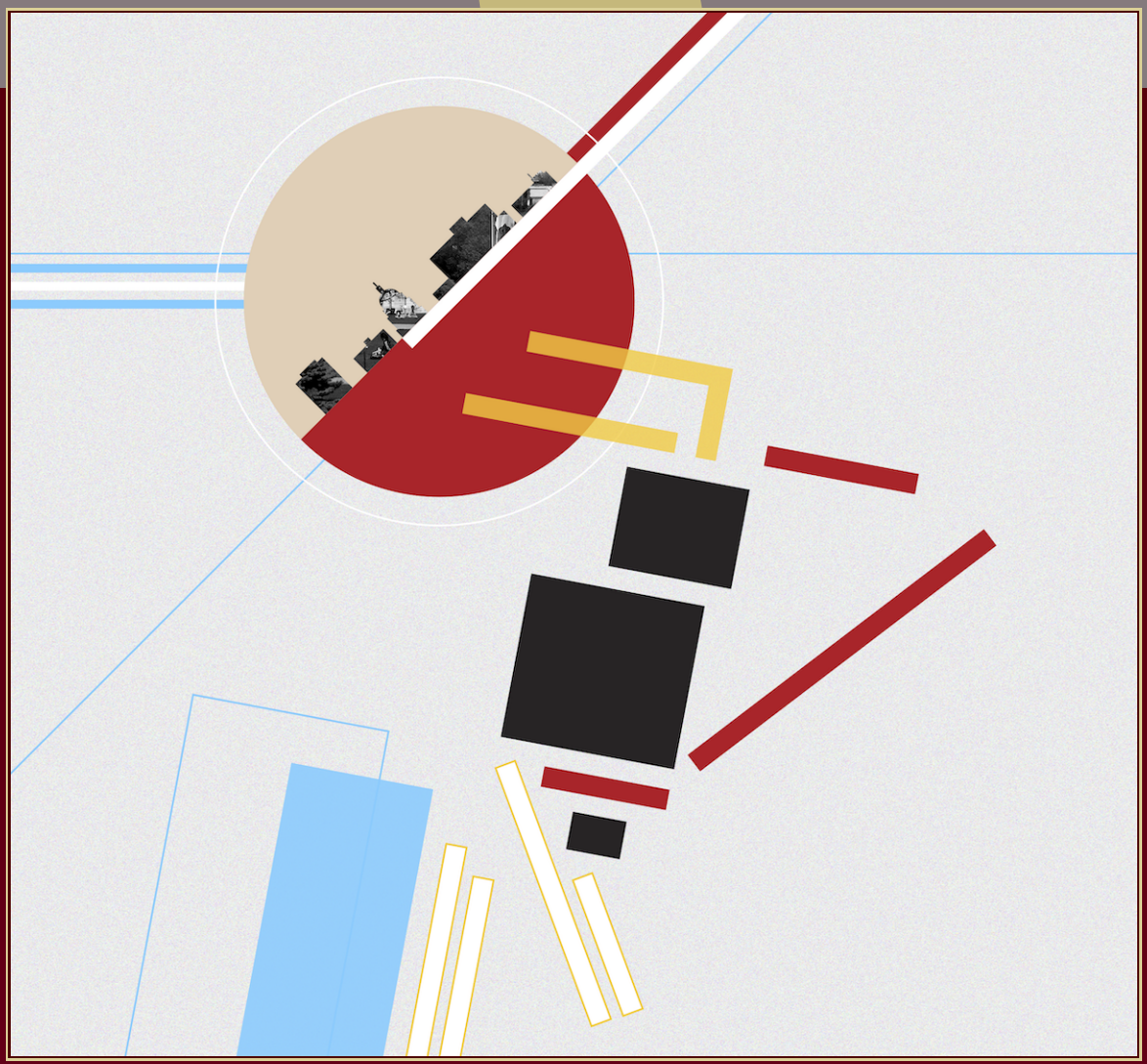
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$

Alexandre Gélin, Everett W. Howe, and Christophe Ritzenthaler



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.257

msp

Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$

Alexandre Gélin, Everett W. Howe, and Christophe Ritzenthaler

We give equations for 13 genus-2 curves over $\overline{\mathbb{Q}}$, with models over $\mathbb{Q}$, whose unpolarized Jacobians are isomorphic to the square of an elliptic curve with complex multiplication by a maximal order. If the generalized Riemann hypothesis is true, there are no further examples of such curves. More generally, we prove under the generalized Riemann hypothesis that there exist exactly 46 genus-2 curves over $\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to the square of an elliptic curve with complex multiplication by a maximal order.

1. Introduction

For $g > 1$, let $\mathfrak{M}_g$ and $\mathfrak{A}_g$ be the moduli spaces classifying absolutely irreducible projective smooth curves of genus g and principally polarized abelian varieties of dimension g, respectively, over $\overline{\mathbb{Q}}$. These spaces are quasiprojective varieties defined over $\mathbb{Q}$, linked by the Torelli map, which associates to a curve its Jacobian. To explain the modular interpretation of rational points on these spaces, we must define the terms *field of definition* and *field of moduli*. If X is a curve or polarized abelian variety over $\overline{\mathbb{Q}}$, we say that a field $F \subseteq \overline{\mathbb{Q}}$ is a *field of definition* of X if there exists a variety X_0/F — called a *model* of X over F — such that $X_0 \simeq_{\overline{\mathbb{Q}}} X$. Since $\overline{\mathbb{Q}}$ is a field of characteristic 0, by [Koi72, Corollary 3.2.2, p. 54] we can define the *field of moduli* of X to be either

- the field fixed by the subgroup $\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid X \simeq X^\sigma\}$, or
- the intersection of the fields of definition of X.

With these terms defined, we can say that the rational points on $\mathfrak{M}_g$ and $\mathfrak{A}_g$ correspond to the isomorphism classes of curves and principally polarized abelian varieties, respectively, over $\overline{\mathbb{Q}}$ that have field of moduli $\mathbb{Q}$ [Bai62].

This work was supported in part by a public grant as part of the *Investissement d'avenir* project, reference ANR-11-LABX-0056-LMH, LabEx LMH.
MSC2010: primary 11G15; secondary 14H25, 14H45.
Keywords: genus-2 curves, abelian varieties, polarizations, fields of moduli, complex multiplication.

There are a number of interesting sets of rational points on $\mathfrak{A}_g$, but the complex multiplication (CM) abelian varieties — that is, the principally polarized abelian varieties having endomorphism rings containing an order in a number field of degree $2g$ over $\mathbb{Q}$ — have attracted the most interest. When such a point on $\mathfrak{A}_g$ lies in the image of $\mathfrak{M}_g$, the corresponding curve is called a *CM-curve*. For $g = 2$, the set of *simple* CM-abelian varieties with field of moduli $\mathbb{Q}$ is known, and for those varieties that are Jacobians explicit equations have been computed for the corresponding curves [Spa94; vW99; MU01; KS15; BS17]; for $g = 3$ the similar set of possible CM maximal orders is determined in [Kıl16] and conjectural equations for the curves are given in [Wen01; KW05; BILV16; LS16; KLL+18]. (And while we have avoided the case $g = 1$ in the discussion above for technical reasons, it is still of course true that the CM-elliptic curves with rational j-invariants are known as well [Sil94, Appendix A.3].)

In this article we consider genus-2 curves whose Jacobians are nonsimple CM-abelian surfaces. Every such surface is isogenous to the square of a CM-elliptic curve, but we restrict our attention in two ways: first, we look only at surfaces that are *isomorphic* (and not just isogenous) to E^2 for a CM-elliptic curve E, and second, we only consider E that have CM by a maximal order. The second restriction is not essential to our methods, and we impose it here in order to simplify some of our calculations. Note that if the elliptic curve E has no CM — i.e., $\mathrm{End}(E) \simeq \mathbb{Z}$ — then E^2 cannot be isomorphic to the Jacobian of a genus-2 curve, because E^2 has no indecomposable principal polarizations [Lan06, Corollary 4.2, p. 159].

Main contributions. We prove under the generalized Riemann hypothesis that there exist exactly 46 genus-2 curves over $\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to the square of an elliptic curve with CM by a maximal order. We show that among these 46 curves exactly 13 can be defined over $\mathbb{Q}$, and we give explicit equations for them. In order to accomplish this, we develop an algorithm to compute, for an imaginary quadratic maximal order $\mathbb{O}$, canonical forms for all positive definite unimodular Hermitian forms on $\mathbb{O} \times \mathbb{O}$. Such Hermitian forms correspond to principal polarizations φ on E^2, and our algorithm computes the automorphism group of the polarized variety (E^2, φ) and identifies the polarizations that come from genus-2 curves.

