf{C}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. For a genus-2 curve, one needs three *absolute Igusa invariants* i_1, i_2, i_3, instead of only one j-invariant, to fix its isomorphism class.

2.1. **Igusa invariants.** Let k be a field of characteristic different from 2. Any curve of genus 2 over k, i.e., a projective, smooth, geometrically irreducible, algebraic curve over k of which the genus is 2, has an affine model of the form $y^2 = f(x)$, where $f \in k[x]$ is a separable polynomial of degree 6. Let $\alpha_1, \ldots, \alpha_6$ be the six distinct roots of f in $\overline{k}$, and let a_6 be the leading coefficient. For any permutation $\sigma \in S_6$, let (ij) denote the difference $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$. We can then define the *homogeneous Igusa-Clebsch invariants* in compact notation that we explain below, as

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

The sum is taken over all distinct expressions (in the roots of f) that are obtained when σ ranges over S_6. The subscript indicates the number of expressions encountered. For example, for I_4 there are 10 ways of partitioning the six roots of f into two subsets of three, and each yields a summand that is the product of two cubic discriminants. For each of the 10 ways of partitioning the six roots of f into two subsets of three, there are 6 ways of giving a bijection between those two subsets, and each gives a summand for I_6.

The invariant I_{10} is simply the discriminant of f, which is non-zero as f is separable. The invariants I_2, I_4, I_6, I_{10} were introduced by Igusa [23], who denoted them by A, B, C, D and based them on invariants of Clebsch.

By the symmetry in the definition, each of the homogeneous invariants is actually a polynomial in the coefficients of f, hence an element of k. Actually, we will use another homogeneous invariant, given by $I_6' = \frac{1}{2}(I_2 I_4 - 3I_6)$, which is "smaller" than I_6 as we will see in Section 8.

We define the *absolute Igusa invariants* by

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

The values of the absolute Igusa invariants of a curve C depend only on the $\overline{k}$-isomorphism class of the curve C. For any triple (i_1^0, i_2^0, i_3^0), if 3 and i_3^0 are non-zero in k, then there exists a curve C of genus 2 (unique up to isomorphism) over $\overline{k}$ with $i_n(C) = i_n^0$ $(n = 1, 2, 3)$, and this curve can be constructed using an algorithm of Mestre [31]. The case $i_3^0 = 0$ can be dealt with by using additional or modified absolute Igusa invariants. See also Section III.5 of the author's thesis [36] (especially equation (5.3)).

2.2. **Igusa class polynomials.**

Definition 2.1. Let K be a primitive quartic CM-field. The *Igusa class polynomials* of K are the three polynomials

$$H_{K,n} = \prod_C (X - i_n(C)) \quad \in \mathbf{Q}[X] \quad (n \in \{1, 2, 3\}),$$

where the product ranges over the isomorphism classes of algebraic genus-2 curves over $\mathbf{C}$ of which the Jacobian has complex multiplication by $\mathcal{O}_K$.

For the definitions of the Jacobian and complex multiplication, see Section 3. We will see in Section 4 that the product in the definition is indeed finite. The polynomial is rational, because any conjugate of a CM curve has CM by the same ring.

2.3. **Alternative invariants.** In the literature, one finds various sets of absolute Igusa invariants. For example, [6], [28], [23], and [35] all make different choices. The invariants of Igusa [23] have good reduction behaviour at all primes, including 2 and 3. The triple of invariants that seems most standard in computations is Spallek's $j_1 = 2^{-3} I_2^5 I_{10}^{-1}$, $j_2 = 2 I_2^3 I_4 I_{10}^{-1}$, $j_3 = 2^3 I_2^2 I_6 I_{10}^{-1}$ (occurring up to powers of 2 in [16, 19, 35, 38, 43, 44]). However, our choice of absolute invariants i_1, i_2, i_3 yields Igusa class polynomials of much smaller height, both experimentally (see Appendix 3 of [36]) and in terms of proven bounds (see Remarks 8.5 and 10.3 below).

If the base field k has characteristic 0, then Igusa's and Spallek's absolute invariants, as well as most of the other invariants in the literature, lie in the $\mathbf{Q}$-algebra A of homogeneous elements of degree 0 of $\mathbf{Q}[I_2, I_4, I_6, I_{10}^{-1}]$. Our main theorem remains true if (i_1, i_2, i_3) in the definition of the Igusa class polynomials is replaced by any finite list of elements of A.

2.4. **Interpolation formulas.** If we take one root of each of the Igusa class polynomials, then we get a triple of invariants and thus (if $i_3 \neq 0$) an isomorphism class of curve of genus 2. That way, the three Igusa class polynomials describe d^3 triples of invariants, where d is the degree of the polynomials. The d triples corresponding to curves with CM by $\mathcal{O}_K$ are among them, but the Igusa class polynomials give no means of telling which they are.

To solve this problem, (and thus greatly reduce the number of curves to be checked during explicit CM constructions), we use the following modified Lagrange interpolation:

$$\widehat{H}_{K,n} = \sum_C \left(i_n(C) \prod_{C' \neq C} (X - i_1(C')) \right) \quad \in \mathbf{Q}[X], \quad (n \in \{2,3\}).$$

If $H_{K,1}$ has no roots of multiplicity greater than 1, then the triples of invariants corresponding to curves with CM by $\mathcal{O}_K$ are exactly the triples (i_1, i_2, i_3) such that

$$H_{K,1}(i_1) = 0, \quad i_n = \frac{\widehat{H}_{K,n}(i_1)}{H'_{K,1}(i_1)} \quad (n \in \{2,3\}).$$

Our main theorem is also valid if we replace $H_{K,2}$ and $H_{K,3}$ by $\widehat{H}_{K,2}$ and $\widehat{H}_{K,3}$.

This way of representing algebraic numbers (like our i_2, i_3) in terms of others (our i_1) appears in Hecke [22, Hilfssatz a in §36], and is sometimes called *Hecke representation* (e.g. [15]). The idea to use this modified Lagrange interpolation in the definition of Igusa class polynomials is due to Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng [17], who give a heuristic argument that the height of the polynomials $\widehat{H}_{K,n}$ is smaller than the height of the usual Lagrange interpolation.

If $H_{K,1}$ has only double roots, then these interpolation formulas are useless. In practice, this never happens, but for the theoretical possibility that it does happen, see Section III.5 of [36]. There it is proven that our main result applies also to computing the CM-by-K locus inside the coarse moduli space $\mathrm{Spec}(A)$ of genus-2 curves.

3. Jacobians and complex multiplication

Instead of enumerating CM curves, we enumerate their *Jacobians*. We now quickly recall the definition from [2]. Given a smooth projective irreducible algebraic curve $C/\mathbf{C}$, let $H^0(\omega_C)^*$ be dual of the complex vector space of holomorphic 1-forms on C. Its dimension g is the genus of C and our main result concerns the case $g = 2$. There is a canonical injection of the homology group $H_1(C, \mathbf{Z})$ into $H^0(\omega_C)^*$, and the image is a lattice of rank $2g$. The quotient complex torus $J(C) = H^0(\omega_C)^*/H_1(C, \mathbf{Z})$ is the *(unpolarized) Jacobian* of C.

The *endomorphism ring* $\mathrm{End}(\mathbf{C}^g/\Lambda)$ of a complex torus $\mathbf{C}^g/\Lambda$ is the ring of $\mathbf{C}$-linear automorphisms of $\mathbf{C}^g$ that map Λ into itself. A *CM-field* is a totally imaginary quadratic extension of a totally real number field. We say that a complex torus T of (complex) dimension g has *complex*

multiplication (or *CM*) by an order $\mathcal{O} \subset K$ if K has degree $2g$ and there exists an embedding $\mathcal{O} \to \mathrm{End}(T)$. We say that a curve C has CM if $J(C)$ does.

It turns out that $J(C)$ is not just any complex torus, but that it comes with a natural *principal polarization*. A polarization of a complex torus $\mathbf{C}^g/\Lambda$ is an alternating $\mathbf{R}$-bilinear form $E : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$ such that $E(\Lambda, \Lambda) \subset \mathbf{Z}$ holds and $(u, v) \mapsto E(iu, v)$ is symmetric and positive definite. The degree of a polarization is the determinant of the matrix M that expresses E in terms of a $\mathbf{Z}$-basis of Λ. We call a polarization *principal* if its degree is 1. If we denote by $\cdot$ the anti-symmetric intersection pairing on $H_1(C, \mathbf{Z})$ extended $\mathbf{R}$-linearly to $H^0(\omega_C)^*$, then $E : (u, v) \mapsto -u \cdot v$ defines a principal polarization on $J(C)$. By the *(polarized) Jacobian* of C, we mean the torus together with this principal polarization.

A torus together with a (principal) polarization, such as the Jacobian of a curve, is called a *(principally) polarized abelian variety*. An *isomorphism* $f : (\mathbf{C}^g/\Lambda, E) \to (\mathbf{C}^g/\Lambda', E')$ of (principally) polarized abelian varieties is a $\mathbf{C}$-linear isomorphism $f : \mathbf{C}^g \to \mathbf{C}^g$ such that $f(\Lambda) = \Lambda'$ and $f^*E' = E$, where $f^*E'(u, v) = E(f(u), f(v))$ for all $u, v \in \mathbf{C}^g$.

Theorem 3.1 (Torelli [2, Thm. 11.1.7])**.** *Two algebraic curves over* $\mathbf{C}$ *are isomorphic if and only if their Jacobians are isomorphic (as polarized abelian varieties).* □

The product of two polarized abelian varieties (T_1, E_1) and (T_2, E_2) has a natural polarization $(v, w) \mapsto E_1(v_1, w_1) + E_2(v_2, w_2)$ called the *product polarization*.

Theorem 3.2 (Weil)**.** *Any principally polarized abelian surface over* $\mathbf{C}$ *is either a product of elliptic curves with the product polarization or the Jacobian of a smooth projective curve of genus* 2*.*

Proof. This is [42, Satz 2] or [2, Corollary 11.8.2]. See also Remark 8.11 below. □

4. Abelian varieties with CM

In this section, we give an algorithm that computes a complete set of representatives of the isomorphism classes CM abelian varieties needed for our main result.

First, Section 4.1 shows how a CM abelian variety is represented as a quotient of $\mathbf{C}^g$ by an ideal of K. Section 4.2 makes this into an algorithm, which works for CM-fields of arbitrary degree. In Section 4.3, we specialize to the case of quartic CM-fields. Finally, Section 4.4 gives details needed for proving that this algorithm is fast enough, and that it gives sufficiently small output.

4.1. CM abelian varieties as quotients by ideals.

Let K be any CM-field of degree $2g$. A *CM-type* of K with values in $\mathbf{C}$ is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ consisting of one embedding $\phi_i : K \to \mathbf{C}$ for each complex conjugate pair of embeddings. We identify Φ with the ring homomorphism $K \to \mathbf{C}^g$ given by $\Phi(\alpha) = (\phi_1(\alpha), \ldots, \phi_g(\alpha))$. Let $\rho_\Phi : K \to \mathrm{End}_{\mathbf{C}}(\mathbf{C}^g) : \alpha \mapsto \mathrm{diag}\,\Phi(\alpha)$.

We say that Φ is *induced* from $K_1 \subset K$ if $\{\phi_{|K_1} : \phi \in \Phi\}$ is a CM-type of K_1. We say that Φ is *primitive* if it is not induced from a CM-subfield $K_1 \neq K$.

Let $A = \mathbf{C}^g/\Lambda$ be an abelian variety with CM by an order in a CM-field K, and let ι be an embedding $K \to \mathrm{End}(A) \otimes \mathbf{Q}$. It is known ([34, §5.2 in Chapter II]) that the composite map $\rho : K \to \mathrm{End}(A) \otimes \mathbf{Q} \to \mathrm{End}_{\mathbf{C}}(\mathbf{C}^g)$ equals ρ_Φ for some CM-type Φ and some choice of basis of $\mathbf{C}^g$. We say that A is *of type* Φ with respect to ι.

Let $\mathcal{D}_{K/\mathbf{Q}}$ be the different of K, let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$-ideal, and suppose that there exists $\xi \in K$ such that $\xi\mathcal{O}_K$ equals $(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ and $\phi(\xi)$ lies on the positive imaginary axis for every $\phi \in \Phi$. Then the map $E = E_{\Phi,\xi} : \Phi(K) \times \Phi(K) \to \mathbf{Q}$ given by

$$E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{K/\mathbf{Q}}(\xi \bar{x} y) \quad \text{for } x, y \in K \tag{4.1}$$

is integer valued on $\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a})$, and can be extended uniquely $\mathbf{R}$-linearly to an $\mathbf{R}$-bilinear form $E = E_{\Phi,\xi} : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$.

Theorem 4.2. *Suppose Φ is a CM-type of a CM-field K of degree $2g$. Then the following holds.*

1. *For any triple $(\Phi, \mathfrak{a}, \xi)$ as above, the pair $(\mathbf{C}^g/\Phi(\mathfrak{a}), E)$ defines a principally polarized abelian variety $A(\Phi, \mathfrak{a}, \xi)$ with CM by $\mathcal{O}_K$ of type Φ.*
2. *Every principally polarized abelian variety over $\mathbf{C}$ with CM by $\mathcal{O}_K$ of type Φ is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triple $(\Phi, \mathfrak{a}, \xi)$ as in part 1.*
3. *The abelian variety $A(\Phi, \mathfrak{a}, \xi)$ is simple if and only if Φ is primitive. If this is the case, then the embedding $\iota : K \to \mathrm{End}(A) \otimes \mathbf{Q}$ is an isomorphism.*
4. *Let $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi, \mathfrak{a}', \xi')$ be triples as above with the same CM-type Φ. If there exists $\gamma \in K^*$ such that*
   (a) *$\mathfrak{a}' = \gamma\mathfrak{a}$ and*
   (b) *$\xi' = (\gamma\overline{\gamma})^{-1}\xi$,*
   then the principally polarized abelian varieties $A(\Phi, \mathfrak{a}, \xi)$ and $A(\Phi, \mathfrak{a}', \xi')$ are isomorphic. If Φ is primitive, then the converse holds.

Proof. This result can be derived from Shimura-Taniyama [34], and first appeared in a form similar to the above in Spallek [35, Sätze 3.13, 3.14, 3.19]. See van Wamelen [38, Thms. 1, 3, 5] for a detailed published proof. □

We call two triples $(\Phi, \mathfrak{a}, \xi)$ with the same type Φ *equivalent* if they satisfy the conditions 4a and 4b of Theorem 4.2.

Let K be any CM-field with maximal totally real subfield K_0. Let h (resp. h_0) be the class number of K (resp. K_0) and let $h_1 = h/h_0$.