Related work. Hayashida and Nishi [HN65] consider in particular when a product of two elliptic curves, with CM by the same maximal order $\mathbb{O}$, is the Jacobian of a curve over $\mathbb{C}$, and they find that this happens if and only if the discriminant of $\mathbb{O}$ is different from -1, -3, -7, and -15. Hayashida [Hay68] gives the number of indecomposable principal polarizations on E^2 where $E/\mathbb{C}$ is an elliptic curve with CM by a maximal order. More recently, Kani [Kan14; Kan16] gives existence results on Jacobians isomorphic to the product of two elliptic curves with control on the polarization, and Schuster [Sch89] and Lange [Lan06] study generalizations to higher dimensions. Rodriguez-Villegas [RV00] considers the same situation as Hayashida and Nishi, and in the case where $\mathbb{O}$ has class number 1 and odd discriminant, he gives an algorithm (relying on quaternion algebras) for producing curves with field of moduli $\mathbb{Q}$. Note finally that Fité and Guitart [FG18] determine when there exists an abelian surface $A/\mathbb{Q}$ that is $\overline{\mathbb{Q}}$-isogenous to E^2, with $E/\overline{\mathbb{Q}}$ a CM-curve.

Outline. Torelli's theorem [Ser01] implies that our genus-2 curve C has field of moduli $\mathbb{Q}$ if and only if its principally polarized Jacobian (E^2, φ) has field of moduli $\mathbb{Q}$. We therefore need to find all elliptic curves E with CM by a maximal order $\mathbb{O}$ and all polarizations φ of E^2 such that (E^2, φ) is isomorphic to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. Proposition 2.1 shows that if E^2 is isomorphic to all of its Galois conjugates — even just as an abelian variety without polarization — then the class group of $\mathbb{O}$ has exponent at most 2. Under the generalized Riemann hypothesis, this gives us an explicit finite list of possible orders (Table 1). For each of these orders $\mathbb{O}$, one can identify the indecomposable principal polarizations φ on E^2 and describe them as certain 2-by-2 matrices M with coefficients in $\mathbb{O}$ (Proposition 3.1). Tables of such matrices were computed by Hoffmann [Hof91] and Schiemann [Sch98] and were published online,[1] but they only include a fraction of the discriminants that we must consider. We therefore describe an algorithm, using a method different from that of Hoffmann and Schiemann, that we use to recompute these tables of matrices (Section 3B). Given such a matrix M, we find explicit algebraic conditions on M for the principally polarized abelian surface (E^2, φ) to have field of moduli $\mathbb{Q}$ (Section 3C). We check whether these conditions are satisfied for each M on our list.

We conclude the article with three more results: we heuristically compute the Cardona–Quer invariants [CQ05] of the associated curves C and see that the factorization of their denominators reveals interesting patterns; we show that the field of moduli is a field of definition if and only if C has a nontrivial group of automorphisms (i.e., of order greater than 2; see Proposition 4.1); and for curves C defined over $\mathbb{Q}$, we compute equations and prove that they are correct.

Notation. In the following, E is an elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication by a maximal order $\mathbb{O}$ of discriminant Δ and with fraction field K, which we sometimes call the *CM-field*.

2. Condition on E^2

We are interested in the field of moduli $\boldsymbol{M}$ of a principally polarized abelian surface (E^2, φ). As outlined above, we first consider the abelian surface E^2 alone and we give a necessary condition for $\boldsymbol{M}$ to be contained in the CM-field K. If $\boldsymbol{M} \subseteq K$ then in particular we have $E^2 \simeq (E^\sigma)^2$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. The class group $\mathrm{Cl}(\mathbb{O})$ acts simply transitively on the set of elliptic curves with CM by $\mathbb{O}$ [Sil94, Proposition 1.2, p. 99]. Since $\mathrm{End}(E^\sigma) = \mathrm{End}(E) = \mathbb{O}$, for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, there exists a unique class of ideals $I_\sigma \in \mathrm{Cl}(\mathbb{O})$ such that $E^\sigma \simeq E/I_\sigma$.

Using a result of Kani [Kan11, Proposition 65, p. 335], we get that, for E, σ, and I_σ defined as above,

$$E^2 \simeq (E/I_\sigma)^2 \iff I_\sigma^2 = [\mathbb{O}],$$

where the last equality is in $\mathrm{Cl}(\mathbb{O})$. Note that since we only work with maximal orders, the conditions on the conductors in Kani's result are trivially satisfied. Moreover by [Sil94, Theorem 4.3, p. 122], since for any $I \in \mathrm{Cl}(\mathbb{O})$ there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ (actually even in $\mathrm{Gal}(K(j(E))/K)$) such that $E/I = E^\sigma$, we get the following proposition.

[1] Available at https://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/.

$\#\mathrm{Cl}(\mathbb{O})$	Discriminants Δ
2^0	$-3, -4, -7, -8, -11, -19, -43, -67, -163$
2^1	$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115,$ $-123, -148, -187, -232, -235, -267, -403, -427$
2^2	$-84, -120, -132, -168, -195, -228, -280, -312,$ $-340, -372, -408, -435, -483, -520, -532, -555,$ $-595, -627, -708, -715, -760, -795, -1012, -1435$
2^3	$-420, -660, -840, -1092, -1155, -1320, -1380,$ $-1428, -1540, -1848, -1995, -3003, -3315$
2^4	-5460

Table 1. Discriminants Δ of the imaginary quadratic maximal orders $\mathbb{O}$ of exponent at most 2, conditional on the generalized Riemann hypothesis.

Proposition 2.1. *A necessary condition for $\boldsymbol{M} \subseteq K$ is that the class group of $\mathbb{O}$ has exponent at most* 2*.*

Louboutin [Lou90] shows that under the assumption of the generalized Riemann hypothesis, the discriminant Δ of an imaginary quadratic field whose class group is of exponent at most 2 satisfies $|\Delta| \leq 2 \cdot 10^7$. In Table 1 we list the 65 fundamental discriminants satisfying this bound that give class groups of exponent at most 2.

3. Polarized abelian surfaces

3A. ***Polarizations on the square of an elliptic curve.*** We now consider the principal polarizations on the product surface $A = E^2$. A principal polarization on A is, in particular, an isogeny of degree 1 from A to the dual $\hat{A}$ of A, but not every isomorphism $A \to \hat{A}$ is a principal polarization; other properties must be satisfied as well [BL92, §4.1]. One such polarization is the product polarization $\varphi_0 = \varphi_E \times \varphi_E$. Given any other principal polarization φ, we can consider the automorphism $M = \varphi_0^{-1}\varphi$ of A, which (in light of the isomorphism $A = E^2$) we view as a matrix[2] in $\mathrm{GL}_2(\mathbb{O})$. Our first result characterizes the matrices that arise in this way; the statement is not new, but we provide a proof here because it introduces some of the ideas used in the sequel. (Recall [Hal58, Exercise 7, p. 134] that two matrices M_1 and M_2 in $\mathrm{GL}_2(\mathbb{O})$ are said to be *congruent* if there exists a matrix $P \in \mathrm{GL}_2(\mathbb{O})$ such that $P^* M_1 P = M_2$, where P^* is the conjugate transpose of P.)

Proposition 3.1. *The map $M \mapsto \varphi_0 \cdot M$ defines a bijection between the positive definite unimodular Hermitian matrices with coefficients in $\mathbb{O}$ and the principal polarizations on A. Two principal polarizations are isomorphic to one another if and only if their associated matrices are congruent to one another.*

Proof. By [BL92, Theorem 5.2.4, p. 121], the matrices M corresponding to principal polarizations are totally positive symmetric endomorphisms of norm 1. Here the symmetry is with respect to the Rosati

[2] All matrices in this paper act on the left.

involution of $\mathrm{End}(A)$ associated to the polarization φ_0, which is the conjugate-transpose involution under the identification $\mathrm{End}(A) = M_2(\mathbb{C})$. Thus, the matrices M corresponding to principal polarizations are exactly the positive definite unimodular Hermitian matrices.

Let φ_1 and φ_2 be two principal polarizations on A, corresponding to matrices M_1 and M_2. The polarizations φ_1 and φ_2 are isomorphic to one another if and only if there exists an automorphism $\alpha : A \to A$ such that $\hat{\alpha}\varphi_1\alpha = \varphi_2$, where $\hat{\alpha} : \hat{A} \to \hat{A}$ is the dual of α. This last condition is equivalent to $(\varphi_0^{-1}\hat{\alpha}\varphi_0)(\varphi_0^{-1}\varphi_1\alpha) = \varphi_0^{-1}\varphi_2$. Now, $\varphi_0^{-1}\hat{\alpha}\varphi_0$ is nothing other than the Rosati involute of α, so if we write α as a matrix $P \in \mathrm{GL}_2(\mathbb{C})$, the condition that determines whether φ_1 and φ_2 are isomorphic is simply $P^*M_1P = M_2$. □

The principal polarizations on A come in two essentially different types.

Definition 3.2. A polarization φ on an abelian variety A over a field k is said to be *geometrically decomposable* if there exist two abelian varieties A_1 and A_2 over $\bar{k}$ of positive dimension, together with polarizations φ_1 and φ_2, such that (A, φ) and $(A_1 \times A_2, \varphi_1 \times \varphi_2)$ are isomorphic over $\bar{k}$. A polarization that is not geometrically decomposable is *geometrically indecomposable*. For brevity's sake, in this paper we drop the adjective *geometrically* and simply use the terms *decomposable* and *indecomposable* for these concepts.

Results in [Wei57; Hoy63; OU73] show that a principally polarized abelian surface is the Jacobian of a curve if and only if the polarization is indecomposable. In the remainder of this section we show how we can easily compute representatives for the congruence classes of matrices representing the decomposable polarizations on E^2; we focus on the indecomposable polarizations in later sections.

Proposition 3.3. *If φ is a decomposable polarization on E^2, then there exist elliptic curves F and F' that have CM by $\mathbb{O}$ such that φ is the pullback to E^2 of the product polarization on $F \times F'$ via some isomorphism $E^2 \simeq F \times F'$. The pair (F, F') giving rise to a given decomposable polarization is unique up to interchanging F and F' and up to isomorphism for each elliptic curve. Moreover, for every F with CM by $\mathbb{O}$ there exists an F' with CM by $\mathbb{O}$ such that $E^2 \simeq F \times F'$.*

Proof. First we note that by definition, if φ is a decomposable polarization on E^2 there must exist elliptic curves F and F', isogenous to E, such that φ is the pullback of the product polarization on $F \times F'$ under some isomorphism $E^2 \simeq F \times F'$. Now, the center of $\mathrm{End}(E^2)$ is $\mathrm{End}(E) = \mathbb{O}$, while the center of $\mathrm{End}(F \times F')$ is $\mathrm{End}(F) \cap \mathrm{End}(F')$; since $\mathbb{O}$ is a maximal order, F and F' both have CM by $\mathbb{O}$.

If $(\alpha, \beta) : G \to F \times F'$ is an embedding of an elliptic curve G into $F \times F'$, then the pullback of the product polarization to G is the morphism

$$\begin{bmatrix} \hat{\alpha} & \hat{\beta} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \hat{\alpha}\alpha + \hat{\beta}\beta = \deg(\alpha) + \deg(\beta);$$

that is, the pullback is the multiplication-by-d map, with $d = \deg(\alpha) + \deg(\beta)$. It follows that if φ is the pullback to E^2 of the product polarization on $F \times F'$ via some isomorphism $E^2 \simeq F \times F'$, then the set of elliptic curves G for which there exists an embedding $\epsilon : G \to E^2$ such that $\epsilon^*\varphi$ is a principal

polarization is simply $\{F, F'\}$. Thus, for a given decomposable principal polarization, the pair (F, F') is unique up to order and isomorphism.

As we noted at the beginning of Section 2, the set of elliptic curves with CM by $\mathbb{O}$ is a principal homogenous space for the class group of $\mathbb{O}$. Given an F with CM by $\mathbb{O}$, let $I \in \mathrm{Cl}(\mathbb{O})$ be the ideal class that takes E to F. If F' is an elliptic curve with CM by $\mathbb{O}$, say corresponding to an ideal class $I' \in \mathrm{Cl}(\mathbb{O})$, then $E^2 \simeq F \times F'$ if and only if I' is the inverse of I [Kan11, Proposition 65, p. 335]. This proves the final statement of the proposition. □

Corollary 3.4. *Let h denote the class number of $\mathbb{O}$, and let t denote the size of the 2-torsion subgroup of the class group. The number of decomposable polarizations on E^2 is equal to $(h+t)/2$.*

Proof. The proof of Proposition 3.3 shows that the unordered pairs (F, F') with $E^2 \simeq F \times F'$ correspond to unordered pairs (I, I^{-1}), where $I \in \mathrm{Cl}(\mathbb{O})$. The number of such pairs is $(h+t)/2$. □

Let F be an elliptic curve with CM by $\mathbb{O}$, and let I be the ideal class that takes E to F. Let $\mathfrak{a}$ be an ideal of $\mathbb{O}$ representing I, such that $\mathfrak{a}$ is not divisible by any nontrivial ideal of $\mathbb{Z}$. We may write $\mathfrak{a} = (n, \alpha)$, where $n = \mathrm{Norm}(\mathfrak{a}) \in \mathbb{Z}$ and where $\alpha \in \mathfrak{a}$ is chosen so that the ideal $\alpha\mathfrak{a}^{-1}$ is coprime to $n\mathbb{O}$; then there exist $x, y \in \mathbb{Z}$ such that $xn^2 - y\,\mathrm{Norm}(\alpha) = n$. Let F' be the elliptic curve such that $E^2 \simeq F \times F'$. We prove the following corollary in Section 3C.

Corollary 3.5. *In the notation of the paragraph above, the isomorphism class of the decomposable polarization on E^2 obtained from pulling back the product polarization on $F \times F'$ is represented by the congruence class of the matrix*

$$\begin{pmatrix} n+\mathrm{Norm}(\alpha)/n & (x+y)\alpha \\ (x+y)\bar{\alpha} & x^2 n + y^2\,\mathrm{Norm}(\alpha)/n \end{pmatrix}.$$

3B. ***How to find the polarizations?*** In Section 2, we identified 65 orders $\mathbb{O}$ for which we need to compute the set of indecomposable principal polarizations, or equivalently, representatives of the congruence classes of indecomposable positive definite unimodular Hermitian matrices with coefficients in $\mathbb{O}$. In this section we describe how we computed these representatives.

Fix an embedding ϵ_0 of K into the complex numbers. For any $\alpha \in \mathbb{O}$, we write $\alpha > 0$ if either the trace of α is positive, or the trace of α is 0 and $\epsilon_0(\alpha)$ has positive imaginary part. Then for $\alpha, \beta \in \mathbb{O}$ we write $\alpha > \beta$ if $\alpha - \beta > 0$. Clearly this gives us a total ordering on $\mathbb{O}$.

Let $\mathcal{H}$ denote the set of positive definite unimodular Hermitian matrices with coefficients in $\mathbb{O}$. Let $\chi : \mathcal{H} \to \mathbb{N} \times \mathbb{N} \times \mathbb{O}$ be the map that sends a matrix $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$ to the triple (a, d, b). We define a total ordering on $\mathcal{H}$ by saying that $M_1 < M_2$ if $\chi(M_1) < \chi(M_2)$ in the lexicographic ordering on $\mathbb{N} \times \mathbb{N} \times \mathbb{O}$.

Given any $M \in \mathcal{H}$, we say that M is *reduced* if $M \le M'$ for all M' congruent to M. Clearly every $M \in \mathcal{H}$ is congruent to a unique reduced matrix. The following algorithm produces the reduced matrix that is congruent to a given M.

Algorithm 3.6.

Input: *A positive definite unimodular Hermitian matrix M with coefficients in $\mathbb{O}$, specified by $a, d \in \mathbb{Z}$ and $b \in \mathbb{O}$ such that $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$.*

Output: *The reduced matrix congruent to M.*

(1) *Set $a' = 1$.*

(2) *Compute the set A' of vectors $\boldsymbol{x} = (x_1, x_2) \in \mathbb{O}^2$ such that $\boldsymbol{x}^* M \boldsymbol{x} = a'$ and such that x_1 and x_2 generate the unit ideal of $\mathbb{O}$. If $A' = \varnothing$, increment a' and repeat.*

(3) *Set $d' = a'$.*

(4) *Compute the set D' of vectors $\boldsymbol{y} = (y_1, y_2) \in \mathbb{O}^2$ such that $\boldsymbol{y}^* M \boldsymbol{y} = d'$ and such that y_1 and y_2 generate the unit ideal of $\mathbb{O}$. If $D' = \varnothing$, increment d' and repeat.*

(5) *Initialize $\mathcal{M}$ to be the empty set.*

(6) *For each $\boldsymbol{x} \in A'$ and $\boldsymbol{y} \in D'$ such that $\boldsymbol{x}$ and $\boldsymbol{y}$ generate $\mathbb{O}^2$ as an $\mathbb{O}$-module, let M' be the matrix representing the Hermitian form M written on the basis $\boldsymbol{x}$, $\boldsymbol{y}$ of $\mathbb{O}^2$, and add M' to the set $\mathcal{M}$.*

(7) *If $\mathcal{M}$ is empty, increment d' and return to Step* (4).