Proposition 4.3. *The number of pairs (Φ, A), where Φ is a CM-type and A is an isomorphism class of abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$ of type Φ, is*

$$h_1 \cdot \#\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*).$$

Proof. Let I be the group of invertible $\mathcal{O}_K$-ideals and S the set of pairs $(\mathfrak{a}, \xi)$ with $\mathfrak{a} \in I$ and $\xi \in K^*$ such that ξ^2 is totally negative and $\xi\mathcal{O}_K = (\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$. The group K^* acts on S via $x(\mathfrak{a}, \xi) = (x\mathfrak{a}, x^{-1}\overline{x}^{-1}\xi)$ for $x \in K^*$. By Theorem 4.2, the set that we need to count is in bijection with the set $K^*\backslash S$ of orbits.

The fact that S is non-empty is [38, Thm. 4]. We give a shorter proof here. Let $z \in K^*$ be such that z^2 is a totally negative element of K_0. Note that $z\mathcal{D}_{K/K_0} = (z(\alpha - \overline{\alpha}) : \alpha \in \mathcal{O}_K)$ is generated by elements of K_0, hence is of the form $\mathfrak{h}\mathcal{O}_K$ for some fractional $\mathcal{O}_{K_0}$-ideal $\mathfrak{h}$. The norm map $N_{K/K_0} : \mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ is surjective because infinite primes ramify in K/K_0 (see [40, Thm. 10.1]). In particular, there exist an element $y \in K_0^*$ and a fractional $\mathcal{O}_K$-ideal $\mathfrak{a}_0$ such that $y\mathfrak{a}_0\overline{\mathfrak{a}_0} = \mathfrak{h}^{-1}\mathcal{D}_{K_0/\mathbf{Q}}^{-1} = z^{-1}\mathcal{D}_{K/\mathbf{Q}}^{-1}$ holds, so $(\mathfrak{a}_0, yz)$ is an element of S.

Let S' be the group of pairs $(\mathfrak{b}, u)$, consisting of a fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ and a totally positive generator $u \in K_0^*$ of $\mathfrak{b}\overline{\mathfrak{b}}$. The group K^* acts on S' via $x(\mathfrak{b}, u) = (x\mathfrak{b}, x\overline{x}u)$ for $x \in K^*$, and we denote the group of orbits by $C = K^*\backslash S'$. The map $C \to K^*\backslash S : (\mathfrak{b}, u) \mapsto (\mathfrak{b}\mathfrak{a}_0, u^{-1}yz)$ is a bijection and the sequence

$$0 \longrightarrow \mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) \underset{u \mapsto (\mathcal{O}_K, u)}{\longrightarrow} C \underset{(\mathfrak{b},u) \mapsto \mathfrak{b}}{\longrightarrow} \mathrm{Cl}(K) \underset{N}{\longrightarrow} \mathrm{Cl}(K_0) \longrightarrow 0$$

is exact, so $K^*\backslash S$ has the correct order. □

Remark 4.4. The existence statement of Proposition 4.3 contradicts the first remark below Proposition 1 of [9]. It turns out that that remark is false, and it follows that the example given in order to prove that remark does not exist. That is, if F is real quadratic with class number 1 and a fundamental unit of norm 1, then there is no cyclic quartic CM-field containing F.

The following two lemmas show what happens with distinct CM-types and thus answer a question of van Wamelen [38].

Lemma 4.5. *For any triple $(\Phi, \mathfrak{a}, \xi)$ as above and $\sigma \in \mathrm{Aut}(K)$, we have*

$$A(\Phi, \mathfrak{a}, \xi) \cong A(\Phi \circ \sigma, \sigma^{-1}(\mathfrak{a}), \sigma^{-1}(\xi)).$$

Proof. We find twice the same complex torus $\mathbf{C}^g/\Phi(\mathfrak{a})$. The first has polarization

$$E : (\Phi(\alpha), \Phi(\beta)) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\alpha}\beta) \tag{4.6}$$

for $\alpha, \beta \in \mathfrak{a}$ while the polarization of the second maps $(\Phi(\alpha), \Phi(\beta))$ to $\mathrm{Tr}_{K/\mathbf{Q}}(\sigma^{-1}(\xi\overline{\alpha}\beta))$, which equals the right hand side of (4.6). □

Definition 4.7. We call two CM-types Φ and Φ' of K *equivalent* if there exists $\sigma \in \mathrm{Aut}(K)$ with $\Phi' = \Phi \circ \sigma$.

Lemma 4.8. *Suppose A and B are abelian varieties over $\mathbf{C}$ with CM by K of types Φ and Φ'. If Φ is primitive and not equivalent to Φ', then A and B are not isogenous. In particular, they are not isomorphic.*

Proof. Suppose $f : A \to B$ are isogenous. The isogeny induces an isomorphism $\varphi : \mathrm{End}(A) \otimes \mathbf{Q} \to \mathrm{End}(B) \otimes \mathbf{Q}$ given by $g \mapsto fgf^{-1}$. Let $\iota_A : K \to \mathrm{End}(A) \otimes \mathbf{Q}$ and $\iota_B : K \to \mathrm{End}(B) \otimes \mathbf{Q}$ be the embeddings of types Φ and Φ'. Let $\sigma = \iota_B^{-1}\varphi\iota_A$ (where ι_B is an isomorphism by Theorem 4.2.3 because Φ' is primitive). Then (A, ι_A) and $(B, \iota_B \circ \sigma)$ have types Φ and $\Phi'\sigma$. As f induces an isomorphism of the tangent spaces, we also see that these types are equal, so Φ and Φ' are equivalent. □

Definition 4.9. We call two triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi', \mathfrak{a}', \xi')$ *equivalent* if there is an automorphism $\sigma \in \mathrm{Aut}(K)$ such that $\Phi \circ \sigma = \Phi'$ holds and $(\Phi, \sigma(\mathfrak{a}'), \sigma(\xi'))$ is equivalent to $(\Phi, \mathfrak{a}, \xi)$ as in our definition below Theorem 4.2.

If Φ is primitive, then it follows from Theorem 4.2.4 and Lemmas 4.5 and 4.8 that $A(\Phi, \mathfrak{a}, \xi)$ and $A(\Phi', \mathfrak{a}', \xi')$ are isomorphic if and only if $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi', \mathfrak{a}', \xi')$ are equivalent.

4.2. **The algorithm.**

Algorithm 4.10.
Input: A CM-field K with maximal totally real subfield K_0 such that K does not contain a strict CM-subfield.
Output: A complete set of representatives for the equivalence classes of principally polarized abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$, each given by a triple $(\Phi, \mathfrak{a}, \xi)$ as in Theorem 4.2.

(1) Let T be a complete set of representatives of the equivalence classes of CM-types of K with values in $\mathbf{C}$.
(2) Let W be a complete set of representatives of the quotient
$$\mathcal{O}_K^*/N_{K/K_0}(\mathcal{O}_K^*).$$
(3) Let I be a complete set of representatives of the ideal class group of K.
(4) Take those $\mathfrak{a}$ in I such that $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ is principal. For each, take a generator ξ_0.
(5) For every pair $(\mathfrak{a}, \xi_0)$ and every $w \in W$ such that $\xi = w\xi_0$ is totally imaginary, take the CM-type Φ consisting of those embeddings of K into $\mathbf{C}$ that map ξ to the positive imaginary axis.
(6) Return those triples $(\Phi, \mathfrak{a}, \xi)$ of step 5 for which Φ is in T.

Proof. By Theorem 4.2.1, the output consists only of principally polarized abelian varieties with CM by $\mathcal{O}_K$. Conversely, by Theorem 4.2.2, every principally polarized abelian variety A with CM by $\mathcal{O}_K$ is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triple $(\Phi, \mathfrak{a}, \xi)$, and we will show now that such a triple is found by the algorithm.

By Lemmas 4.5 and 4.8, the CM-type Φ is unique exactly up to equivalence of CM-types. This uniquely determines Φ in T.

By Theorem 4.2.4, the ideal class of $\mathfrak{a}$ is then uniquely determined, hence we find a unique $\mathfrak{a} \in I$. The class of ξ modulo $N_{K/K_0}(\mathcal{O}_K^*)$ is uniquely determined by Theorem 4.2.4, hence so is ξ as found in the algorithm. □

Remark 4.11. Algorithm 4.10 is basically Algorithm 1 of van Wamelen [38] with the difference that we do not have any duplicate abelian varieties.

4.3. **Quartic CM-fields.** We now describe, in the quartic case, the sets T and W of Algorithm 4.10, and the number of isomorphism classes of principally polarized CM abelian surfaces.

Lemma 4.12 (Example 8.4(2) of [34])**.** *Let K be a quartic CM-field with a CM-type $\Phi = \{\phi_1, \phi_2\}$. Exactly one of the following holds.*

1. *$K/\mathbf{Q}$ is Galois with Galois group $C_2 \times C_2$ and each CM-type of K is non-primitive and induced from an imaginary quadratic subfield of K,*
2. *$K/\mathbf{Q}$ is cyclic Galois, and all four CM-types are equivalent and primitive,*
3. *$K/\mathbf{Q}$ is non-Galois, its normal closure has Galois group D_4, each CM-type is primitive, and the equivalence classes of CM-types are $\{\Phi, \overline{\Phi}\}$ and $\{\Phi', \overline{\Phi'}\}$ with $\Phi' = \{\phi_1, \overline{\phi_2}\}$.* □

Note that in particular, either all CM-types are primitive or none of them are. This is why we use the word *(non-)primitive* also for the quartic CM-fields themselves.

Lemma 4.12 shows that we can take the set T to consist of a single CM-type if K is cyclic and we can take $T = \{\Phi, \Phi'\}$ if K is non-Galois.

The following lemma gives the set W.

Lemma 4.13. *If K is a primitive quartic CM-field, then*

$$\mathcal{O}_K^* = \mu_K \mathcal{O}_{K_0}^* \quad \text{and} \quad N_{K/K_0}(\mathcal{O}_K^*) = (\mathcal{O}_{K_0}^*)^2,$$

where $\mu_K \subset \mathcal{O}_K^*$ is the group of roots of unity, which has order 2 or 10.

Proof. As K has degree 4 and does not contain a primitive third or fourth root of unity, it is either $\mathbf{Q}(\zeta_5)$ or does not contain a root of unity different from ± 1. This proves that μ_K has order 2 or 10. A direct computation shows that the lemma is true for $K = \mathbf{Q}(\zeta_5)$, so we assume that we have $\mu_K = \{\pm 1\}$.

Note that the second identity follows from the first, so we only need to prove the first. Let ϵ (resp. ϵ_0) be a generator of $\mathcal{O}_K^*$ (resp. $\mathcal{O}_{K_0}^*$) modulo $\langle -1 \rangle$. Then without loss of generality, we have $\epsilon_0 = \epsilon^k$ for some positive integer k. so either $k = 1$ and we are done, or $k = 2$.

Suppose that we have $k = 2$. As $K = K_0(\sqrt{\epsilon_0})$ is a CM-field, we find that ϵ_0 is totally negative, and hence ϵ_0^{-1} is the conjugate of ϵ_0. Let $x = \epsilon - \epsilon^{-1} \in K$. Then $x^2 = -2 + \epsilon_0 + \epsilon_0^{-1} = -2 + \mathrm{Tr}(\epsilon_0) \in \mathbf{Z}$ is negative, so $\mathbf{Q}(x) \subset K$ is imaginary quadratic, contradicting primitivity of K. □

In particular, we can take $W = \mu_K \cup \epsilon \mu_K$ for a fundamental unit ϵ of $\mathcal{O}_{K_0}^*$.

Lemma 4.14. *Let K be a quartic CM-field. If K is cyclic, then there are h_1 isomorphism classes of principally polarized abelian surfaces with CM by $\mathcal{O}_K$. If K is non-Galois, then there are $2h_1$ such isomorphism classes.*

Proof. Proposition 4.3 gives the number $h_1 \cdot \#\mathcal{O}_{K_0}^* / N_{K/K_0}(\mathcal{O}_K^*)$, but counts every abelian variety twice if K is non-Galois and four times if K is cyclic Galois (see Lemma 4.12). Lemma 4.13 shows that we have $\#\mathcal{O}_{K_0}^* / N_{K/K_0}(\mathcal{O}_K^*) = 4$. □

4.4. **Implementation details.** In practice, Algorithm 4.10 takes up only a very small portion of the time needed for Igusa class polynomial computation. The purpose of this section is to show that, for primitive quartic CM-fields, indeed Algorithm 4.10 can be run in time $\widetilde{O}(\Delta)$ and to show that the size of the output for each isomorphism class is small: only polynomial in $\log \Delta$.

It is well known that lists of representatives for the class groups of number fields K of fixed degree can be computed in time $\widetilde{O}(|\Delta|^{\frac{1}{2}})$, where Δ is the discriminant of K. For details, see Schoof [33]. The representatives of the ideal classes that are given in the output are integral ideals of norm below the Minkowski bound, which is $3/(2\pi^2)\,|\Delta|^{1/2}$ for a quartic CM-field.

The algorithms in [33] show that for each $\mathfrak{a}$, we can check in time $\widetilde{O}(|\Delta|^{\frac{1}{2}})$ if $\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}}$ is principal and, if so, write down a generator ξ. As $\mathcal{O}_K^* = \mu_K \mathcal{O}_{K_0}^*$, it suffices to check, for each of the roots of unity ζ in K, if $\zeta\xi$ is totally imaginary (note that $\mathbf{Q}(\zeta_5)$ is the only primitive quartic CM-field with more than 2 roots of unity). Then the set T and the group $\mathcal{O}_{K_0}^* / N_{K/K_0}(\mathcal{O}_K^*)$ are already given in Section 4.3, where the fundamental unit ϵ is a by-product of the class group computations. In particular, it takes time at most $\widetilde{O}(|\Delta|)$ to perform all the steps of Algorithm 4.10.

A priori, the bit size of ξ can be as large as the regulator of K, but we can easily make it much smaller as follows. We identify $K \otimes \mathbf{R}$ with $\mathbf{C}^2$ via the embeddings ϕ_1, ϕ_2 in the CM-type Φ, and we consider the standard Euclidean norm on $\mathbf{C}^2$. Then we find a short vector

$$b\,|\xi|^{-1/2} = \left(\phi_1(b)\,|\phi_1(\xi)|^{-1/2}, \phi_2(b)\,|\phi_2(\xi)|^{-1/2}\right)$$

in the lattice $\mathcal{O}_K\,|\xi|^{-1/2} \subset \mathbf{C}^2$ and replace $\mathfrak{a}$ by $b\mathfrak{a}$ and ξ by $(b\bar{b})^{-1}\xi$. To find this short vector, we use a version of the LLL-algorithm that is linear in the bit size of the input for fixed dimension, as in [12].