(8) *Find the smallest element M' of $\mathcal{M}$ under the ordering of $\mathcal{H}$ defined above.*

(9) *Output M'.*

Remark 3.7. In Steps (2) and (4) of Algorithm 3.6, we need to find vectors in $\mathbb{O}^2$ of a given length under the quadratic form specified by M. We note that this is a finite computation: if $\boldsymbol{x} = (x_1, x_2)$ satisfies $\boldsymbol{x}^* M \boldsymbol{x} = n$, with $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$, then

$$\mathrm{Norm}(ax_1 + bx_2) + \mathrm{Norm}(x_2) = an.$$

Thus, to solve $\boldsymbol{x}^* M \boldsymbol{x} = n$, we can simply enumerate all pairs $(u, v) \in \mathbb{O}^2$ with $\mathrm{Norm}(u) + \mathrm{Norm}(v) = an$, and keep those pairs for which $u - bv$ is divisible by a.

Note that solving $\boldsymbol{x}^* M \boldsymbol{x} = n$ can be done more quickly when the value of a is small. Thus, in Algorithm 3.6, once one finds a short vector $\boldsymbol{x} = (x_1, x_2)$ with x_1 and x_2 coprime, it is worthwhile to compute *any* vector $\boldsymbol{y}$ such that $\boldsymbol{x}$ and $\boldsymbol{y}$ generate $\mathbb{O}$, and to replace M with the congruent form obtained by rewriting M on the basis $\boldsymbol{x}$, $\boldsymbol{y}$.

Theorem 3.8. *Algorithm 3.6 terminates with the correct result.*

Proof. Let $M' = \left(\begin{smallmatrix} a' & b' \\ \bar{b}' & d' \end{smallmatrix}\right)$ be the reduced matrix congruent to M. If $P = \left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right)$ is an element of $\mathrm{GL}_2(\mathbb{O})$ such that $P^* M P = M'$, and if we set $\boldsymbol{x} = (x_1, x_2)$ and $\boldsymbol{y} = (y_1, y_2)$, then $a' = \boldsymbol{x}^* M \boldsymbol{x}$ and $d' = \boldsymbol{y}^* M \boldsymbol{y}$. By the very definition of the ordering on $\mathcal{H}$, then, we want to find vectors $\boldsymbol{x}$ and $\boldsymbol{y}$, each with coordinates that are coprime to one another, such that $\boldsymbol{x}^* M \boldsymbol{x}$ is as small as possible and $\boldsymbol{y}^* M \boldsymbol{y}$ is as small as possible, given that $\boldsymbol{x}$ and $\boldsymbol{y}$ generate $\mathbb{O}^2$ as an $\mathbb{O}$-module. This is what the algorithm does. Finally, among all possible such pairs $(\boldsymbol{x}, \boldsymbol{y})$, we simply need to choose the one that gives the smallest matrix. □

Hayashida [Hay68] gives a formula for the number of isomorphism classes of indecomposable principal polarizations on E^2 in the case where E has CM by a maximal order.[3] Hayashida's proof does not immediately lead to a constructive method of finding polarizations representing the isomorphism classes, but simply knowing the number of isomorphism classes is the key to a straightforward algorithm for producing such representatives.

Algorithm 3.9.

Input: *A fundamental discriminant* $\Delta < 0$.

Output: *A list of reduced matrices representing the distinct congruence classes of positive definite unimodular Hermitian matrices with entries in the order* $\mathbb{O}$ *of discriminant* Δ, *separated into the decomposable and indecomposable classes.*

(1) *Compute the number* N *of indecomposable polarizations on* E^2 *using Hayashida's formula.*

(2) *Compute the set* $\mathcal{D}$ *of reduced matrices representing decomposable polarizations, using Corollary 3.5 and Algorithm 3.6.*

(3) *Initialize* $\mathcal{I}$ *to be the empty set and set* $P = 0$.

(4) *Increment* P, *and compute the set* S *of elements of* $\mathbb{O}$ *of norm* $P - 1$.

(5) *For every divisor* a *of* P *with* $a \leq P/a$, *and for every* $b \in S$:

  (a) *Compute the reduced form* M *of the matrix* $\left(\begin{smallmatrix} a & b \\ \bar{b} & P/a \end{smallmatrix}\right)$.

  (b) *If* M *is not contained in* $\mathcal{D} \cup \mathcal{I}$, *then add* M *to the set* $\mathcal{I}$.

(6) *If* $\#\mathcal{I} < N$, *then return to Step* (4).

(7) *Return* $\mathcal{D}$ *and* $\mathcal{I}$.

Of course, for our goal of producing genus-2 curves over $\mathbb{Q}$ with Jacobians isomorphic to E^2, we only need the indecomposable polarizations.

Theorem 3.10. *Algorithm 3.9 terminates with the correct result.*

Proof. The algorithm is very straightforward. Every isomorphism class of principal polarization appears somewhere on the countable list that we are considering, and we simply enumerate the polarizations and compute their reduced forms until we have found the right number of isomorphism classes. □

Remark 3.11. In our applications, when the class group of $\mathbb{O}$ has exponent at most 2, we can speed up our algorithm as follows: once we have a principal polarization M on E^2, we can view the same matrix as giving a polarization on F^2 for any elliptic curve F with CM by $\mathbb{O}$. Since the class group has exponent at most 2, there exists an isomorphism $E^2 \to F^2$, and pulling M back to E^2 via such an isomorphism gives a new positive definite unimodular Hermitian matrix M'. Each time we find a new

[3] There is a typographical error in Hayashida's paper. In the second line of page 43, the term $(1/4)(1-(-1))^{(m^2-1)/8}$ should be $(1/4)(1-(-1)^{(m^2-1)/8})h$. Note that the correction involves both moving a parenthesis and adding an instance of the variable h.

reduced polarization M, we compute the reduced forms of the polarizations M' associated to all the curves F isogenous to E, and add these reduced forms to the set $\mathfrak{D}$ if they are new.

If φ is a principal polarization on E^2 and M is the corresponding Hermitian matrix, then the automorphism group of the polarized abelian variety (E^2, φ), denoted by $\mathrm{Aut}(E^2, \varphi)$, is isomorphic to the group $\{P \in \mathrm{GL}_2(\mathbb{O}) \mid P^* M P = M\}$. Note that if φ is indecomposable, so that (E^2, φ) is the polarized Jacobian of a curve C, then Torelli's theorem [Ser01] shows that this group is also isomorphic to $\mathrm{Aut}(C)$. In any case, computing $\mathrm{Aut}(E^2, \varphi)$ is straightforward:

Algorithm 3.12.

Input: *A positive definite unimodular Hermitian matrix* $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$ *with entries in an imaginary quadratic maximal order* $\mathbb{O}$.

Output: *A list of all matrices* $P \in \mathrm{GL}_2(\mathbb{O})$ *such that* $P^* M P = M$.

(1) *Compute the set* A *of vectors* $\boldsymbol{x} = (x_1, x_2) \in \mathbb{O}^2$ *such that* $\boldsymbol{x}^* M \boldsymbol{x} = a$ *and such that* x_1 *and* x_2 *generate the unit ideal of* $\mathbb{O}$.

(2) *Compute the set* D *of vectors* $\boldsymbol{y} = (y_1, y_2) \in \mathbb{O}^2$ *such that* $\boldsymbol{y}^* M \boldsymbol{y} = d$ *and such that* y_1 *and* y_2 *generate the unit ideal of* $\mathbb{O}$.

(3) *Initialize* $\mathcal{A}$ *to be the empty set.*

(4) *For each* $\boldsymbol{x} \in A$ *and* $\boldsymbol{y} \in D$ *such that* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *generate* $\mathbb{O}^2$ *as an* $\mathbb{O}$*-module*:
   (a) *Compute* $b' = \boldsymbol{x}^* M \boldsymbol{y}$.
   (b) *If* $b' = b$ *then add the matrix* $\left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right)$ *to the set* $\mathcal{A}$.

(5) *Output* $\mathcal{A}$.

(See Remark 3.7 for an explanation of how to implement the two first steps.)

Theorem 3.13. *Algorithm 3.12 terminates with the correct result.*

Proof. If $P = \left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{O})$ satisfies $P^* M P = M$, then $\boldsymbol{x} = (x_1, x_2)$ and $\boldsymbol{y} = (y_1, y_2)$ are vectors in $\mathbb{O}^2$ such that $\boldsymbol{x}^* M \boldsymbol{x} = a$ and $\boldsymbol{y}^* M \boldsymbol{y} = d$ and $\boldsymbol{x}^* M \boldsymbol{y} = b$. The algorithm simply enumerates all $\boldsymbol{x}$ and $\boldsymbol{y}$ that meet the first two conditions, and checks to see whether they meet the third. □

3C. ***Conditions on the polarization.*** Throughout this section, E is an elliptic curve with CM by a maximal order $\mathbb{O}$ of an imaginary quadratic field K whose class group has exponent at most 2. Also φ is a principal polarization on E^2 corresponding (as in Proposition 3.1) to a positive definite unimodular Hermitian matrix M with entries in $\mathbb{O}$ and $\boldsymbol{M}$ is the field of moduli of the polarized abelian variety (E^2, φ). We resume our analysis of the condition that $\boldsymbol{M} = \mathbb{Q}$.

Proposition 3.14. *Let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ *be ideals of* $\mathbb{O}$ *representing all of the elements of the class group of* $\mathbb{O}$, *and for each* i *let* $n_i \in \mathbb{Z}_{>0}$ *generate* $\mathrm{Norm}(\mathfrak{a}_i)$. *Then* $\boldsymbol{M} = \mathbb{Q}$ *if and only if for every* i *there exists a matrix* $P_i \in \mathrm{GL}_2(K)$, *with entries in* $\mathfrak{a}_i$, *such that* $n_i M = P_i^* M P_i$.

Proof. Lemma 3.15 below shows that $\boldsymbol{M} = \mathbb{Q}$ if and only if $\boldsymbol{M} \subseteq K$, and this is the case if and only if for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ there exists an isomorphism $\alpha_\sigma : (E^2, \varphi) \to ((E^\sigma)^2, \varphi^\sigma)$. To understand this condition, we use the classical theory of complex multiplication of abelian varieties; the book of Shimura and Taniyama [ST61] is one possible reference, especially Chapter II.

Under the embedding $\epsilon_0 : K \to \mathbb{C}$ we chose earlier, the isomorphism classes of elliptic curves over $\overline{\mathbb{Q}} \subset \mathbb{C}$ with CM by $\mathbb{O}$ correspond to the lattices $\epsilon_0(\mathfrak{a})$ up to scaling, for fractional ideals $\mathfrak{a}$ of $\mathbb{O}$. Since the class group of the order $\mathbb{O}$ is 2-torsion, we have $E^2 \simeq F^2$ for every E and F with CM by $\mathbb{O}$, so we may as well choose our E so that it corresponds to the trivial ideal $\mathbb{O}$.

Let Δ be the discriminant of $\mathbb{O}$ and let $\delta \in \mathbb{O}$ be a square root of Δ, chosen so that $\epsilon_0(\delta)$ is positive imaginary. Note that the trace dual $\mathfrak{a}^\dagger$ of an arbitrary fractional $\mathbb{O}$-ideal $\mathfrak{a}$ is $(1/\delta)\mathfrak{a}^{-1}$. If F is the elliptic curve corresponding to $\mathfrak{a}$, then the dual of F is the elliptic curve corresponding to the complex conjugate of $\mathfrak{a}^\dagger$, and the canonical principal polarization of F is the isomorphism $\mathfrak{a} \to (1/\delta)\bar{\mathfrak{a}}^{-1}$ given by $x \mapsto x/(n\delta)$, where $n \in \mathbb{Q}$ is the positive generator of $\mathrm{Norm}(\mathfrak{a})$. (See [ST61, §6.3] for more details.)

Let φ_0 be the product polarization on E^2. For $\alpha_\sigma : E^2 \to (E^\sigma)^2$ to give an isomorphism between (E^2, φ) and $((E^\sigma)^2, \varphi^\sigma)$, the following diagram must be commutative:

$$\begin{array}{ccccc} E^2 & \xrightarrow{M} & E^2 & \xrightarrow{\varphi_0} & \widehat{E}^2 \\ \downarrow{\scriptstyle \alpha_\sigma} & & & & \uparrow{\scriptstyle \hat{\alpha}_\sigma} \\ (E^\sigma)^2 & \xrightarrow{M} & (E^\sigma)^2 & \xrightarrow{\varphi_0^\sigma} & (\widehat{E}^\sigma)^2 \end{array}$$

To express this diagram in terms of lattices, we let $\mathfrak{a}$ be an ideal corresponding to E^σ, we let $n = \mathrm{Norm}(\mathfrak{a})$, and we let P_σ be the matrix in $\mathrm{GL}_2(K)$ corresponding to α_σ. Then the preceding diagram becomes

$$\begin{array}{ccccc} \mathbb{O} \times \mathbb{O} & \xrightarrow{M} & \mathbb{O} \times \mathbb{O} & \xrightarrow{1/\delta} & (1/\delta)(\mathbb{O} \times \mathbb{O}) \\ \downarrow{\scriptstyle P_\sigma} & & & & \uparrow{\scriptstyle P_\sigma^*} \\ \mathfrak{a} \times \mathfrak{a} & \xrightarrow{M} & \mathfrak{a} \times \mathfrak{a} & \xrightarrow{1/(n\delta)} & (1/\delta)(\bar{\mathfrak{a}}^{-1} \times \bar{\mathfrak{a}}^{-1}) \end{array}$$

Thus, there exists an isomorphism $(E^2, \varphi) \to ((E^\sigma)^2, \varphi^\sigma)$ of polarized varieties if and only if there exists a matrix P, with entries in $\mathfrak{a}$, such that $nM = P^* M P$. Since the Galois group of $\overline{\mathbb{Q}}/K$ acts transitively on the set of elliptic curves with CM by $\mathbb{O}$, the field of moduli of (E^2, φ) is contained in K if and only if we can find such a matrix P for each of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$. □

Lemma 3.15. *Let E, φ, and $\boldsymbol{M}$ be as mentioned at the beginning of this section. Then $\boldsymbol{M} = \mathbb{Q}$ if and only if $\boldsymbol{M} \subseteq K$.*

Proof. Let us assume that $\boldsymbol{M} \subseteq K$; we must show that $\boldsymbol{M} = \mathbb{Q}$. Since $\mathbb{O}$ has a class group of exponent at most 2, [Shi71, Exercise 5.8, p. 124] implies that $\mathbb{Q}(j(E))$ is totally real. Let ι be any complex conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so that ι acts trivially on $\mathbb{Q}(j(E))$ and nontrivially on K. Given any element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we want to show that $(E^2, \varphi) \simeq ((E^\sigma)^2, \varphi^\sigma)$.

If σ acts trivially on K, then such an isomorphism exists, because $\boldsymbol{M} \subseteq K$. Otherwise, $\sigma\iota$ acts trivially on K, and we have $(E^2, \varphi) \simeq ((E^{\sigma\iota})^2, \varphi^{\sigma\iota})$, and therefore $((E^\iota)^2, \varphi^\iota) \simeq ((E^\sigma)^2, \varphi^\sigma)$. So it is enough for us to show that $(E^2, \varphi) \simeq ((E^\iota)^2, \varphi^\iota)$. If we choose our model of E to be defined over $\mathbb{Q}(j(E))$, then $E^\iota = E$, and we simply need to show that there exists an element P of $\mathrm{GL}_2(\mathbb{O})$ such that $\overline{M} = P^* M P$. If $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$, we can simply take $P = \left(\begin{smallmatrix} b & d \\ -a & -\bar{b} \end{smallmatrix}\right)$. □

At this point, we have reviewed enough CM theory to prove Corollary 3.5.