By part 4 of Theorem 4.2, the change of $(\mathfrak{a}, \xi)$ to $(b\mathfrak{a}, (b\bar{b})^{-1}\xi)$ does not change the corresponding isomorphism class of principally polarized abelian varieties. This also doesn't change the fact that ξ^{-1} is in $\mathcal{O}_K$ and that $\mathfrak{a}$ is an integral ideal. Finally, we compute an LLL-reduced basis of $\mathfrak{a} \subset \mathcal{O}_K \otimes \mathbf{R} = \mathbf{C}^2$. We get the following result.

Lemma 4.15. *If we run Algorithm 4.10 in the way we have just described, then on input of a primitive quartic CM-field K, given as*

$$K = \mathbf{Q}(\sqrt{\Delta_0}, \sqrt{-a + b\sqrt{\Delta_0}})$$

for integers a, b, Δ_0 with $0 < a < \Delta$, it takes time $\widetilde{O}(\Delta)$. For each triple $(\Phi, \mathfrak{a}, \xi)$ in the output, the ideal $\mathfrak{a}$ is given by an LLL-reduced basis, and both $\xi \in K$ and the basis of $\mathfrak{a}$ have bit size $O(\log \Delta)$.

Proof. First, compute the ring of integers $\mathcal{O}_K$ of K using the algorithm of Buchmann and Lenstra [5]. This takes polynomial time plus the time needed to factor the discriminant of the defining polynomial of K, which is small enough because of the assumption $0 < a < \Delta$. Then do the class group computations as explained above.

For each triple $(\Phi, \mathfrak{a}, \xi)$, before we apply the LLL-reduction, we can assume that $\mathfrak{a}$ is an integral ideal of norm below the Minkowski bound, hence we have

$$N_{K/\mathbf{Q}}(\xi^{-1}) = N_{K/\mathbf{Q}}(\mathfrak{a})^2 N_{K/\mathbf{Q}}(\mathcal{D}_{K/\mathbf{Q}}) \leq C\Delta^3$$

for some constant C.

The covolume of the lattice

$$|\xi|^{-1/2}\,\mathcal{O}_K \subset \mathcal{O}_K \otimes \mathbf{R} = \mathbf{C}^2$$

is $N_{K/\mathbf{Q}}(\xi^{-1})\Delta^{1/2}$, so we find a vector $b\,|\xi|^{-1/2} \in |\xi|^{-1/2}\,\mathcal{O}_K$ of length $\leq C'(N_{K/\mathbf{Q}}(\xi^{-1})\Delta)^{1/8}$ for some constant C'. In particular, $b\bar{b}\xi^{-1}$ has all absolute values below ${C'}^2 N_{K/\mathbf{Q}}(\xi^{-1})^{1/4}\Delta^{1/4}$. Therefore, $b\bar{b}\xi^{-1}$ has bit size $O(\log\Delta)$ and norm at most ${C'}^8 N_{K/\mathbf{Q}}(\xi^{-1})\Delta$, so b has norm at most ${C'}^4\Delta^{1/2}$.

This implies that $b\mathfrak{a}$ has norm at most $C''\Delta$, so an LLL-reduced basis has a bit size that is $O(\log(\mathrm{covol}(b\mathfrak{a}))) = O(\log\Delta)$.

All elements $x \in K$ that we encounter can be given (up to multiplication by units in $\mathcal{O}_{K_0}^*$) with all absolute values below $\sqrt{N_{K/\mathbf{Q}}(a)}\,|\epsilon|$. Therefore, the bit size of the numbers that are input to the LLL-algorithm is $\widetilde{O}(\mathrm{Reg}_K) = \widetilde{O}(\Delta^{1/2})$, hence every execution of the LLL algorithm takes time only $\widetilde{O}(\Delta^{1/2})$ for each ideal class. □

5. Symplectic bases

5.1. **Symplectic bases, period matrices, and the action of the symplectic group.** Let $(\mathbf{C}^g/\Lambda, E)$ be a principally polarized abelian variety. For any basis $b_1, \ldots, b_{2g}$ of Λ, we associate to the form E the matrix $N = (n_{ij})_{ij} \in \mathrm{Mat}_{2g}(\mathbf{Z})$ given by $n_{ij} = E(b_i, b_j)$. We say that E is given with respect to the basis $b_1, \ldots, b_{2g}$ by the matrix N.

The lattice Λ has a basis that is *symplectic* with respect to E, i.e., a $\mathbf{Z}$-basis $e_1, \ldots, e_g, v_1, \ldots, v_g$ with respect to which E is given by the matrix Ω, given in terms of $(g \times g)$-blocks as

$$\Omega = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}. \tag{5.1}$$

The vectors v_i form a $\mathbf{C}$-basis of $\mathbf{C}^g$ and if we rewrite $\mathbf{C}^g$ and Λ in terms of this basis, then Λ becomes $Z\mathbf{Z}^g + \mathbf{Z}^g$, where Z is a *period matrix*, i.e., a symmetric matrix over $\mathbf{C}$ with positive definite imaginary part. The set of all $g \times g$ period matrices is called the *Siegel upper half space* and denoted by $\mathcal{H}_g$. It is a subset of the Euclidean $2g^2$-dimensional real vector space $\mathrm{Mat}_g(\mathbf{C})$.

There is an action on this space by the *symplectic group*

$$\mathrm{Sp}_{2g}(\mathbf{Z}) = \{M \in \mathrm{GL}_{2g}(\mathbf{Z}) : M^{\mathrm{t}}\Omega M = \Omega\} \subset \mathrm{GL}_{2g}(\mathbf{Z}),$$

given in terms of $(g \times g)$-blocks by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}(Z) = (AZ + B)(CZ + D)^{-1}.$$

The association of Z to $(\mathbf{C}^g/Z\mathbf{Z}^g + \mathbf{Z}^g, E)$ gives a bijection between the set $\mathrm{Sp}_{2g}(\mathbf{Z})\backslash\mathcal{H}_g$ of orbits and the set of principally polarized abelian varieties over $\mathbf{C}$ up to isomorphism.

5.2. **Finding a symplectic basis for $\Phi(\mathfrak{a})$.** Now it is time to compute symplectic bases. In Algorithm 4.10, we computed a set of abelian varieties over $\mathbf{C}$, each given by a triple $(\Phi, \mathfrak{a}, \xi)$, where $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$, given by a basis, ξ is in K^* and Φ is a CM-type of K. We identify $\mathfrak{a}$ with the lattice $\Lambda = \Phi(\mathfrak{a}) \subset \mathbf{C}^g$ and recall that the bilinear form $E : \mathfrak{a} \times \mathfrak{a} \to \mathbf{Z}$ is given by $E : (x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{x}y)$. We can write down the matrix $N \in \mathrm{Mat}_{2g}(\mathbf{Z})$ of E with respect to the basis of $\mathfrak{a}$. Computing a symplectic basis of $\mathfrak{a}$ then comes down to computing a change of basis $M \in \mathrm{GL}_{2g}(\mathbf{Z})$ of $\mathfrak{a}$ such that $M^{\mathrm{t}}NM = \Omega$, with Ω as in (5.1). This is done by the following algorithm.

Algorithm 5.2.
Input: A matrix $N \in \mathrm{Mat}_{2g}(\mathbf{Z})$ such that $N^{\mathrm{t}} = -N$ and $\det N = 1$.

Output: $M \in \mathrm{GL}_{2g}(\mathbf{Z})$ satisfying $M^{\mathrm{t}} N M = \Omega$.
For $i = 1, \ldots, g$, do the following.

(1) Let $e'_i \in \mathbf{Z}^{2g}$ be a vector linearly independent of
$$\{e_1, \ldots, e_{i-1}, v_1, \ldots, v_{i-1}\}.$$
(2) From e'_i, compute the following vector e_i, which is orthogonal to $e_1, \ldots, e_{i-1}$, $v_1, \ldots, v_{i-1}$:
$$e_i = \tfrac{1}{k}\left(e'_i - \textstyle\sum_{j=1}^{i-1}(e_j^{\mathrm{t}} N e'_i) v_j + \sum_{j=1}^{i-1}(v_j^{\mathrm{t}} N e'_i) e_j\right),$$
where k is the largest positive integer such that the resulting vector e_i is in $\mathbf{Z}^{2g}$.
(3) Let v'_i be such that $e_i^{\mathrm{t}} N v'_i = 1$. We will explain this step below.
(4) From v'_i, compute the following vector v_i, which is orthogonal to $e_1, \ldots, e_{i-1}$, $v_1, \ldots, v_{i-1}$ and satisfies $e_i^{\mathrm{t}} N v_i = 1$:
$$v_i = v'_i - \textstyle\sum_{j=1}^{i-1}(e_j^{\mathrm{t}} N v'_i) v_j + \sum_{j=1}^{i-1}(v_j^{\mathrm{t}} N v'_i) e_j.$$

Output the matrix M with columns $e_1, \ldots, e_g, v_1, \ldots, v_g$.

Existence of v'_i as in step 3 follows from the facts that N is invertible and that $e_i \in \mathbf{Z}^{2g}$ is not divisible by integers greater than 1. Actually finding v'_i means finding a solution of a linear equation over $\mathbf{Z}$, which can be done using the LLL-algorithm as in [29, Section 14].

If we apply the Algorithm 5.2 to the matrix N mentioned above it, then the output matrix M is a basis transformation that yields a symplectic basis of Λ with respect to E. For fixed g, Algorithm 5.2 takes time polynomial in the size of the input, hence polynomial time in the bit sizes of $\xi \in K$ and the basis of $\mathfrak{a}$. Lemma 4.15 tells us that for $g = 2$, we can make sure that both $\xi \in K$ and the basis of $\mathfrak{a}$ have a bit size that is polynomial in $\log \Delta$, so obtaining a period matrix Z from a triple $(\Phi, \mathfrak{a}, \xi)$ takes time only polynomial in $\log \Delta$. This implies also that the bit size of Z (as a matrix with entries in a number field) is polynomial in $\log \Delta$.

6. The fundamental domain of the Siegel upper half space

In the genus-1 case, to compute the j-invariant of a point $z \in \mathcal{H} = \mathcal{H}_1$, one should first move z to the *fundamental domain* for $\mathrm{SL}_2(\mathbf{Z})$, or at least away from $\operatorname{Im} z = 0$, to get good convergence. We use the term *fundamental domain* loosely, meaning a connected subset $\mathcal{F}$ of $\mathcal{H}_g$ such that every $\mathrm{Sp}_{2g}(\mathbf{Z})$-orbit has a representative in $\mathcal{F}$, and that this representative is unique, except possibly if it is on the boundary of $\mathcal{F}$.

In genus 2, when computing θ-values at a point $Z \in \mathcal{H}_2$, as we will do in Section 8, we move the point to the fundamental domain for $\mathrm{Sp}_4(\mathbf{Z})$.

We will treat the genus-1 case first, not only because of the analogy, but also because the reduction algorithm for the genus-1 case is part of the reduction algorithm for the genus-2 case.

6.1. **The genus-1 case.** For $g = 1$, the fundamental domain $\mathcal{F} \subset \mathcal{H}$ is the set of $z = x + iy \in \mathcal{H}$ that satisfy

(F1) $-\frac{1}{2} < x \leq \frac{1}{2}$ and
(F2) $|z| \geq 1$.

One usually adds a third condition $x \geq 0$ if $|z| = 1$ in order to make the orbit representatives unique, but we will omit that condition as we allow boundary points of $\mathcal{F}$ to be non-unique in their orbit. To move z into this fundamental domain, we simply iterate the following until $z = x + iy$ is in $\mathcal{F}$:

(6.1)
1. $z \leftarrow z + \lfloor -x + \frac{1}{2} \rfloor$,
2. $z \leftarrow -z^{-1}$ if $|z| < 1$.

We now phrase this procedure in terms of positive definite (2×2)-matrices $Y \in \mathrm{Mat}_2(\mathbf{R})$, which will come in handy in the genus-2 case. We identify such a matrix

$$Y = \begin{pmatrix} y_1 & y_3 \\ y_3 & y_2 \end{pmatrix}$$

with the positive definite binary quadratic form $f = y_1X^2 + 2y_3XY + y_2Y^2 \in \mathbf{R}[X, Y]$. Let ϕ be the map that sends Y to the unique element $z \in \mathcal{H}$ satisfying $f(z, 1) = 0$.

Note that $\mathrm{SL}_2(\mathbf{Z})$ acts on Y via $(U, Y) \mapsto UYU^{\mathrm{t}}$. The map ϕ induces an isomorphism of $\mathrm{SL}_2(\mathbf{Z})$-sets to $\mathcal{H}$ from the set of positive definite (2×2)-matrices $Y \in \mathrm{Mat}_2(\mathbf{R})$ up to scalar multiplication.

Note that $\phi^{-1}(\mathcal{F})$ is the set of matrices Y satisfying

$$-y_1 < 2y_3 \leq y_1 \leq y_2, \tag{6.2}$$

where the first two inequalities correspond to (F1), and the third inequality to (F2). We say that the matrix Y is $\mathrm{SL}_2(\mathbf{Z})$-reduced if it satisfies (6.2).

We phrase and analyze algorithm (6.1) in terms of the matrices Y. Even though we will give some definitions in terms of Y, all inequalities and all steps in the algorithm will depend on Y only up to scalar multiplication.

Algorithm 6.3.
Input: A positive definite symmetric (2×2)-matrix Y_0 over $\mathbf{R}$.
Output: $U \in \mathrm{SL}_2(\mathbf{Z})$ and $Y = UY_0U^{\mathrm{t}}$ such that Y is SL_2-reduced.
Start with $Y = Y_0$ and $U = 1 \in \mathrm{SL}_2(\mathbf{Z})$ and iterate the following two steps until Y is SL_2-reduced.

(1) Let

$$U \leftarrow \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} U \quad \text{and} \quad Y \leftarrow \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} Y \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$$

for $r = \lfloor -y_3/y_1 + \frac{1}{2} \rfloor$.

(2) If $y_1 > y_2$, then let

$$U \leftarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} U \quad \text{and} \quad Y \leftarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Y \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Output U, Y.