Proof of Corollary 3.5. We are given an ideal $\mathfrak{a} = (n, \alpha)$ of $\mathbb{O}$, where $n \in \mathbb{Z}$ is the norm of $\mathfrak{a}$ and where $\alpha \in \mathbb{O}$, and we have $x, y \in \mathbb{Z}$ such that $xn^2 - y\,\mathrm{Norm}(\alpha) = n$. The complex conjugate $\bar{\mathfrak{a}}$ of $\mathfrak{a}$ represents the inverse of the class of $\mathfrak{a}$ in $\mathrm{Cl}(\mathbb{O})$, and the matrix $P = \left(\begin{smallmatrix} n & y\alpha \\ \bar{\alpha} & xn \end{smallmatrix}\right)$ takes the lattice $\mathbb{O} \times \mathbb{O} \subset K^2$ onto the lattice $\mathfrak{a} \times \bar{\mathfrak{a}}$. The dual lattice for $\mathfrak{a} \times \bar{\mathfrak{a}}$ is $(n\delta)^{-1} \cdot (\mathfrak{a} \times \bar{\mathfrak{a}})$ (where δ is the positive imaginary square root of Δ as in the proof of Proposition 3.14) and the product polarization from $\mathfrak{a} \times \bar{\mathfrak{a}}$ to its dual is simply multiplication by $1/(n\delta)$. Pulling this polarization back to $\mathbb{O} \times \mathbb{O}$ via P gives us the polarization $(n\delta)^{-1} P^* P$. Since the product polarization on $\mathbb{O} \times \mathbb{O}$ is $1/\delta$, the pullback polarization is represented by the endomorphism $(1/n) P^* P$ of $\mathbb{O} \times \mathbb{O}$, and we compute that $(1/n) P^* P$ is the matrix given in the statement of the corollary. □

We close this section by indicating how we can check the criterion given in Proposition 3.14: namely, given the polarization matrix M and an ideal $\mathfrak{a}$ with $\mathrm{Norm}(\mathfrak{a}) = n\mathbb{Z}$, how can we determine whether there exists a matrix $P \in M_2(\mathfrak{a})$ that satisfies $nM = P^* M P$?

Suppose there exists such a matrix P. If $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$ let us take $L = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, so that $L^* L = aM$. Let $Q = L P L^{-1}$. Then the condition $nM = P^* M P$ becomes the condition $n\,\mathrm{Id} = Q^* Q$. This equality can only hold if Q is of the form

$$Q = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathrm{GL}_2(K)$$

where $x, y, z, t \in K$ satisfy $\mathrm{Norm}(x) + \mathrm{Norm}(z) = \mathrm{Norm}(y) + \mathrm{Norm}(t) = n$ and $\bar{x}y + \bar{z}t = 0$. Since we have

$$P = L^{-1} Q L = \begin{pmatrix} x - bz & (bx + y - b^2 z - bt)/a \\ az & bz + t \end{pmatrix} \in M_2(\mathfrak{a}),$$

we see that we must have $x = X/a$, $y = Y/a$, $z = Z/a$, and $t = T/a$ with $X, Y, Z, T \in \mathfrak{a}$.

Therefore, to check whether a matrix P with the desired properties exists, it suffices to compute and store all solutions $(X, Z) \in \mathfrak{a} \times \mathfrak{a}$ to the norm equation $\mathrm{Norm}(X) + \mathrm{Norm}(Z) = a^2 n$ (which can be done efficiently). Then, for every two solutions (X, Z) and (Y, T) satisfying $\overline{X}Y + \overline{Z}T = 0$, we can check whether the corresponding matrix P lies in $M_2(\mathfrak{a})$. If we obtain such a P for each of the ideals $\mathfrak{a}_i$ from Proposition 3.14, then the field of moduli for (E^2, φ) is $\mathbb{Q}$. In fact, we need only find a P for each $\mathfrak{a}_i$ in a set that generates the class group of $\mathbb{O}$.

3D. ***Results.*** We have implemented the algorithms described in the previous sections. We were able to test all polarizations on the 65 possible orders identified in Section 2. The results are presented in Table 2.

h	Δ	$\#\varphi$	$\#C$	h	Δ	$\#\varphi$	$\#C$	h	Δ	$\#\varphi$	$\#C$
1	−3	0	0	4	−84	2	0	8	−420	10	0
	−4	0	0		−120	5	3		−660	16	0
	−7	0	0		−132	3	1		−840	22	0
	−8	1	1		−168	4	0		−1092	22	0
	−11	1	1		−195	8	0		−1155	32	0
	−19	1	1		−228	5	1		−1320	36	0
	−43	2	2		−280	14	0		−1380	34	0
	−67	3	3		−312	11	1		−1428	28	0
	−163	7	7		−340	14	0		−1540	46	0
					−372	8	0		−1848	46	0
2	−15	0	0		−408	14	0		−1995	56	0
	−20	1	1		−435	16	0		−3003	72	0
	−24	1	1		−483	12	0		−3315	128	0
	−35	2	0		−520	25	3				
	−40	2	2		−532	14	0	16	−5460	128	0
	−51	2	0		−555	20	0				
	−52	2	2		−595	28	2				
	−88	4	2		−627	16	0				
	−91	4	0		−708	15	1				
	−115	6	0		−715	36	0				
	−123	4	0		−760	41	1				
	−148	5	3		−795	28	2				
	−187	8	0		−1012	28	0				
	−232	9	5		−1435	64	0				
	−235	12	0								
	−267	8	0								
	−403	18	0								
	−427	16	0								

Table 2. The number of indecomposable principal polarizations φ and the number of isomorphism classes of curves C with field of moduli $\mathbb{Q}$ for each discriminant Δ, grouped by class number h.

There exist 1226 indecomposable polarizations, in total. Our algorithms, implemented in Magma on a laptop with a 2.50 GHz Intel Core i7-4710MQ processor, took less than 21 minutes to compute all of the polarizations; about 10 minutes of that time was spent on the largest discriminant. The computation required about 2.8 GB of memory.

Once we computed the polarizations, it took about 26 minutes (on the same laptop) to check the conditions of Proposition 3.14. For this calculation, the largest discriminant represented more than two-thirds of the computation time.

In the end, we obtained exactly 46 polarizations φ such that the principally polarized abelian surface (E^2, φ) is isomorphic to the Jacobian of a curve C with field of moduli $\mathbb{Q}$. These 46 curves are obtained only from orders whose class groups have order 1, 2, or 4.

4. Computation of invariants and final remarks

4A. ***Invariants of the genus-2 curves C.*** A genus-2 curve C has field of moduli $\mathbb{Q}$ if and only if all of its absolute invariants are defined over $\mathbb{Q}$ (see for example [LRS13, §3]). This is in particular true for the triplet (g_1, g_2, g_3) of invariants defined by Cardona and Quer in [CQ05], which characterizes a genus-2 curve up to $\overline{\mathbb{Q}}$-isomorphism and enables one to find an equation $y^2 = f(x)$ for the curve. We quickly review here a strategy for obtaining the Cardona–Quer invariants for the 46 curves whose invariants are $\mathbb{Q}$-rational.

The first quantity we are able to derive is a Riemann matrix τ, using the same method as [Rit10, §3.3]. Starting with the positive definite unimodular Hermitian matrix M corresponding to the polarization $\varphi = \varphi_0 \cdot M$, we obtain the Riemann matrix τ associated to φ and the CM-elliptic curve $E \simeq \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\omega)$ where $\omega = (1 + \sqrt{\Delta})/2$ if Δ is odd and $\omega = \sqrt{\Delta}$ otherwise.

This matrix we get is defined up to the action of the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$. One then works out a matrix τ_0 in the orbit of τ for which the computation of the theta constants $(\theta_i)_{0\le i\le 9}$ at τ_0 is fast (see [Lab16] for instance).

A complex model of a curve $C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ with Riemann matrix τ_0 can then be classically approximated using Rosenhain's formulas [Ros51, p. 417]

$$\lambda_1 = \frac{\theta_0^2\theta_2^2}{\theta_1^2\theta_3^2}, \qquad \lambda_2 = \frac{\theta_2^2\theta_7^2}{\theta_3^2\theta_9^2}, \quad \text{and} \quad \lambda_3 = \frac{\theta_0^2\theta_7^2}{\theta_1^2\theta_9^2}.$$

By computing the theta constants to higher and higher precision, we are able to get a sufficiently good approximation of the Cardona–Quer invariants to recognize them as rationals. The numbers we get are a priori only heuristic as there is no bound known for the denominators of these rationals; however, we can sometimes prove that these heuristic values are correct, as follows.

Given a set of Cardona–Quer invariants that we suspect are equal to the invariants of a curve whose Jacobian is isomorphic to E^2 for an E with complex multiplication, we can easily produce a curve C having those invariants. Then we can use the techniques of [CMSV18] to provably compute the endomorphism ring of the Jacobian of C. If this endomorphism ring is isomorphic to the ring $M_2(\mathrm{End}\, E)$, then we have provably found a curve of the type we are looking for.

We computed heuristic values for the Cardona–Quer invariants of our 46 principally polarized abelian surfaces, and the list of these invariants is available on authors' web pages,[4] together with all the programs to compute them. We are grateful to J. Sijsling for computing the endomorphism rings for the Jacobians of 13 of our 46 curves; he is currently developing a faster and more robust algorithm which should be able to handle the remaining cases. For each of these 13 curves, the endomorphism ring was $M_2(\mathrm{End}\, E)$, so the heuristic values of the Cardona–Quer invariants of these curves are provably correct.

We observe that for the 13 provably correct sets of invariants, all the denominators are smooth integers. It would be very interesting, in the same spirit as [GL07; LV15] for the CM genus-2 case, to find formulas

[4] Available at https://alexgelin.github.io/, http://ewhowe.com, and https://perso.univ-rennes1.fr/christophe.ritzenthaler/.

Δ	M	Cardona–Quer invariants $[g_1, g_2, g_3]$
-8	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 2 \end{pmatrix}$	$[2^4\cdot 5^5,\ 2\cdot 3\cdot 5^4,\ -5^3]$
-11	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 2 \end{pmatrix}$	$\left[\frac{19^5}{2^2},\ \frac{3^2\cdot 11\cdot 19^3}{2^5},\ -\frac{19^2\cdot 47}{2^6}\right]$
-19	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 3 \end{pmatrix}$	$\left[\frac{5^5\cdot 29^5}{2^2\cdot 3^7},\ \frac{5^3\cdot 7\cdot 29^3\cdot 31\cdot 73}{2^5\cdot 3^8},\ -\frac{5^2\cdot 17\cdot 29^2\cdot 2719}{2^6\cdot 3^{10}}\right]$
-20	$\begin{pmatrix} 2 & \omega \\ -\omega & 3 \end{pmatrix}$	$\left[\frac{5^5\cdot 7^5}{2^2},\ \frac{5^5\cdot 7^3\cdot 11}{2^5},\ -\frac{3\cdot 5^3\cdot 7^2}{2^6}\right]$
-24	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 4 \end{pmatrix}$	$\left[\frac{2^4\cdot 23^5}{3},\ \frac{2\cdot 23^3\cdot 421}{3^2},\ -\frac{23^2\cdot 37}{3^4}\right]$
-40	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 6 \end{pmatrix}$	$\left[\frac{2^4\cdot 5^5\cdot 43^5}{3^7},\ \frac{2\cdot 5^4\cdot 43^3\cdot 6977}{3^8},\ -\frac{5^4\cdot 13\cdot 43^2}{3^{10}}\right]$
-52	$\begin{pmatrix} 2 & \omega \\ -\omega & 7 \end{pmatrix}$	$\left[\frac{5^5\cdot 173^5}{2^2\cdot 3^7},\ \frac{5^4\cdot 173^3\cdot 112061}{2^5\cdot 3^8},\ -\frac{5^3\cdot 7\cdot 37\cdot 173^2}{2^6\cdot 3^{10}}\right]$

Table 3. Cardona–Quer invariants for seven of the 46 genus-2 curves with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to E^2, where E has CM by a maximal order $\mathbb{O}$. The discriminant of $\mathbb{O}$ is Δ, the corresponding principal polarization on E^2 is $\varphi_0 \cdot M$, and ω denotes either $\sqrt{\Delta}/2$ or $(1+\sqrt{\Delta})/2$, depending on whether Δ is even or odd.

to explain the prime powers dividing these denominators. An example of such a closed formula appears in the introduction of [RV00] without any details. The denominators of the 33 sets of invariants that we have not proven to be correct also are smooth, which provides some further heuristic evidence that the values are correct.

We present in Table 3 the invariants for a few of the curves we could provably compute.

4B. ***When is $\mathbb{Q}$ also a field of definition for C?*** To conclude let us consider any of the 46 pairs (A, φ). We know that there exists a genus-2 curve $C/\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ such that $(\mathrm{Jac}(C), j) \simeq_{\overline{\mathbb{Q}}} (A, \varphi)$, where j is the canonical polarization on $\mathrm{Jac}(C)$. If the order of $\mathrm{Aut}(A, \varphi) \simeq \mathrm{Aut}(C)$ is larger than 2, then it is known [CQ05] that the field of moduli of C is a field of definition and that there exists a genus-2 curve $C_0 : y^2 = f(x)$ with $f \in \mathbb{Q}[x]$ such that $(\mathrm{Jac}(C_0), j_0) \simeq_{\overline{\mathbb{Q}}} (A, \varphi)$. In particular $\mathbb{Q}$ is also a field of definition for (A, φ).

Proposition 4.1 (compare [RV00, §4]). *The field $\mathbb{Q}$ is a field of definition of C — and thus of (A, φ) — if and only if the order of* $\mathrm{Aut}(A, \varphi) \simeq \mathrm{Aut}(C)$ *is greater than* 2.

Proof. It remains to prove that when $\mathrm{Aut}(A, \varphi) = \{\pm 1\}$, there is no model of (A, φ) over $\mathbb{Q}$. Actually we show there is even no model (B, μ) over $\mathbb{R}$. Indeed, an isomorphism $\psi : (A, \varphi)/\mathbb{C} \to (B, \mu)/\mathbb{R}$, defined

Δ	M	d	equation for C
-8	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 2 \end{pmatrix}$	1	$y^2 = x^5 + x$
-11	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 2 \end{pmatrix}$	$(-11)^{1/3}$	$y^2 = 2x^6 + 11x^3 - 2 \cdot 11$
-19	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 3 \end{pmatrix}$	-19	$y^2 = x^6 + 1026x^5 + 627x^4 + 38988x^3 - 627 \cdot 19x^2 + 1026 \cdot 19^2 x - 19^3$
-43	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 6 \end{pmatrix}$	-43	$y^2 = x^6 + 48762x^5 + 1419x^4 + 4193532x^3 - 1419 \cdot 43x^2 + 48762 \cdot 43^2 x - 43^3$
-67	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 9 \end{pmatrix}$	-67	$y^2 = x^6 + 785106x^5 + 2211x^4 + 105204204x^3 - 2211 \cdot 67x^2 + 785106 \cdot 67^2 x - 67^3$
-163	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 21 \end{pmatrix}$	-163	$y^2 = x^6 + 1635420402x^5 + 5379x^4 + 533147051052x^3 - 5379 \cdot 163x^2 + 1635420402 \cdot 163^2 x - 163^3$
-20	$\begin{pmatrix} 2 & \omega \\ -\omega & 3 \end{pmatrix}$	$\sqrt{5}$	$y^2 = x^5 + 5x^3 + 5x$
-24	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 4 \end{pmatrix}$	$\sqrt{2}$	$y^2 = 3x^5 + 8x^3 + 3 \cdot 2x$
-40	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 6 \end{pmatrix}$	$\sqrt{5}$	$y^2 = 9x^5 + 40x^3 + 9 \cdot 5x$
-52	$\begin{pmatrix} 2 & \omega \\ -\omega & 7 \end{pmatrix}$	$\sqrt{13}$	$y^2 = 9x^5 + 65x^3 + 9 \cdot 13x$
-88	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 12 \end{pmatrix}$	$\sqrt{2}$	$y^2 = 99x^5 + 280x^3 + 99 \cdot 2x$
-148	$\begin{pmatrix} 2 & \omega \\ -\omega & 19 \end{pmatrix}$	$\sqrt{37}$	$y^2 = 441x^5 + 5365x^3 + 441 \cdot 37x$
-232	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 30 \end{pmatrix}$	$\sqrt{29}$	$y^2 = 9801x^5 + 105560x^3 + 9801 \cdot 29x$

Table 4. Genus-2 curves defined over $\mathbb{Q}$ with Jacobian isomorphic over $\overline{\mathbb{Q}}$ to E^2, where E has CM by a maximal order $\mathbb{O}$. The discriminant of $\mathbb{O}$ is Δ, the corresponding principal polarization on E^2 is $\varphi_0 \cdot M$, and ω denotes either $\sqrt{\Delta}/2$ or $(1+\sqrt{\Delta})/2$, depending on whether Δ is even or odd. This list is complete if the generalized Riemann hypothesis holds. Each curve is a double cover of its corresponding E (as can be seen by the fact that the upper-left entry of each polarization matrix is 2), and the associated involution of C is given by $(x, y) \mapsto (d/x, d^{3/2}y/x^3)$ for the value of d given in the third column.

over $\mathbb{C}$, would induce an isomorphism

$$\alpha_\iota = (\psi^{-1})^\iota \circ \psi : (A, \varphi) \to (A, \varphi)^\iota,$$

for the complex conjugation ι, such that ${\alpha_\iota}^\iota \circ \alpha_\iota = ((\psi^{-1}) \circ \psi^\iota) \circ ((\psi^{-1})^\iota \circ \psi) = \mathrm{Id}$.