We can bound the running time in terms of the *minima* of the matrix Y_0. We define the *first and second minima* $m_1(Y)$ and $m_2(Y)$ of a symmetric positive definite (2×2)-matrix Y as follows. Let $m_1(Y) = p^{\mathrm{t}}Yp$ be minimal among all column vectors $p \in \mathbf{Z}^2$ different from 0 and let $m_2(Y) = q^{\mathrm{t}}Yq$ be minimal among all $q \in \mathbf{Z}^2$ linearly independent of p. Note that the definition of $m_2(Y)$ is independent of the choice of p. We call $m_1(Y)$ also simply the *minimum* of Y. If Y is SL_2-reduced, then we have

$$m_1(Y) = y_1, \quad m_2(Y) = y_2 \quad \text{and} \quad \frac{3}{4}y_1y_2 \leq \det Y \leq y_1y_2,$$

so for every positive definite symmetric matrix Y, we have

$$\frac{3}{4}m_1(Y)m_2(Y) \leq \det Y \leq m_1(Y)m_2(Y). \tag{6.4}$$

As we have

$$Y^{-1} = \frac{1}{\det Y} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Y \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

it also follows that

$$m_i(Y^{-1}) = \frac{m_i(Y)}{\det Y}, \quad (i \in \{1, 2\}). \tag{6.5}$$

For any matrix A, let $|A|$ be the maximum of the absolute values of its entries.

Lemma 6.6. *Algorithm 6.3 is correct and takes $O(\log(|Y_0|/m_1(Y_0)))$ additions, multiplications, and divisions in $\mathbf{R}$. The inequalities*

$$|Y| \leq |Y_0| \quad \text{and} \quad |U| \leq 2(\det Y_0)^{-1/2}\,|Y_0|$$

hold for the output, and also for the values of Y and U throughout the execution of the algorithm.

Proof. This result is well-known. For details, see [36, Lemma II.5.6]. □

6.2. **The fundamental domain.** For genus 2, the *fundamental domain* $\mathcal{F}_2$ is defined to be the set of $Z = X + iY \in \mathcal{H}_2$ for which

(S1) the real part $X = \begin{pmatrix} x_1 & x_3 \\ x_3 & x_2 \end{pmatrix}$ is reduced, i.e., $-\frac{1}{2} \leq x_i < \frac{1}{2}$ $(i = 1, 2, 3)$,
(S2) the imaginary part Y is (GL_2-)reduced, i.e., $0 \leq 2y_3 \leq y_1 \leq y_2$, and
(S3) $|\det M^*(Z)| \geq 1$ for all $M \in \mathrm{Sp}_4(\mathbf{Z})$, where $M^*(Z)$ is defined by

$$M^*(Z) = CZ + D \quad \text{for} \quad M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Every point in $\mathcal{H}_2$ is $\mathrm{Sp}_4(\mathbf{Z})$-equivalent to a point in $\mathcal{F}_2$, and we will compute such a point with Algorithm 6.8 below. This point is unique up to identifications of the boundaries of $\mathcal{F}_2$. We call points $\mathrm{Sp}_4(\mathbf{Z})$-*reduced* if they are in $\mathcal{F}_2$.

Reduction of the real part is trivial and obtained by $X \mapsto X + B$, for a unique $B \in \mathrm{Mat}_2(\mathbf{Z})$. Here $X \mapsto X + B$ corresponds to the action of

$$\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$$

on Z.

Reduction of the imaginary part is reduction of positive definite symmetric matrices as in Algorithm 6.3, but with the extra condition $y_3 \geq 0$, which can be obtained by applying the $\mathrm{GL}_2(\mathbf{Z})$-matrix

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

It follows that UYU^{t} is reduced for some $U \in \mathrm{GL}_2(\mathbf{Z})$, and to reduce the imaginary part of Z, we replace Z by

$$UZU^{\mathrm{t}} = \begin{pmatrix} U & 0 \\ 0 & (U^{\mathrm{t}})^{-1} \end{pmatrix}(Z). \tag{6.7}$$

Condition (S3) has a finite formulation. Let $\mathfrak{G}$ consist of the 38 matrices

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & e_1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & e_1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & d & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & e_1 & e_3 \\ 0 & 1 & e_3 & e_2 \end{pmatrix},$$

in $\mathrm{Sp}_4(\mathbf{Z})$, where d ranges over $\{0, \pm 1, \pm 2\}$ and each e_i over $\{0, \pm 1\}$. Gottschling [21] proved that, under conditions (S1) and (S2), condition (S3) is equivalent to the condition

(G) $|\det M^*(Z)| \geq 1$ for all $M \in \mathfrak{G}$.

Actually, Gottschling went even further and gave a subset of 19 elements of $\mathfrak{G}$ of which he proved that it is minimal such that (G) is equivalent to (S3), assuming (S1) and (S2).

For our purposes of bounding and computing the values of Igusa invariants, it suffices to consider the set $\mathcal{B} \subset \mathcal{H}_2$, given by (S1), (S2), and

(B) $y_1 \geq \sqrt{3/4}$.

Note that the set $\mathcal{B}$ contains $\mathcal{F}_2$. Indeed, condition (B) follows immediately from (S1) and $|z_1| = |\det(N_0^*(Z))| \geq 1$, where N_0 is the first matrix in our defintion of $\mathfrak{G}$.

6.3. **The reduction algorithm.** The reduction algorithm that moves $Z \in \mathcal{H}_2$ into $\mathcal{F}_2$ is as follows.

Algorithm 6.8.
Input: $Z_0 \in \mathcal{H}_2$.
Output: Z in $\mathcal{F}_2$ and a matrix

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$$

such that we have $Z = M(Z_0) = (AZ_0 + B)(CZ_0 + D)^{-1}$.
Start with $Z = Z_0$ and iterate the following 3 steps until Z is in $\mathcal{F}_2$. During the course of the algorithm, keep track of $M \in \mathrm{Sp}_4(\mathbf{Z})$ such that $Z = M(Z_0)$, as we did with U in Algorithm 6.3.

(1) Reduce the imaginary part as explained in Section 6.2.
(2) Reduce the real part as explained in Section 6.2.
(3) Apply N to Z for $N \in \mathfrak{G}$ with $|\det N^*(Z)| < 1$ minimal, if such an N exists.

The algorithm that moves $Z \in \mathcal{H}_2$ into $\mathcal{B}$ is exactly the same, but with $\mathcal{F}_2$ replaced by $\mathcal{B}$ everywhere and with $\mathfrak{G}$ replaced by $\{N_0\}$. We will give an analysis of the running time and output of Algorithm 6.8 below. The only property of the subset $\mathfrak{G} \subset \mathrm{Sp}_4(\mathbf{Z})$ that this analysis uses is that it is finite and contains N_0, hence the analysis is equally valid for the modification that moves points into $\mathcal{B}$.

6.4. **The number of iterations.** We will bound the number of iterations by showing that $\det Y$ is increasing and bounded in terms of Y_0, that every step with $|y_1| < \frac{1}{2}$ leads to a doubling of $\det Y$, and that we have an absolutely bounded number of steps with $|y_1| \geq \frac{1}{2}$.

Lemma 6.9. *For any point $Z \in \mathcal{H}_2$ and any matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$, we have*

$$\det \mathrm{Im}\, M(Z) = \frac{\det \mathrm{Im}\, Z}{|\det M^*(Z)|^2}.$$

Proof. In [27, Proof of Proposition 1.1] it is computed that

$$\mathrm{Im}\, M(Z) = (M^*(Z)^{-1})^{\mathrm{t}} (\mathrm{Im}\, Z) M^*(\overline{Z})^{-1}. \tag{6.10}$$

Taking determinants on both sides proves the result. □

Steps 1 and 2 of Algorithm 6.8 do not change $\det Y$, and Lemma 6.9 shows that step 3 increases $\det Y$, so $\det Y$ is increasing throughout the algorithm.

Lemma 6.11. *At every iteration of step 3 of Algorithm 6.8 in which we have $y_1 < \frac{1}{2}$, the value of $\det Y$ increases by a factor of at least 2.*

Proof. If $y_1 < \frac{1}{2}$, then for the element $N_0 \in \mathfrak{G}$, we have $|\det N_0^*(Z)|^2 = |z_1|^2 = |x_1|^2 + |y_1|^2 \leq \frac{1}{2}$, so by Lemma 6.9, the value of $\det Y$ increases by a factor ≥ 2. □

Lemma 6.12. *There is an absolute upper bound c, independent of the input Z_0, on the number of iterations of Algorithm 6.8 in which Z satisfies $y_1 \geq \frac{1}{2}$ at the beginning of step 3.*

Proof. Let $\mathcal{C}$ be the set of points in $\mathcal{H}_2$ that satisfy (S1), (S2) and $y_1 \geq \frac{1}{2}$. At the beginning of step 3, both (S1) and (S2) hold, so we need to bound the number of iterations for which Z is in $\mathcal{C}$ at the beginning of step 3. Suppose that such an iteration exists, and denote the value of Z at the beginning of step 3 of that iteration by Z'. As $\det Y$ increases during the algorithm, each iteration has a different value of Z, so it suffices to bound the number of $Z \in \mathrm{Sp}_4(\mathbf{Z})(Z') \cap \mathcal{C}$. By [27, Theorem 3.1], the set

$$\mathfrak{C} = \{M \in \mathrm{Sp}_4(\mathbf{Z}) : \mathcal{C} \cap M(\mathcal{C}) \neq \emptyset\}$$

is finite. As $\mathfrak{C}$ surjects onto $\mathrm{Sp}_4(\mathbf{Z})(Z') \cap \mathcal{C}$ via $M \mapsto M(Z')$, we get the absolute upper bound $\#\mathfrak{C}$ on the number of iterations with $Z \in \mathcal{C}$. □

We can now bound the number of iterations. For any matrix $Z = X + iY \in \mathcal{H}_2$, let $t(Z) = \log \max\{m_1(Y)^{-1}, m_2(Y)\}$.

Proposition 6.13. *The number of iterations of Algorithm 6.8 is at most $O(t(Z_0))$ for every input Z_0.*

Proof. Let c be the constant of Lemma 6.12, let Z_0 be the input of Algorithm 6.8 and let Z be the value after k iterations. By Lemmas 6.11 and 6.14, we have

$$2^{k-c} \det Y_0 \leq \det Y \leq m_2(Y)^2 \leq (\frac{4}{3})^2 \max\{m_1(Y_0)^{-2}, m_2(Y_0)^2\},$$

hence (6.4) implies

$$2^{k-c} \leq (\frac{4}{3})^3 \max\{m_1(Y_0)^{-3} m_2(Y_0)^{-1}, m_1(Y_0)^{-1} m_2(Y_0)\}.$$ □

To avoid a laborious error analysis, all computations are performed inside some number field $L \subset \mathbf{C}$ of absolutely bounded degree. Indeed, for an abelian surface A with CM by $\mathcal{O}_K$, any period matrix $Z \in \mathcal{H}_2$ that represents A is in $\mathrm{Mat}_2(L)$, where L is the normal closure of K, which has degree at most 8. For a running time analysis, we need to bound the *height* of the numbers involved. Such height bounds are also used for lower bounds on the off-diagonal part of the output Z, which we will need in Section 8.

The height $h(x)$ of an element $x \in L^*$ is defined as follows. Let S be the set of absolute values of L that extend either the standard archimedean absolute value of $\mathbf{Q}$ or one of the non-archimedean absolute values $|x| = p^{-\mathrm{ord}_p(x)}$. For each $v \in S$, let $\deg(v) = [L_v : \mathbf{Q}_v]$ be the degree of the completion L_v of L at v. Then

$$h(x) = \sum_v \deg(v) \max\{\log |x|_v, 1\}.$$

We denote the maximum of the heights of all entries of a matrix $Z \in \mathcal{H}_2$ by $h(Z)$.

6.5. **The size of the numbers.** Next, we give bounds on the value of $|M|$ during the execution of the algorithm. This will provide us with a bound on the height of the entries of Z. Indeed, if we have $Z = M(Z_0)$, then it follows that $h(Z) \leq 16(\log |M| + h(Z_0) + \log 4)$. The following result allows us to bound $m_2(Y)$ and $\det Y$ from above during the algorithm, which we need to do in order to bound the size of the numbers encountered.

Lemma 6.14. *For any point $Z = X + iY \in \mathcal{H}_2$ and any matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$, we have*

$$m_2(\mathrm{Im}\, M(Z)) \leq \frac{4}{3} \max\{m_1(Y)^{-1}, m_2(Y)\}.$$

Proof. We imitate part of the proof of [27, Lemma 3.1]. If we replace M by

$$\begin{pmatrix} (U^{\mathrm{t}})^{-1} & 0 \\ 0 & U \end{pmatrix} M$$

for $U \in \mathrm{GL}_2(\mathbf{Z})$, then the matrix $(\operatorname{Im} M(Z))^{-1}$ gets replaced by the matrix $U(\operatorname{Im} M(Z))^{-1}U^{\mathrm{t}}$, so we can assume without loss of generality that $(\operatorname{Im} M(Z))^{-1}$ is reduced. By (6.10), we have

$$\begin{aligned} (\operatorname{Im} M(Z))^{-1} &= (CX - iCY + D)Y^{-1}(CX + iCY + D)^{\mathrm{t}} \\ &= (CX + D)Y^{-1}(XC^{\mathrm{t}} + D^{\mathrm{t}}) + CYC^{\mathrm{t}}, \\ \text{where} \quad M &= \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \end{aligned} \tag{6.15}$$

As the left hand side of (6.15) is reduced, its minimum m_1 is its upper left entry. Denote the third row of M by (c_1, c_2, d_1, d_2) and let $c = (c_1, c_2)$, $d = (d_1, d_2) \in \mathbf{Z}^2$. We compute that the upper left entry of (6.15) is $m_1((\operatorname{Im} M(Z))^{-1}) = (cX + d)Y^{-1}(Xc^{\mathrm{t}} + d^{\mathrm{t}}) + cYc^{\mathrm{t}}$.

The matrix M is invertible, so if c is zero, then d is non-zero. As both Y^{-1} and Y are positive definite, this implies that

$$m_1((\operatorname{Im} M(Z))^{-1}) \geq \min\{m_1(Y), m_1(Y^{-1})\}.$$

By (6.4) and (6.5), we get

$$\begin{aligned} m_2(\operatorname{Im} M(Z)) &\leq \frac{4 \det \operatorname{Im} M(Z)}{3m_1(\operatorname{Im} M(Z))} = \frac{4}{3m_1((\operatorname{Im} M(Z))^{-1})} \\ &\leq \frac{4}{3} \max\{\frac{1}{m_1(Y)}, \frac{\det Y}{m_1(Y)}\} \\ &\leq \frac{4}{3} \max\{m_1(Y)^{-1}, m_2(Y)\}, \end{aligned}$$

which proves the result. □

Lemma 6.16. *There exists an absolute constant $c > 0$ such that the following holds. The value of $\log|M|$ is at most $c\max\{\log|Z_0|, 1\}$ during the first iteration of Algorithm 6.8 and, in each iteration, increases by at most $c\max\{t(Z_0), 1\}$, where t is as above Proposition 6.13.*

Proof. For step 1, it follows from equation (6.7) and Lemma 6.6 that the value of $\log|M|$ increases by at most $\log|Z| + t(Z) + \log 8$. In step 2, the value of $\log|M|$ increases by at most $\log(1 + 2|Z|)$. In step 3, the value of $\log|M|$ increases by at most $\log 4$ by the definition of $\mathfrak{G}$.

Therefore, it suffices to bound $\log|Z|$ appropriately at the beginning of steps 1 and 2. Note that $\log|Y|$ decreases during step 1, while $\log|X|$ increases by at most $\max\{\log|Z|, 0\} + \log 16$. Therefore, it suffices to give a bound for $\log|Z|$ only at the beginning of step 1. Note that for the first iteration, the bound $\log|Z| = \log|Z_0|$ suffices.

At the beginning of step 3, we have $|x_i| \leq \frac{1}{2}$, and Y is reduced. We can thus use Lemma 6.14 to bound the coefficients of Y, and get $|Y| \leq 4e^{t(Z_0)}/3$. This proves that we have $\log|Z| \leq 3\max\{t(Z_0), 1\}$. During step 3, the matrix Z gets replaced by

$$\begin{aligned} N(Z) &= (AZ + B)(CZ + D)^{-1} \\ &= \tfrac{1}{\det(CZ+D)}(AZ + B)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(CZ + D)\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \end{aligned}$$

where

$$N = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is in the set $\mathfrak{G}$. We have $|N(Z)| \leq |\det(CZ+D)|^{-1} (2|Z|+1)^2 |N|^2$. We have already bounded $|Z|$, and we also have $|N| \leq 4$, so we only need to bound $|\det(CZ+D)|^{-1}$. Lemma 6.9 gives

$$|\det(CZ+D)|^{-2} = (\det \operatorname{Im} N(Z))(\det \operatorname{Im}(Z))^{-1}.$$

Let M' be such that we have $Z = M'(Z_0)$ and let $M = NM'$, then Lemma 6.14 tells us that the numerator is at most

$$4 \max\{m_1(Y_0)^{-1}, m_2(Y_0)\}/3.$$

Applying the fact that the determinant of $\operatorname{Im}(Z)$ increases during the execution of the algorithm, we thus find

$$|\det(CZ+D)|^{-2} = 4 \max\{m_1(Y_0)^{-1}, m_2(Y_0)\}/(3 \det \operatorname{Im}(Z_0)),$$

which is at most $16/9 \max\{m_1(Y_0), m_2(Y_0)\}^3$ by (6.4). Therefore, for Z and N as in step 3, we have $\log|N(Z)| = c' \max\{t(Z_0), 1\}$, hence we find that $c' \max\{t(Z_0), 1\}$ is an upper bound for $\log|Z|$ at the beginning of step 1 for every iteration but the first. □

6.6. **The running time.**

Theorem 6.17. *Let $L \subset \mathbf{C}$ be a number field. Algorithm 6.8, on input $Z_0 \in \operatorname{Mat}_2(L) \cap \mathcal{H}_2$, returns an $\operatorname{Sp}_4(\mathbf{Z})$-equivalent matrix $Z \in \mathcal{F}_2$. The running time is $\widetilde{O}(h(Z_0) \log|Z_0|) + \widetilde{O}(t(Z_0)^4)$. Moreover, the output Z satisfies*

$$h(Z) = c' \max\{h(Z_0), t(Z_0)^2, 1\},$$

for some absolute constant c'.

Proof. By Proposition 6.13 and Lemma 6.16, the value of $\log|M|$ is bounded by $O(\log|Z_0|) + O(t(Z_0)^2)$ throughout the algorithm, so the height of every entry of Z is bounded by $O(t(Z_0)^2) + O(h(Z_0))$. This implies that each basic arithmetic operation in the algorithm takes time at most $\widetilde{O}(t(Z_0)^2) + \widetilde{O}(h(Z_0))$. By Lemma 6.6, the first iteration takes $O(\log|Z_0|) + O(t(Z_0))$ such operations, and all other $O(t(Z_0))$ iterations take $O(t(Z_0))$ operations, so there are $O(\log|Z_0|) + O(t(Z_0)^2)$ arithmetic operations, yielding a total running time for the algorithm of $\widetilde{O}(t(Z_0)^4) + \widetilde{O}(h(Z_0) \log|Z_0|)$ □

In Section 8, we bound the Igusa invariants in terms of the entries of the period matrix Z. One of the bounds that we need in that section is a lower bound on the absolute value of the off-diagonal entry z_3 of Z. It is supplied by the following corollary.

Corollary 6.18. Let $Z_0 \in \operatorname{Mat}_2(L) \cap \mathcal{H}_2$ be the input of Algorithm 6.8 and let z_3 be the off-diagonal entry of the output. Then we have either $z_3 = 0$ or $-\log|z_3| \leq c' \max\{h(Z_0), t(Z_0)^2, 1\}$ for an absolute constant c'.

Proof. The field L is a subfield of $\mathbf{C}$, which gives us a standard absolute value v. If z_3 is non-zero, then the product formula tells us that we have $-\log|z_3| = -\log|z_3|_v = \sum_{w \neq v} \log|z_3|_w \leq h(z_3)$, which is at most $c' \max\{h(Z_0), t(Z_0)^2, 1\}$ by Theorem 6.17. □

7. Bounding the period matrices

In this section, we prove the following result. Here, the set $\mathcal{B} \subset \mathcal{H}_2$ is as defined in Section 6.2, and contains the fundamental domain $\mathcal{F}_2$.

Theorem 7.1. *Let $Z \in \mathcal{B}$ be such that the principally polarized abelian variety corresponding to it has complex multiplication by $\mathcal{O}_K$. Then we have $m_2(\operatorname{Im} Z) \leq \frac{2}{3\sqrt{3}} \max\{2\Delta_0, \Delta_1^{1/2}\}$, where Δ_0 is the discriminant of the real quadratic subfield $K_0 \subset K$, and Δ_1 is the norm of the relative discriminant of K/K_0.*

Let $\mathfrak{a}$ and $\Phi = \{\phi_1, \phi_2\}$ be an ideal and CM-type of K corresponding to Z as in Section 4.1. Let e, f, v, $w \in K$ be a symplectic basis of $\mathfrak{a}$ giving rise to Z as in Section 5.2. By scaling, we may assume $v = 1$. Write $w_k = \phi_k(w)$ for $k = 1, 2$.

Lemma 7.2. *We have*

$$|\det \operatorname{Im} Z| = |w_1 - w_2|^{-2} \operatorname{covol}(\Phi(\mathfrak{a})) \quad \textit{and} \quad \operatorname{covol}(\Phi(\mathfrak{a})) = \frac{1}{4} N(\mathfrak{a}) \Delta^{1/2} \leq \frac{1}{4} \Delta^{1/2}$$

Proof. Let $\varphi : \mathbf{C}^2 \to \mathbf{C}^2$ be the $\mathbf{C}$-linear map sending $(1, 0)$ to $(1, 1) = \Phi(1)$ and $(0, 1)$ to $(w_1, w_2) = \Phi(w)$, so $\varphi(Z\mathbf{Z}^2 + \mathbf{Z}^2) = \Phi(\mathfrak{a})$. As an $\mathbf{R}$-linear map, it has determinant $|w_1 - w_2|^2$. We find

$$|\det \operatorname{Im} Z| = \operatorname{covol}(Z\mathbf{Z}^2 + \mathbf{Z}^2) = |w_1 - w_2|^{-2} \operatorname{covol}(\Phi(\mathfrak{a})).$$

Moreover, we have $\operatorname{covol}(\Phi(\mathfrak{a})) = N(\mathfrak{a})^{-1} \operatorname{covol}(\Phi(\mathcal{O}_K))$, where $\operatorname{covol}(\Phi(\mathcal{O}_K)) = \frac{1}{4}\Delta^{1/2}$. Finally, our assumption $v = 1$ implies that $\mathfrak{a}^{-1}$ is an integral ideal, so $N(\mathfrak{a}) \leq 1$. □

Lemma 7.3. *Suppose $w \notin K_0$. Then we have $|\det \operatorname{Im} Z| < \frac{1}{2}\Delta_0$.*

Proof. Write $w_k = x_k + iy_k$ and let ξ be as in Section 4.1. We have $\operatorname{Tr}_{K/\mathbf{Q}}(\xi w) = E(\Phi(w), \Phi(1)) = 0$ as $(e, f, 1, w)$ is a symplectic basis. Write $\phi_k(\xi) = i\nu_k$, so ν_k is a positive real number. We get $0 = 2(\nu_1 y_1 + \nu_2 y_2)$, so $y_2 = -\frac{\nu_1}{\nu_2} y_1$. In particular, we have $|w_1 - w_2| \geq |y_1 - y_2| = |y_1|(1 + \frac{\nu_1}{\nu_2})$. Analogously, we have $|w_1 - w_2| \geq |y_2 - y_1| = |y_2|(1 + \frac{\nu_2}{\nu_1})$. Taking the product of these identities yields $|w_1 - w_2|^2 \geq |y_1 y_2|(2 + \frac{\nu_1^2 + \nu_2^2}{\nu_1 \nu_2}) > 2|y_1 y_2|$.

On the other hand, $\mathfrak{a}$ contains $\mathcal{O}_{K_0} + w\mathcal{O}_{K_0}$, which has covolume $\Delta_0 |y_1 y_2|$. We get our result by inserting these values into the first equality of Lemma 7.2. □

Write $Z = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix}$ and $z_k = x_k + iy_k$.

Lemma 7.4. *Suppose $w \in K_0$ and write $\mathfrak{b} = \mathbf{Z} + w\mathbf{Z}$. Then we have*

$$|\det \operatorname{Im} Z| = \frac{1}{4} N_{K/\mathbf{Q}}(\mathfrak{a}^{-1}\mathfrak{b})^{-1} \Delta_1^{1/2} \leq \frac{1}{4} \Delta_1^{1/2},$$

where $N_{K/\mathbf{Q}}(\mathfrak{a}^{-1}\mathfrak{b})$ is an integer.

Proof. Note that $\mathfrak{b} = (K_0 \cap \mathfrak{a})$ is an $\mathcal{O}_{K_0}$-ideal and that we have $\mathfrak{a} \supset \mathcal{O}_K \mathfrak{b}$. We compute

$$N_{K/\mathbf{Q}}(\mathfrak{a}) = N_{K_0/\mathbf{Q}}(\mathfrak{b})^2 N_{K/\mathbf{Q}}(\mathfrak{a}\mathfrak{b}^{-1}) = |w_1 - w_2|^2 \Delta_0^{-1} N_{K/\mathbf{Q}}(\mathfrak{a}^{-1}\mathfrak{b})^{-1}.$$

We find the result by inserting this into the second equality of Lemma 7.2. □

Proof of Theorem 7.1. Equations (6.4) and (B) of Section 6 give $m_2(\operatorname{Im} Z) \leq \frac{4\sqrt{4}}{3\sqrt{3}} \det \operatorname{Im} Z$, hence Lemmas 7.3 and 7.4 prove the result. □

Remark 7.5. The bound of Theorem 7.1 is not optimal. For example, Corollary II.6.2 of the author's thesis [36] improves it to $\max\{\frac{2\sqrt{2}}{\sqrt{3}\pi}\Delta_0, \frac{4}{9}\Delta_1^{1/4}\Delta_0^{1/2}\}$ using the *Hilbert* upper half space and multiple pages of computations. However, we will be satisfied with Theorem 7.1, as it is easier to prove and not the bottleneck of our running time analysis.

8. Theta constants

To compute the absolute Igusa invariants corresponding to a point $Z \in \mathcal{H}_2$, we use *theta constants*, also known as *theta null values*. For $z \in \mathbf{C}$, let $e(z) = e^{2\pi i z}$. We call an element $c \in \{0, \frac{1}{2}\}^4$ a *theta characteristic* and write $c = (c_1, c_2, c_3, c_4)$, $c' = (c_1, c_2)$ and $c'' = (c_3, c_4)$. We define the *theta constant of characteristic* c to be the function $\theta[c] : \mathcal{H}_2 \to \mathbf{C}$ given by

$$\theta[c](Z) = \sum_{n \in \mathbf{Z}^2} e(\frac{1}{2}(n + c')Z(n + c')^{\mathrm{t}} + (n + c')c''^{\mathrm{t}}),$$

and following Dupont [11], we use the short-hand notation

$$\theta_{16c_2+8c_1+4c_4+2c_3} = \theta[c].$$

We call a theta characteristic — and the corresponding theta constant — even or odd depending on whether $4c'c''^{\mathrm{t}}$ is even or odd. The odd theta constants are zero by the anti-symmetry in the definition, and there are exactly 10 even theta constants $\theta_0, \theta_1, \theta_2, \theta_3, \theta_4, \theta_6, \theta_8, \theta_9, \theta_{12}$ and θ_{15}.

8.1. **Igusa invariants in terms of theta constants.** Let T be the set of even theta characteristics and define

$$S = \{C \subset T \mid \#C = 4, \sum_{c \in C} c \in \mathbf{Z}^4\}.$$

Then S consists of 15 subsets of T called *Göpel quadruples*, each consisting of 4 even theta characteristics. We call a set $\{b, c, d\} \subset T$ of three distinct even theta characteristics *syzygous* if it is a subset of a Göpel quadruple, so there are 60 syzygous triples. Define

$$h_4 = \sum_{c \in T} \theta[c]^8, \qquad h_6 = \sum_{\substack{b,c,d \in T \\ \text{syzygous}}} \pm(\theta[b]\theta[c]\theta[d])^4 \tag{8.1}$$

$$h_{10} = \prod_{c \in T} \theta[c]^2, \qquad h_{12} = \sum_{C \in S} \prod_{c \in T \setminus C} \theta[c]^4,$$

where we explain the signs in h_6 below. Each h_k is a sum of t_k monomials of degree $2k$ in the 10 even theta constants, where $t_4 = 10$, $t_6 = 60$, $t_{10} = 1$, and $t_{12} = 15$. The signs in h_6 are defined uniquely by the facts that h_6 is a modular form for $\mathrm{Sp}_4(\mathbf{Z})$ and that the coefficient of $\theta_0^4\theta_1^4\theta_2^4$ is $+1$. More explicitly, we give h_6 in Figure 1.

$$\begin{aligned}
&t0{*}t1{*}t2 + t0{*}t1{*}t3 + t0{*}t2{*}t3 + t1{*}t2{*}t3 - t0{*}t2{*}t4 + t1{*}t3{*}t4 - t0{*}t2{*}t6 \\
&+t1{*}t3{*}t6 - t0{*}t4{*}t6 - t1{*}t4{*}t6 - t2{*}t4{*}t6 - t3{*}t4{*}t6 - t0{*}t1{*}t8 + t2{*}t3{*}t8 \\
&+t0{*}t4{*}t8 + t3{*}t4{*}t8 - t1{*}t6{*}t8 - t2{*}t6{*}t8 - t0{*}t1{*}t9 + t2{*}t3{*}t9 - t1{*}t4{*}t9 \\
&-t2{*}t4{*}t9 + t0{*}t6{*}t9 + t3{*}t6{*}t9 - t0{*}t8{*}t9 - t1{*}t8{*}t9 - t2{*}t8{*}t9 - t3{*}t8{*}t9 \\
&+t1{*}t2{*}t12 - t0{*}t3{*}t12 + t0{*}t4{*}t12 + t1{*}t4{*}t12 - t2{*}t6{*}t12 - t3{*}t6{*}t12 \\
&+t0{*}t8{*}t12 + t2{*}t8{*}t12 + t4{*}t8{*}t12 + t6{*}t8{*}t12 - t1{*}t9{*}t12 - t3{*}t9{*}t12 \\
&+t4{*}t9{*}t12 + t6{*}t9{*}t12 + t1{*}t2{*}t15 - t0{*}t3{*}t15 - t2{*}t4{*}t15 - t3{*}t4{*}t15 \\
&+t0{*}t6{*}t15 + t1{*}t6{*}t15 - t1{*}t8{*}t15 - t3{*}t8{*}t15 + t4{*}t8{*}t15 + t6{*}t8{*}t15 \\
&+t0{*}t9{*}t15 + t2{*}t9{*}t15 + t4{*}t9{*}t15 + t6{*}t9{*}t15 - t0{*}t12{*}t15 - t1{*}t12{*}t15 \\
&-t2{*}t12{*}t15 - t3{*}t12{*}t15
\end{aligned}$$

Figure 1. An explicitly written out version of h_6 (see (8.1)). We write tj instead of θ_j^4 for ease of copying with a computer.

Remark 8.2. Another way of defining h_k is by letting ψ_k be the Eistenstein series of weight k on $\mathcal{H}_2$ and setting $h_4 = 2^2\psi_4$, $h_6 = 2^2\psi_6$,

$$h_{10} = -2^{14}\chi_{10} \quad \text{for} \quad \chi_{10} = -43867(2^{12}3^5 5^2 7 \cdot 53)^{-1}(\psi_4\psi_6 - \psi_{10}), \quad \text{and}$$
$$h_{12} = 2^{17}3\chi_{12} \quad \text{for} \quad \chi_{12} = 131 \cdot 593(2^{13}3^7 5^3 7^2 337)^{-1}(3^2 7^2 \psi_4^3 + 2 \cdot 5^3\psi_6^2 - 691\psi_{12}).$$

See also Igusa [24, p. 189] and [25, p. 848].

Lemma 8.3. *Let Z be a point in $\mathcal{H}_2$. If $h_{10}(Z)$ is non-zero, then the principally polarized abelian variety corresponding to Z is the Jacobian of a curve $C/\mathbf{C}$ of genus 2 with invariants*

$$I_2(C) = h_{12}(Z)/h_{10}(Z), \qquad I_4(C) = h_4(Z),$$
$$I_6'(C) = h_6(Z), \qquad I_{10}(C) = h_{10}(Z).$$

Proof. This is the result on page 848 of Igusa [25]. □

Remark 8.4. Thomae's formula ([32, Thm. IIIa.8.1], [37]) gives an equation for a curve C with $J(C)$ corresponding to Z in terms of the theta constants. Formulas of the form of Lemma 8.3 can be derived by writing out the definition of I_k using Thomae's formula and standard identities between the theta constants. This was done by Bolza [3], and also by Spallek [35]. Spallek did not give h_6, but instead gave an explicitly written out version of h_4, h_{10}, h_{12}, and

$$h_{16} = \sum_{\substack{C \in S \\ d \in C}} \theta[d]^8 \prod_{c \in T \setminus C} \theta[c]^4,$$

filling a full page, together with the formulas for I_2, I_4, I_{10} of Lemma 8.3 and the formula

$$I_6(C) = h_{16}(Z)/h_{10}(Z).$$

The same page-filling formulas later appeared in [43] and [16].

Remark 8.5. Our invariants i_1, i_2, and i_3 are chosen to have the minimal number of factors h_{10} in the denominator. The bounds in Corollaries 8.8 and 8.9 below are part of the motivation for this choice. This choice is also good for the denominators, as we will see in Remark 10.3.

Corollary 8.6. Each element of the ring $A = \mathbf{Q}[I_2, I_4, I_6', I_{10}^{-1}]$ can be expressed as a polynomial in the theta constants divided by a power of the product of all even theta constants. □

By Corollary 8.6, if we give upper and lower bounds on the absolute values of the theta constants, then we get upper bounds on the absolute values of the absolute Igusa invariants. Furthermore, we can bound the precision needed for the theta constants in terms of the precision needed for the absolute invariants.

8.2. **Bounds on the theta constants.** For $Z \in \mathcal{H}_2$, denote the real part of Z by X and the imaginary part by Y, write Z as

$$Z = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix},$$

and let x_j be the real part of z_j and y_j the imaginary part for $j = 1, 2, 3$. Recall that $\mathcal{B} \subset \mathcal{H}_2$ is given by

(S1) X is reduced, i.e., $-1/2 \le x_i < 1/2$ for $i = 1, 2, 3$,
(S2) Y is reduced, i.e., $0 \le 2y_3 \le y_1 \le y_2$, and
(B) $y_1 \ge \sqrt{3/4}$.

Proposition 8.7. *For every $Z \in \mathcal{B}$, we have*

$$\begin{aligned} |\theta_j(Z) - 1| &< 0.405 && j \in \{0,1,2,3\} \\ \left|\frac{\theta_j(Z)}{2e(\frac{1}{8}z_1)} - 1\right| &< 0.348 && j \in \{4,6\} \\ \left|\frac{\theta_j(Z)}{2e(\frac{1}{8}z_2)} - 1\right| &< 0.348 && j \in \{8,9\} \quad \textit{and} \\ \left|\frac{\theta_j(Z)}{2((-1)^j + e(\frac{1}{2}z_3))e(\frac{1}{8}(z_1+z_2-2z_3))} - 1\right| &< 0.438 && j \in \{12,15\}. \end{aligned}$$

Proof. The proof of Proposition 9.2 of Klingen [27] gives infinite series as upper bounds for the left hand sides. A numerical inspection shows that the limits of these series are less than 0.553, 0.623, 0.623 and 0.438. Klingen's bounds can be improved by estimating more terms of the theta constants individually and thus getting a smaller error term. This has been done in Propositions 6.1 through 6.3 of Dupont [11], improving the first three bounds to 0.405, $2\,|e(z_1/4)| \leq 0.514$ and $2\,|e(z_2/4)| \leq 0.514$. The proof of [11, Proposition 6.2] shows that for the second and third bound, we can also take 0.348. □

Corollary 8.8. For every $Z \in \mathcal{B}$, we have

$$\begin{aligned} |\theta_j(Z)| &< 1.41, \quad (j \in \{0,1,2,3\}) \\ |\theta_j(Z)| &< 1.37, \quad (j \in \{4,6,8,9\}) \\ |\theta_j(Z)| &< 1.56. \quad (j \in \{12,15\}) \end{aligned}$$

Proof. These upper bounds follow immediately from (S2), (B), and Proposition 8.7. □

Corollary 8.9. For every $Z \in \mathcal{B}$, we have

$$\begin{aligned} 0.59 &< |\theta_j(Z)|, && (j \in \{0,1,2,3\}) \\ 1.3\ \exp(-\tfrac{\pi}{4}y_1) &< |\theta_j(Z)|, && (j \in \{4,6\}) \\ 1.3\ \exp(-\tfrac{\pi}{4}y_2) &< |\theta_j(Z)|, && (j \in \{8,9\}) \\ 1.05\ \exp(-\tfrac{\pi}{4}(y_1+y_2-2y_3)) &< |\theta_{12}(Z)|, && \text{and} \\ 1.12\ \exp(-\tfrac{\pi}{4}(y_1+y_2-2y_3))\nu &< |\theta_{15}(Z)|, \end{aligned}$$

where $\nu = \min\{\frac{1}{4}, |z_3|\}$.

Proof. This follows from Proposition 8.7 if we use $|1 - e(z_3/2)| \geq \nu$ and the bounds

$$|1 + e(z_3/2)| > 1, \quad \exp(-\frac{\pi}{4}y_i) \geq 0.506 \quad (i \in \{1,2\}) \quad \text{and}$$

$$\exp\left(-\frac{\pi}{4}(y_1 + y_2 - 2\,|y_3|)\right) > \exp\left(-\frac{\pi}{2}y_2\right) \geq 0.256.$$ □

Theorem 8.10. *For every $Z \in \mathcal{B}$ and $n \in \{1,2,3\}$, we have*

$$\log_2 |i_n(Z)| < 2\pi(y_1 + y_2 - y_3) + 64 + 2\max\{2, -\log_2 |z_3|\}.$$

Proof. Corollary 8.8 yields bounds $\log_2 |h_4(Z)| < 8$, $\log_2 |h_6(Z)| < 13$, $\log_2 |h_{10}(Z)| < 11$ and $\log_2 |h_{12}(Z)| < 17$. On the other hand, Corollary 8.9 yields

$$-\log_2 |h_{10}(Z)| < \pi(y_1 + y_2 - y_3) + 3 + \max\{2, -\log_2 |z_3|\}.$$

The upper bounds on i_n follow from the formulas of Lemma 8.3 and the bounds on h_k. □

Remark 8.11. Lemma 8.3, together with Theorem 8.10, gives a constructive version of (Weil's) Theorem 3.2. Indeed, if $z_3 = 0$, then the principally polarized abelian surface $A(Z)$ corresponding to Z is the product of the polarized elliptic curves $\mathbf{C}/(z_1\mathbf{Z}+\mathbf{Z})$ and $\mathbf{C}/(z_2\mathbf{Z}+\mathbf{Z})$, while if $z_3 \neq 0$, then Theorem 8.10 shows that we have $h_{10}(Z) \neq 0$, so $A(Z)$ is the Jacobian of the curve of genus 2 given by Lemma 8.3.

8.3. **Evaluating theta constants and Igusa invariants.** We use the naive way of evaluating theta constants. That is, we simply sum all terms in the definition of θ for with $|n_i|$ below a certain bound R. The analysis of the terms that are left out, and of the rounding errors, is straightforward and easy. Suppose we want an error $\leq 2^{-s}$. As the logarithm of the absolute value of a term decreases quadratically with n, the bound R needs only to grow linearly with the square root of s. We find that the number of terms, as well as the complexity of computing and summing these terms via fast multiplication, is quasi-linear in s (i.e., $\widetilde{O}(s)$).

Making this explicit (see [36] for details), we get the following result. For s a positive integer, let

$$R = \lceil (0.4s + 2.2)^{1/2} \rceil \quad \text{and} \quad t = s + 2 + \lfloor 2\log_2(2R+1) \rfloor,$$

so $t/s \to 1$ as $s \to \infty$.

Theorem 8.12. *There exists an algorithm with the following input and output that has running time $\widetilde{O}(s^2)$. Input: $j \in \{0, \ldots, 15\}$, a positive integer s, and a matrix $\widetilde{Z} \in \mathcal{B}$ with $|\widetilde{Z} - Z| < 2^{-t}$ for some $Z \in \mathcal{H}_2$. Output: a complex number A with $|A - \theta_j(Z)| < 2^{-s}$.* □

Remark 8.13. Note that this running time is quasi-quadratic, while Dupont's (generalized AGM-)method [11, Section 10.2] is heuristically quasi-linear. Proving correctness of Dupont's method, and analysing the required precision and the running time, is beyond the scope of this article.

After computing approximations of the theta constants, approximating the absolute Igusa invariants is straightforward: they are polynomials in the theta constants divided by the product of the theta constants. The absolute values of the theta constants and the errors of their approximations can then be used to bound the precision loss and hence tell us how much precision to use. For details and explicit bounds, see Section II.7.3 of the author's thesis [36].

9. The degree of the class polynomials

Let K be a primitive quartic CM-field. In this section we give asymptotic upper and lower bounds on the degree of Igusa class polynomials of K. These bounds are not used in the algorithm itself, but are used in the analysis of the algorithm.

Denote the class numbers of K and K_0 by h and h_0 respectively, and let $h_1 = h/h_0$. The degree of the Igusa class polynomials $H_{K,n}$ for $n = 1, 2, 3$ is the number h' of isomorphism classes of curves of genus 2 with CM by $\mathcal{O}_K$. By Lemma 4.14 we have $h' = h_1$ if K is cyclic and $h' = 2h_1$ otherwise. The degree of the polynomials $\widehat{H}_{K,n}$ is $h'-1$. The following result gives an asymptotic bound on h_1, and hence on the degree h'.

Lemma 9.1 (Louboutin [30])**.** *There exist effective constants $d > 0$ and N such that for all primitive quartic CM-fields K with $\Delta > N$, we have*

$$\Delta_1^{1/2}\Delta_0^{1/2}(\log\Delta)^{-d} \leq h_1 \leq \Delta_1^{1/2}\Delta_0^{1/2}(\log\Delta)^{d}.$$

Proof. Louboutin [30, Theorem 14] gives bounds

$$\left| \frac{\log h_1}{\log(\Delta_1\Delta_0)} - \frac{1}{2} \right| \leq d\frac{\log\log\Delta}{\log\Delta}$$

for $\Delta > N$. As we have $\Delta > \Delta_0\Delta_1$, this proves the result. □

10. Denominators

Let K be a primitive quartic CM-field. In this section we give upper bounds on the denominators of the Igusa class polynomials of K. By the *denominator* of a polynomial $f \in \mathbf{Q}[X]$, we mean the smallest positive integer c such that cf is in $\mathbf{Z}[X]$.

10.1. **Background.** A prime p occurs in the denominator of H_1 only if there is a curve C with CM by $\mathcal{O}_K$ such that C has *bad reduction* at a prime $\mathfrak{p}$ over p. It is known that abelian varieties with complex multiplication have potential *good* reduction at all primes, but this doesn't imply that Jacobians reduce as Jacobians: the reduction of the Jacobian of a smooth curve C of genus two can be a polarized product of elliptic curves $E_1 \times E_2$. The reduction of C is then the union of those elliptic curves intersecting transversely. For details, we refer to Goren and Lauter [19, 20], who study this phenomenon and use the embedding

$$\mathcal{O}_K \to \mathrm{End}(E_1 \times E_2)$$

to bound both p and the valuation of the denominator of H_1 at p.

We use the bounds of Goren and Lauter which hold in general, but are expected to be far from asymptotically optimal, in our running time analysis. The bounds of Bruinier and Yang [4, 44] are better, but are proven only for very special quartic CM-fields.

10.2. **Statement of the results.** Goren and Lauter [19, 20] give their bounds in terms of integers a, b, d such that K is given by $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$. For d, one can take the discriminant $d = \Delta_0$ of the real quadratic subfield K_0. We will prove in Lemma 10.9 below that one can take $a < 8\pi^{-1}(\Delta_1\Delta_0)^{1/2}$, where $\Delta_1 = N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$ is the norm of the relative discriminant. The denominator itself does not depend on the choice of a, so we can replace a by this bound on a in all denominator bounds below.

The main result of this section is the following.

Theorem 10.1. *Let K be a primitive quartic CM-field and write*

$$K = \mathbf{Q}\Big(\sqrt{-a+b\sqrt{d}}\Big) \quad \textit{with} \quad a,b,d \in \mathbf{Z}.$$

The denominator of each of the Igusa class polynomials of K divides $2^{14h'}D^2$ for

$$D = \left(\prod_{\substack{p < 4da^2 \\ p \text{ prime}}} p^{\lfloor 4f(p)(1+\log(2da^2)/\log p)\rfloor} \right)^{h'},$$

where $f(p)$ is given by $f(p) = 8$ if p ramifies in $K/\mathbf{Q}$ and satisfies $p \leq 3$, and given by $f(p) = 1$ otherwise.

Furthermore, the result above remains true if we replace d by Δ_0 and a by $\lfloor 8\pi^{-1}(\Delta_1\Delta_0)^{1/2}\rfloor$ in the definition of D. We then have $\log D = \widetilde{O}(h'\Delta) = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ as Δ tends to infinity.

We will prove this result below.

Remark 10.2. Theorem 10.1 as stated holds for the absolute Igusa invariants i_1, i_2, i_3 of Section 2. For another choice of a set S of absolute Igusa invariants, take positive integers c_3 and k such that $c_3(2^{-12}I_{10})^k S$ consists of modular forms of degree k with integral Fourier expansion. Then the denominator divides $c_3^{h'}D^k$. See the proof of Theorem 10.1 below for details.

Using the formulas for the Igusa invariants of Lemma 8.3, one can verify that all elements of $\mathbf{Z}[2^{-15}I_2I_{10}, 2^{-2}I_4, 2^{-2}I_6', 2^{-12}I_{10}]$ have an integral Fourier expansion (see [36, Appendix 1]). For our invariants, we have $c_3 = 2^{14}$ and $k = 2$.

Remark 10.3. Our invariants i_1, i_2, and i_3 are chosen to have the minimal value for k. Remark 10.2 is part of the motivation for this choice. This choice is also good for getting small absolute values of the coefficients, as we have seen in Remark 8.5. We have $k = 1$ for i_1 and $k = 2$ for i_2 and i_3.

We did not normalize our invariants with powers of 2 to get $c_3 = 1$, because invariants without these powers of 2 are easier to remember and yield smaller class polynomials in practice.

Remark 10.4. It follows from Goren [18, Thms. 1 and 2] that Theorem 10.1 remains true if one restricts in the product defining D to primes p that divide $2 \cdot 3 \cdot c_3\Delta$ or factor as a product of two prime ideals in $\mathcal{O}_K$. See also Goren and Lauter [20, Tables 3.3.1 and 3.5.1].

10.3. **The bounds as stated by Goren and Lauter.** The first part of the proof of Theorem 10.1 is the following bound on the primes that occur in the denominator.

Lemma 10.5 (Goren and Lauter [19])**.** *The coefficients of each of the polynomials $H_{K,n}(X)$ and $\widehat{H}_{K,n}$ for $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$ a primitive quartic CM-field are S-integers, where S is the set of primes smaller than $4da^2$.*

Proof. Corollary 5.2.1 of [19] is this result with $4d^2a^2$ instead of $4da^2$. We can however adapt the proof as follows to remove a factor d. In [19, Corollary 2.1.2], it suffices to have only $N(k_1)N(k_2) < p/4$ in order for two elements k_1 and k_2 of the quaternion order ramified in p and infinity to commute. Then, in the proof of [19, Theorem 3.0.4], it suffices to take as hypothesis only $p > d(\mathrm{Tr}(r))^2$. As we have $d(\mathrm{Tr}(r))^2 \geq d\delta_1\delta_2 \geq N(x)N(by^\vee)$, this implies that x and $by^\vee$ are in the same imaginary quadratic field K_1. As in the original proof, this implies that $ywy^\vee$ is also contained in K_1 and hence $\psi(\sqrt{r}) \in M_2(K_1)$, so there is a morphism $K = \mathbf{Q}(\sqrt{r}) \mapsto M_2(K_1)$, contradicting primitivity of K. □

Remark 10.6. Lemma 10.5 as phrased above is for class polynomials defined in terms of the invariants i_1, i_2, i_3 of Section 2. If other invariants are used, then the result is still valid if the primes dividing c_3 of Remark 10.2 are added to S.

Recent results of Eyal Goren bound the exponents to which primes may occur in the denominator as follows.

Lemma 10.7 (Goren-Lauter [20])**.** *Let K be a primitive quartic CM-field and $C/\mathbf{C}$ a curve of genus 2 that has CM by $\mathcal{O}_K$. Let v be a non-archimedean valuation of $L(i_n(C))$, normalized with respect to $\mathbf{Q}$ in the sense that $v(\mathbf{Q}^*) = \mathbf{Z}$ holds, and let e be its ramification index (so ev is normalized with respect to $L(i_n(C))$. Let k and c_3 be as in Remark 10.2.*

Then we have

$$-v(i_n(C)) \leq 4k(\log(2da^2)/\log(p) + 1) + v(c_3) \qquad \text{if } e \leq p-1, \text{ and}$$

$$-v(i_n(C)) \leq 4k(8\log(2da^2)/\log(p) + 2) + v(c_3) \qquad \text{otherwise.} \tag{10.8}$$

Moreover, $e \leq p-1$ is automatic for $p \neq 2$, 3.

Proof. Theorem 7.0.4 of Goren and Lauter [20] gives the valuation bounds.

Next, we show $e \leq 4$ for $p > 2$. Let $L \subset \mathbf{C}$ be isomorphic to the normal closure of K, let Φ be the CM-type of C and $K^{\mathrm{r}} \subset L$ its reflex field. The extension $K^{\mathrm{r}}(i_n(C))/K^{\mathrm{r}}$ is unramified by the main theorem of complex multiplication [34, Main Theorem 1 in §15.3 in Chap. IV]. In particular, the ramification index of any prime in $L(i_n(C))/\mathbf{Q}$ is at most its ramification index in $L/\mathbf{Q}$. By Lemma 4.12, the field L has degree 4 over $\mathbf{Q}$ or has degree 2 over a biquadratic subfield, hence we have $e \leq 4$ for $p > 2$. □

10.4. **The bounds in terms of discriminants.** Lemmas 10.5 and 10.7 hold for any representation of K of the form $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$, hence in particular for such a representation with da^2 minimal. The following result gives a lower and an upper bound on the minimal da^2.

Lemma 10.9. *Let K be a quartic CM-field with discriminant Δ and let Δ_0 be the discriminant of the real quadratic subfield K_0.*

For all $a, b, d \in \mathbf{Z}$ such that $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$ holds, we have $a^2 > \Delta_1$ and $d \geq \frac{1}{4}\Delta_0$. Conversely, there exist such $a, b, d \in \mathbf{Z}$ with $d = \Delta_0$ and $a^2 < (\frac{8}{\pi})^2 \Delta_1 \Delta_0$.

Proof. The lower bounds are trivial, because Δ_0 divides $4d$ and Δ_1 divides $a^2 - b^2 d \leq a^2$. For the upper bound, we show the existence of a suitable element $-a + b\sqrt{\Delta_0}$ using a geometry of numbers argument.

We identify $K \otimes_{\mathbf{Q}} \mathbf{R}$ with $\mathbf{C}^2$ via its pair of infinite primes. Then $\mathcal{O}_K$ is a lattice in $\mathbf{C}^2$ of covolume $2^{-2}\sqrt{\Delta}$. Let ω_1, ω_2 be a $\mathbf{Z}$-basis of $\mathcal{O}_{K_0}$, and consider the open parallelogram $\omega_1(-1,1) + \omega_2(-1,1) \subset \mathcal{O}_{K_0} \otimes \mathbf{R} \cong \mathbf{R}^2$. We define the open convex symmetric region

$$V_Y = \{x \in \mathbf{C}^2 : \mathrm{Re}(x) \in \omega_1(-1,1) + \omega_2(-1,1), (\mathrm{Im}\, x_1)^2 + (\mathrm{Im}\, x_2)^2 < Y\}.$$

Then $\mathrm{vol}(V_Y) = 4\pi\sqrt{\Delta_0}Y$ and by Minkowski's convex body theorem, V_Y contains a non-zero element $\alpha \in \mathcal{O}_K$ if we have

$$\mathrm{vol}(V_Y) > 2^4 \,\mathrm{covol}\, \mathcal{O}_K = 4\sqrt{\Delta}.$$

We pick $Y = \sqrt{\Delta_1\Delta_0}\pi^{-1} + \epsilon$, so that α exists.

Let $r = 4(\alpha - \overline{\alpha})^2$, which is of the form $-a + b\sqrt{\Delta_0}$ with integers a and b. Now $a = \frac{1}{2}|r_1 + r_2| = 2(2\,\mathrm{Im}\, x_1)^2 + 2(2\,\mathrm{Im}\, x_2)^2 < 8Y = 8\sqrt{\Delta_1\Delta_0}\pi^{-1} + 8\epsilon$. As a is in the discrete set $\mathbf{Z}$, and we can take ϵ arbitrarily close to 0, we find that we can even get $a \leq 8\sqrt{\Delta_1\Delta_0}\pi^{-1}$ and hence $a^2 \leq (\frac{8}{\pi})^2\Delta_1\Delta_0$. □

Proof of Theorem 10.1. Lemma 10.5 proves that the denominator of the Igusa class polynomials is divisible only by primes dividing D.

Next, let v be any normalized non-archimedean valuation of H_{K^r} and c any coefficient of $H_{K,n}$ or $\widehat{H}_{K,n}$. Then c is a sum of products, where each product consists of at most h' factors $i_n(C)$ for certain n's and C's. This shows that $-v(c)$ is at most h' times the right hand side of (10.8), hence $v(Dc) \geq 0$. As this holds for all v, it follows that Dc is an integer. This concludes the proof that $DH_{K,n}$ and $D\widehat{H}_{K,n}$ are in $\mathbf{Z}[X]$.

The fact that we can replace a and d as in the theorem is Lemma 10.9. Next, we prove the asymptotic bound on D. Note that the exponent of every prime in $D^{1/h'}$ is linear in $\log\Delta$, as is the bit size of every prime divisor of D. Therefore, $\log D$ is $\widetilde{O}(h'N)$, where $N = O(\Delta)$ is the number of prime divisors of D, which finishes the proof of Theorem 10.1. □

11. Recovering a polynomial from its roots

At this point, we know how to find approximations of the roots of the polynomial $H_1(X)$, and we wish to combine these into approximations of the coefficients of $H_1(X)$. In other words, we need to take the product of a set of linear polynomials.

11.1. **Numerically multiplying many polynomials.** We compute the product of a set of linear polynomials by arranging them in a binary tree, and computing the products of pairs of polynomials using fast multiplication. This method is well known, and a complete analysis of its running time and rounding errors is given by Kirrinnis [26].

Define the norm of a polynomial $p = \sum a_k x^k \in \mathbf{C}[x]$ to be $|p| = |p|_1 = \sum |a_k|$. Let $p_1, \ldots, p_n$ be linear polynomials such that $|p_i| \leq 2^{t_i}$ holds with $t_i \geq 1$, and let $t = \sum t_i$. In particular, if $p_i = (x - z_i)$, take $t_i \geq \max\{\log_2(|z_i| + 1), 1\}$.

Theorem 11.1 (Kirrinnis [26])**.** *There exists an explicit algorithm, independent of the data mentioned above, with the following input, output and running time.*
Input: *Positive integers n, s and $t_1, \ldots, t_n$, and linear polynomials $\widetilde{p}_1, \ldots, \widetilde{p}_n$ satisfying*

$$|\widetilde{p}_i - p_i| < 2^{-(s+t-t_i+2\lceil \log_2 n \rceil)},$$

Output: *A polynomial $\widetilde{p}$ satisfying $|p_1 \cdots p_n - \widetilde{p}| < 2^{-s}$,*
Running time: *$O(\psi(n \cdot \log n \cdot (s+t)))$, where $\psi(k) = O(k \log k \log\log k)$ is the time needed for multiplication of two k-bit integers.*

Proof. We reduce to the case $t_i = 1$ by the substitution $t_i \mapsto 1$, $t \mapsto n$, $s \mapsto s+t-n$, $p_i \mapsto 2^{-t_i+1}p_i$, $\widetilde{p}_i \mapsto 2^{-t_i+1}\widetilde{p}_i$, $\widetilde{p} \mapsto 2^{-t+n}\widetilde{p}$. Note that it takes linear time to move the point $t_i - 1$ places to the left in $\widetilde{p}_i$ and to move it back to its correct position in the output $\widetilde{p}$.

For the case $t_i = 1$, this result is a special case of Algorithm 5.1 of [26]. To see this in the notation of loc. cit., note $t = n$, let $l = n$, and let $\mathbf{n} = (n_1, \ldots, n_l) = (1, \ldots, 1)$. The definitions of $H_1(\mathbf{n})$ and $d_i(\mathbf{n})$ can be found on page 407 of [26], and it follows that in our case $d_i(\mathbf{n}) \leq \lceil \log_2 n \rceil$ and $H_1(\mathbf{n}) \leq n\lceil \log_2 n \rceil$ hold. For ψ, see [26, p. 383], and for $|p|$ and Π_n, see [26, p. 381]. □

Remark 11.2. The restriction to linear input polynomials is only to make the bounds on the running time and the required input precision easier to state. It is not present in [26].

Remark 11.3. For more details about the history of the algorithm, see [26, Section 3.2].

11.2. **Recognizing rational coefficients.** There are various ways of recognizing a polynomial $f \in \mathbf{Q}[X]$ from an approximation $\widetilde{f}$. If one knows an integer D such that the denominator of f divides D, and the error $|\widetilde{f} - f|$ is less than $(2D)^{-1}$, then Df is obtained from $D\widetilde{f}$ by rounding the coefficients to the nearest integers.

Other methods to compute f from $\widetilde{f}$ are based on continued fractions, where the coefficients of f are obtained via the continued fraction expansion of the coefficients of $\widetilde{f}$, or on the LLL-algorithm, where the coefficients of an integral multiple of f arise as coordinates of a small vector in a lattice [29, Section 7]. These methods have the advantage that only a bound B on the denominator needs to be known, instead of an actual multiple D. This is very useful in practical implementations, because one can guess a small value for B, which may be much smaller than any easily computable proven D. In the case of Igusa class polynomials, there exist a few good heuristic checks of the output when using a non-proven bound B, such as smoothness of the denominators, and successfulness of CM constructions of abelian surfaces over finite fields.

For our purpose of giving a proven running time bound however, we prefer the first method of rounding $D\widetilde{f}$, since it is easy to analyze and asymptotically fast.

It takes time $\widetilde{O}(\log D)$ to compute D of Theorem 10.1 using sieving to find the primes and a binary tree to multiply them together. We conclude that we can compute $H_{K,n}$ from $\widetilde{H}_{K,n}$ in time $\widetilde{O}(\log D)$ plus time linear in the bit size of $\widetilde{H}_{K,n}$, provided that we have $|\widetilde{H}_{K,n} - H_{K,n}| < (2D)^{-1}$.

12. The algorithm

We now have all the required ingredients for our algorithm and a proof of the main theorem.

Algorithm 12.1.
Input: A positive quadratic fundamental discriminant Δ_0 and positive integers a and b such that the the field $K = \mathbf{Q}(\sqrt{-a + b\sqrt{\Delta_0}})$ is a primitive quartic CM-field of discriminant greater than a.
Output: The Igusa class polynomials $H_{K,n}$ for $n = 1, 2, 3$.

(1) Compute a $\mathbf{Z}$-basis of $\mathcal{O}_K$ using the algorithm of Buchmann and Lenstra [5] and use this to compute the discriminant Δ of K.

(2) Compute a complete set $\{A_1, \dots, A_{h'}\}$ of representatives of the h' isomorphism classes of principally polarized abelian surfaces over $\mathbf{C}$ with CM by $\mathcal{O}_K$, using Algorithm 4.10. Here each A_j is given by a triple $(\Phi_j, \mathfrak{a}_j, \xi_j)$ as in Section 4.4.
(3) From Δ and h', compute D such that $DH_{K,n}$ is in $\mathbf{Z}[X]$ for $n = 1, 2, 3$, as in Section 11.2.
(4) For $j = 1, \dots, h'$, do the following.
  (a) Compute a symplectic basis of $\mathfrak{a}_j$ using Algorithm 5.2. This provides us with a period matrix $W_j \in \mathcal{H}_2 \cap \mathrm{Mat}_2(L)$, where $L \subset \mathbf{C}$ is the normal closure of K.
  (b) Replace the period matrix W_j by an $\mathrm{Sp}_4(\mathbf{Z})$-equivalent period matrix $Z_j \in \mathcal{F}_2 \cap \mathrm{Mat}_2(L)$, using Algorithm 6.8.
  (c) Let $u_j = \lceil 3 + (y_1 + y_2 - y_3)\pi + \max\{2, -\log_2 |z_3|\} \rceil$, where

$$Z_j = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix} \quad \text{and} \quad y_k = \operatorname{Im} z_k \quad (k = 1, 2, 3).$$

(5) Let $p = \lceil \log_2 D + 3 \log_2 h' + 4 \rceil + \sum_{j=1}^{h'} (2u_j + 40)$. This is the precision with which we will approximate the Igusa invariants.
(6) For $j = 1, \dots, h'$, do the following.
  (a) Evaluate the theta constants in Z_j to precision $r_j = 101 + 7u_j + p$ as explained above Theorem 8.12.
  (b) Use Lemma 8.3 to evaluate $i_n(A_j)$ for $(n = 1, 2, 3)$ to precision p.
(7) For $n = 1, 2, 3$, do the following.
  (a) Use the algorithm of Theorem 11.1 to compute an approximation $\widetilde{H}_{K,n}$ of $H_{K,n}$ for $n = 1, 2, 3$ from the approximations of Igusa invariants of step 6b.
  (b) Compute $DH_{K,n}$ by rounding the coefficients of $D\widetilde{H}_{K,n}$ to nearest integers.
  (c) Output $H_{K,n}$.

The polynomials $\widehat{H}_{K,n}$ $(n = 2, 3)$ of Section 2.4 can be computed from the approximations of $i_n(C)$ and $i_1(C)$ efficiently using Algorithm 10.9 of [39] (see also [15, Section 4]). However, instead of doing a detailed rounding error analysis of that algorithm, we give a more naive and slower algorithm that is still much faster than the running time in our Main Theorem. To compute the polynomials $\widehat{H}_{K,n}$, we simply modify step 7a as follows:

(1) Evaluate each summand in the definition of the polynomial $\widehat{H}_{K,n}$ using the algorithm of Theorem 11.1.
(2) Approximate $\widetilde{H}_{K,n}$ by arranging its summands in a binary tree and adding them.

We now recall and prove the main theorem.

Main Theorem. *Algorithm 12.1 computes $H_{K,n}$ $(n = 1, 2, 3)$ for any primitive quartic CM-field K. It has a running time of $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ and the bit size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.*

Proof. We start by proving that the output is correct. Using Lemma 8.3 and Theorem 8.12, one can show (see [36, Proposition II.7.14]) that the precision r_j for the theta constants suffices to get the absolute Igusa invariants with precision p. Theorem 8.10 tells us that we have $|i_n(Z_j)| \leq 2^{6u_j+77}$. These bounds and Theorem 11.1 show that it suffices to know the absolute Igusa invariants to precision p in order to get a precision of $1 + \log_2 D$ bits for the coefficients of $H_{K,n}$. By Theorem 10.1, the polynomials $DH_{K,n}$ have integer coefficients, so a precision of $1 + \log_2 D$ for the coefficients of $H_{K,n}$ suffices for recognizing these coefficients and getting a correct output. This proves that the output of Algorithm 12.1 is correct.

Next, we bound the precisions p and r_j. We start by bounding u_j, for which we need an upper bound on $y_1 + y_2 - y_3$ and a lower bound on z_3. We have $y_2 \geq y_1$ and $y_3 \geq 0$, hence $y_1 + y_2 - y_3 \leq 2y_2$, and Theorem 7.1 gives the upper bound $y_2 \leq \frac{2}{3\sqrt{3}} \max\{2\Delta_0, \Delta_1^{1/2}\}$.

We claim that the off-diagonal entry z_3 of $Z_j \in \mathcal{H}_2$ is non-zero. Indeed, if $z_3 = 0$, then $Z_j = \mathrm{diag}(z_1, z_2)$ with $z_1, z_2 \in \mathcal{H} = \mathcal{H}_1$ and A_j is the product of the elliptic curves corresponding to z_1 and z_2, contradicting the fact that A_j is simple (Theorem 4.2.3). The claim and Corollary 6.18 together now give an upper bound on $\log(1/z_3)$, which is polynomial in $\log \Delta$ by Lemma 4.15.

We now have

$$u_j = O(\max\{\Delta_0, \Delta_1^{1/2}\}), \quad h' = \widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2}),$$

and by Theorem 10.1 also $\log D = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$. We find that p is dominated by our bounds on $\log D$, hence we have $p = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ and also $r_j = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$.

Finally, we can bound the running time. Under the assumption that K is given as $K = \mathbf{Q}(\sqrt{-a + b\sqrt{\Delta_0}})$, where Δ_0 is a positive fundamental discriminant and a, b are positive integers such that $a < \Delta_0$, we can factor $(a^2 - b^2\Delta_0)\Delta_0^2$ and hence find the ring of integers in step 1 in time $O(\Delta)$.

As shown in Section 4.4, step 2 takes time $\widetilde{O}(\Delta^{1/2})$. Step 3 takes time $\widetilde{O}(D) = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$.

For every j, step 4a takes time polynomial in $\log \Delta$ by Lemma 4.15 and Theorem 6.17. The same holds for steps 4b and 4c and each summand of step 5. The number of iterations or summands of these steps is $2h' = \widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$ by Lemmas 9.1 and 4.14. In particular, steps 4 and 5 take time $\widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$.

We now come to the most costly step. By Theorem 8.12, it takes time $\widetilde{O}(r_j^2)$ to do a single iteration of step 6a. In particular, all iterations of this step together take time $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$.

The j-th iteration of step 6b takes time $\widetilde{O}(r)$ and hence all iterations of this step together take time $\widetilde{O}(\Delta_1^2\Delta_0^3)$. Finally, by Theorem 11.1, step 7a takes time $\widetilde{O}(h')$ times $\widetilde{O}(p)$, which is $\widetilde{O}(\Delta_1^2\Delta_0^3)$. The same amount of time is needed for the final two steps.

The output consists of $h' + 1$ rational coefficients, each of which has a bit size of $\widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$, hence the size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.

This proves the main theorem, except when using the polynomials $\widehat{H}_{K,n}$ $(n = 2, 3)$ of Section 2.4. With the naive method of evaluating $\widehat{H}_{K,n}$ that we described in Algorithm 12.1, it takes $\widetilde{O}(h_1)$ times as much time to evaluate $\widetilde{H}_{K,n}$ from the Igusa invariants as it does to evaluate $H_{K,n}$. This $\widetilde{O}(\Delta_1^{5/2}\Delta_0^{7/2})$ is still dominated by the running time of the rest of the algorithm. □

References

[1] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic Number Theory – ANTS-VIII (Banff, 2008)*, volume 5011 of *LNCS*, pages 282–295. Springer, 2008.

[2] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer, second edition, 2004.

[3] Oskar Bolza. Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen ϑ-Functionen. *Math. Ann.*, 30(4):478–495, 1887.

[4] Jan Hendrik Bruinier and Tonghai Yang. CM-values of Hilbert modular functions. *Invent. Math.*, 163(2):229–288, 2006.

[5] Johannes Buchmann and Hendrik W. Lenstra, Jr. Approximating rings of integers in number fields. *Journal de Théorie des Nombres de Bordeaux*, 6:221–260, 1994.

[6] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Scientific, 2005.

[7] Robert Carls, David Kohel, and David Lubicz. Higher-dimensional 3-adic CM construction. *J. Algebra*, 319(3):971–1006, 2008.

[8] Robert Carls and David Lubicz. A p-adic quasi-quadratic time point counting algorithm. *Int. Math. Res. Not. IMRN*, (4):698–735, 2009.

[9] E. de Shalit and E. Z. Goren. On special values of theta functions of genus two. *Ann. Inst. Fourier (Grenoble)*, 47(3):775–799, 1997.

[10] Régis Dupont. Fast evaluation of modular functions using Newton iterations and the AGM. To appear in *Mathematics of Computation*, `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/preprints/Dupont_FastEvalMod.ps.gz`, 2006.

[11] Régis Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École Polytechnique, 2006. `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`.
[12] Friedrich Eisenbrand and Günter Rote. Fast reduction of ternary quadratic forms. In *Cryptography and lattices (Providence, RI, 2001)*, volume 2146 of *Lecture Notes in Comput. Sci.*, pages 32–44. Springer, Berlin, 2001.
[13] Kirsten Eisenträger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. To appear in *Arithmetic, Geometry and Coding Theory, AGCT-10* (Marseille, 2005), 2005.
[14] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Mathematics of Computation*, 78(266):1089–1107, 2009.
[15] Andreas Enge and François Morain. Fast decomposition of polynomials with known Galois group. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 254–264, Berlin, 2003. Springer.
[16] Gerhard Frey and Tanja Lange. Complex multiplication. In H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors, *Handbook of elliptic and hyperelliptic curve cryptography*, pages 455–473. Chapman & Hall/CRC, 2006.
[17] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129, Berlin, 2006. Springer-Verlag.
[18] Eyal Z. Goren. On certain reduction problems concerning abelian surfaces. *manuscripta mathematica*, 94(1):33–43, 1997.
[19] Eyal Z. Goren and Kristin Lauter. Class invariants for quartic CM fields. *Annales de l'Institut Fourier*, 57(2):457–480, 2007.
[20] Eyal Z. Goren and Kristin Lauter. Genus 2 curves with complex multiplication. arXiv:1003.4759v1, 2010.
[21] Erhard Gottschling. Die Randflächen des Fundamentalbereiches der Modulgruppe. *Math. Annalen*, 138:103–124, 1959.
[22] Erich Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen*. Chelsea Publishing Co., Bronx, N.Y., 1970. Second edition of the 1923 original, with an index.
[23] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.
[24] Jun-Ichi Igusa. On siegel modular forms of genus two. *American Journal of Mathematics*, 84(1):175–200, 1962.
[25] Jun-Ichi Igusa. Modular forms and projective invariants. *American Journal of Mathematics*, 89(3):817–855, 1967. `http://www.jstor.org/stable/2373243`.
[26] Peter Kirrinnis. Partial fraction decompostion in $\mathbb{C}(z)$ and simultaneous Newton iteration for factorization in $\mathbb{C}[z]$. *J. Complexity*, 14(3):378–444, 1998.
[27] Helmut Klingen. *Introductory lectures on Siegel modular forms*, volume 20 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.
[28] David Kohel et al. ECHIDNA algorithms for algebra and geometry experimentation. `http://echidna.maths.usyd.edu.au/~kohel/dbs/complex_multiplication2.html`.
[29] Hendrik W. Lenstra, Jr. Lattices. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory*, volume 44 of *MSRI Publications*, pages 127 – 181. Cambridge University Press, 2008.
[30] Stéphane Louboutin. Explicit lower bounds for residues at $s = 1$ of Dedekind zeta functions and relative class numbers of CM-fields. *Trans. Amer. Math. Soc.*, 355(8):3079–3098 (electronic), 2003.
[31] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334, Boston, MA, 1991. Birkhäuser Boston.
[32] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser, 1984.
[33] René Schoof. Computing Arakelov class groups. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory*, volume 44 of *MSRI Publications*, pages 447 – 495. Cambridge University Press, 2008.
[34] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.
[35] Anne-Monika Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994. `http://www.uni-due.de/zahlentheorie/theses_de.shtml`.
[36] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010. `http://hdl.handle.net/1887/15572`.
[37] Carl Johannes Thomae. Beitrag zur Bestimmung von $\vartheta(0, \cdots, 0)$ durch die Klassenmoduln algebraischer Funktionen. *J. reine angew. Math.*, 71:201–222, 1870.

[38] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.

[39] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[40] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Number 83 in Graduate Texts in Mathematics. Springer, 1982.

[41] Heinrich Weber. *Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Braunschweig, Friedrich Vieweg, 1908.

[42] André Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:33–53, 1957.

[43] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, 2002.

[44] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. `http://www.math.wisc.edu/~thyang/RecentPreprint.html`, 2007.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
E-mail address: `marco.streng@gmail.com`