Since we have seen that $E^\iota = E$, the isomorphism α_ι can be represented as a matrix $P \in \mathrm{GL}_2(\mathbb{O})$ such that $\overline{P}P = \mathrm{Id}$. Moreover the commutativity of the diagram

$$\begin{array}{ccc} E^2 & \xrightarrow{\quad\varphi\quad} & \widehat{E}^2 \\ {\scriptstyle\alpha_\iota}\downarrow & & \uparrow{\scriptstyle\hat{\alpha}_\iota} \\ E^2 & \xrightarrow{\quad\varphi^\iota\quad} & \widehat{E}^2 \end{array}$$

translates into the equality $P^*\overline{M}P = M$. If we denote $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$, then it is easy to see that the matrix $P_0 = \left(\begin{smallmatrix} \bar{b} & d \\ -a & -b \end{smallmatrix}\right)$ satisfies the last equality. Any other $P = P_0R$ differs from P_0 by an automorphism R of (A, φ) since $R^*P^*\overline{M}PR = R^*MR = M$. Because the automorphism group of (A, φ) is $\{\pm 1\}$, this means that the only possible P are $\pm P_0$. It is easy to check that $P_0\overline{P_0} = (-P_0)(-\overline{P_0}) = -\mathrm{Id}$, so the condition $\overline{P}P = \mathrm{Id}$ cannot be satisfied. □

4C. ***Provably correct equations for the curves defined over*** $\mathbb{Q}$**.** Using Proposition 4.1 we found that exactly 13 of our curves can be defined over $\mathbb{Q}$, and these 13 are precisely the curves for which we could provably compute the invariants. This is no coincidence, as having an equation over $\mathbb{Q}$ definitely simplifies the computation. We present these curves in Table 4.

References

[Bai62] Walter L. Baily, Jr., *On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves*, Ann. of Math. (2) **75** (1962), no. 2, 342–381. MR

[BILV16] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent, *Constructing genus-3 hyperelliptic Jacobians with CM*, LMS J. Comput. Math. **19** (2016), suppl. A, 283–300. MR

[BL92] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, Grundlehren der Math. Wissenschaften, no. 302, Springer, 1992. MR

[BS17] Gaetan Bisson and Marco Streng, *On polarised class groups of orders in quartic CM-fields*, Math. Res. Lett. **24** (2017), no. 2, 247–270. MR

[CMSV18] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. (2018).

[CQ05] Gabriel Cardona and Jordi Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., no. 13, World Sci., Hackensack, NJ, 2005, pp. 71–83. MR

[FG18] Francesc Fité and Xavier Guitart, *Fields of definition of elliptic k-curves and the realizability of all genus 2 Sato–Tate groups over a number field*, Trans. Amer. Math. Soc. **370** (2018), no. 7, 4623–4659. MR

[GL07] Eyal Z. Goren and Kristin E. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 2, 457–480. MR

[Hal58] Paul R. Halmos, *Finite-dimensional vector spaces*, 2nd ed., Van Nostrand, Princeton, 1958. MR

[Hay68] Tsuyoshi Hayashida, *A class number associated with the product of an elliptic curve with itself*, J. Math. Soc. Japan **20** (1968), 26–43. MR

[HN65] Tsuyoshi Hayashida and Mieo Nishi, *Existence of curves of genus two on a product of two elliptic curves*, J. Math. Soc. Japan **17** (1965), no. 1, 1–16. MR

[Hof91] Detlev W. Hoffmann, *On positive definite Hermitian forms*, Manuscripta Math. **71** (1991), no. 4, 399–429. MR

[Hoy63] William L. Hoyt, *On products and algebraic families of jacobian varieties*, Ann. of Math. (2) **77** (1963), no. 3, 415–423. MR

[Kan11] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. **62** (2011), no. 3, 297–339. MR

[Kan14] ———, *Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms*, J. Number Theory **139** (2014), 138–174. MR

[Kan16] ———, *The moduli spaces of Jacobians isomorphic to a product of two elliptic curves*, Collect. Math. **67** (2016), no. 1, 21–54. MR

[Kıl16] Pınar Kılıçer, *The CM class number one problem for curves*, Ph.D. thesis, Université de Bordeaux, 2016.

[KLL+18] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng, *Plane quartics over $\mathbb{Q}$ with complex multiplication*, Acta Arith. **185** (2018), no. 2, 127–156. MR

[Koi72] Shoji Koizumi, *The fields of moduli for polarized abelian varieties and for curves*, Nagoya Math. J. **48** (1972), 37–55. MR

[KS15] Pınar Kılıçer and Marco Streng, *The CM class number one problem for curves of genus* 2, preprint, 2015. arXiv

[KW05] Kenji Koike and Annegret Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518. MR

[Lab16] Hugo Labrande, *Explicit computation of the Abel–Jacobi map and its inverse*, Ph.D. thesis, Université de Lorraine, 2016.

[Lan06] Herbert Lange, *Principal polarizations on products of elliptic curves*, The geometry of Riemann surfaces and abelian varieties, Contemp. Math., no. 397, Amer. Math. Soc., Providence, RI, 2006, pp. 153–162. MR

[Lou90] Stéphane Louboutin, *Minorations* (*sous l'hypothèse de Riemann généralisée*) *des nombres de classes des corps quadratiques imaginaires: application*, C. R. Acad. Sci. Paris Sér. I Math. **310** (1990), no. 12, 795–800. MR

[LRS13] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent*, Proceedings of the Tenth Algorithmic Number Theory Symposium—ANTS X, Open Book Ser., no. 1, Math. Sci. Publ., Berkeley, 2013, pp. 463–486. MR

[LS16] Joan-C. Lario and Anna Somoza, *A note on Picard curves of CM-type*, preprint, 2016. arXiv

[LV15] Kristin Lauter and Bianca Viray, *An arithmetic intersection formula for denominators of Igusa class polynomials*, Amer. J. Math. **137** (2015), no. 2, 497–533. MR

[MU01] Naoki Murabayashi and Atsuki Umegaki, *Determination of all $\mathbb{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces*, J. Algebra **235** (2001), no. 1, 267–274. MR

[OU73] Frans Oort and Kenji Ueno, *Principally polarized abelian varieties of dimension two or three are Jacobian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 377–381. MR

[Rit10] Christophe Ritzenthaler, *Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves*, LMS J. Comput. Math. **13** (2010), 192–207. MR

[Ros51] Georg Rosenhain, *Mémoire sur les fonctions de deux variables et à quatre périodes, qui sont les inverses des intégrales ultra-elliptiques de la première classe*, Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut National de France, no. 11, Imprimerie Royale, Paris, 1851, pp. 361–468.

[RV00] Fernando Rodriguez-Villegas, *Explicit models of genus 2 curves with split CM*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., no. 1838, Springer, 2000, pp. 505–513. MR

[Sch89] Peter Schuster, *Produkte elliptischer Kurven der Dimension 2 und 3*, Ph.D. thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, 1989.

[Sch98] Alexander Schiemann, *Classification of Hermitian forms with the neighbour method*, J. Symbolic Comput. **26** (1998), no. 4, 487–508. MR

[Ser01] J.-P. Serre, *Appendice*, Appendix to Kristin Lauter, "Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields", *J. Algebraic Geom.* **10**:1 (2001), 19–36.

[Shi71] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, no. 1, Iwanami Shoten, Tokyo, 1971. MR

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math., no. 151, Springer, 1994. MR

[Spa94] Anne-Monika Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, Ph.D. thesis, Universität Duisburg-Essen, 1994.

[ST61] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, no. 6, Math. Soc. Japan, Tokyo, 1961. MR

[vW99] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320. MR

[Wei57] André Weil, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1957** (1957), 33–53. MR

[Wen01] Annegret Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372. MR

Received 28 Feb 2018. Revised 15 Sep 2018.

ALEXANDRE GÉLIN: alexandre.gelin@uvsq.fr
Laboratoire de Mathématiques de Versailles, Université de Versailles Saint-Quentin-en-Yvelines, Centre national de la recherche scientifique, Université Paris-Saclay, Versailles, France

EVERETT W. HOWE: however@alumni.caltech.edu
Center for Communications Research, Institute for Defense Analyses, San Diego, CA, United States

CHRISTOPHE RITZENTHALER: christophe.ritzenthaler@univ-rennes1.fr
Institut de recherche mathématique de Rennes, Université de Rennes 1, Campus de Beaulieu, Rennes, France

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

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

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

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

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

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

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine