

# A PRYM VARIETY WITH EVERYWHERE GOOD REDUCTION OVER $\mathbb{Q}(\sqrt{61})$

NICOLAS MASCOT, JEROEN SIJSLING, AND JOHN VOIGHT

ABSTRACT. We compute an equation for a modular abelian surface  $A$  that has everywhere good reduction over the quadratic field  $K = \mathbb{Q}(\sqrt{61})$  and that does not admit a principal polarization over  $K$ .

## 1. INTRODUCTION

A foundational theorem of Abrashkin [1] and Fontaine [17] asserts that there is no abelian variety over  $\mathbb{Q}$  with everywhere good reduction; this theorem is an analogue in arithmetic geometry of Minkowski's theorem that every number field has a ramified prime. More generally, the finiteness of the set of isomorphism classes of abelian varieties over a given number field of given dimension and with good reduction outside a given finite set is a key ingredient in the proof of Faltings [15] that a curve of genus at least two defined over a number field has finitely many rational points. For this reason and many others, it remains an important task to explicitly study abelian varieties over number fields with controlled ramification [3, 33].

Moving beyond elliptic curves, Dembélé–Kumar [12] have given examples of abelian surfaces with everywhere good reduction over real quadratic fields. More recently, Dembélé [11] gave a classification of abelian varieties with everywhere good reduction over  $\mathbb{Q}(\sqrt{d})$  with  $d = 53, 61, 73$ : assuming the generalized Riemann hypothesis (GRH), he proves that every such abelian variety is isogenous to the power of a unique abelian surface  $A'_d$ . Moreover, for  $d = 53, 73$  he was able to find an explicit equation for a genus 2 curve whose Jacobian is isogenous to  $A'_d$ . In this article, we finish off the case  $d = 61$  as follows.

**Theorem 1.1.** *Let  $K := \mathbb{Q}(\sqrt{61})$ , let  $\nu := (1 + \sqrt{61})/2$ , and let  $X$  be the projective plane curve over  $K$  defined by the equation  $F(x, y, z) = 0$  where*

$$(1.2) \quad \begin{aligned} F(x, y, z) := & (5\nu + 17)x^4 - (14\nu + 48)x^2y^2 + (8\nu + 28)x^2yz \\ & - (4\nu + 14)x^2z^2 + (10\nu + 33)y^4 - (12\nu + 44)y^3z \\ & + (2\nu + 26)y^2z^2 + (4\nu - 16)yz^3 + (\nu - 6)z^4 \end{aligned}$$

*Then the following statements hold.*

- (a) *The curve  $X$  is smooth of genus 3 and has bad reduction at the prime (2) only.*
- (b) *The curve  $X$  admits an involution  $\iota: (x : y : z) \mapsto (-x : y : z)$  over  $K$ , and the quotient of  $X$  by  $\iota$  defines a map from  $X$  onto an elliptic curve  $E$  of conductor (64). An equation for  $E$  is given by*

$$-(10\nu + 34)y^2 = x^3 - \nu x^2 + (-\nu + 1)x - 1.$$

- (c) *Up to isogeny over  $K$ , we have  $\text{Jac}(X) \sim A \times E$ , where  $A$  is the Prym variety of the natural map  $\text{Jac}(X) \rightarrow \text{Jac}(E)$ , an abelian surface over  $K$  with everywhere good reduction.*
- (d) *All geometric endomorphisms of  $A$  are defined over  $K$ , and  $\text{End}(A) \simeq \mathbb{Z}[\sqrt{3}]$  so  $A$  is of  $\text{GL}_2$ -type over  $K$ . Moreover,  $A$  is isogenous to  $A'_{61}$  over  $K$ .*
- (e) *The abelian surface  $A$  has a polarization over  $K$  of type  $(1, 2)$ , but no abelian surface isogenous to  $A$  over  $K$  admits a principal polarization over  $K$ .*

Although the full classification results of Dembél e are conditional on the GRH, the realization in Theorem 1.1 of the particular abelian surface  $A$  uses a direct computation, making it unconditional.

The abelian surface  $A'_{61}$  arises naturally as an isogeny factor over  $\mathbb{Q}(\sqrt{61})$  of a modular abelian fourfold  $A_{61}$  associated via the Eichler–Shimura construction to the Hecke irreducible space  $S_2(\Gamma_0(61), \chi)$  of classical modular forms of level 61 with quadratic character  $\chi$ , a space having nontrivial inner twist. Shimura [34, p. 210] conjectured and Casselman [9, Theorem 1.1] proved that  $A'_{61}$  has everywhere good reduction (more generally, for good reduction properties of the Jacobians of modular curves, see Katz–Mazur [23, Theorem 14.7.2]). Using the Atkin–Lehner involution and explicit period computations, Demb el e–Kumar [12, Remark 3] observed that  $A'_{61}$  is naturally  $(1, 2)$ -polarized but not principally polarized (using a general criterion of Gonz alez–Gu ardia–Rotger [18]); consequently, this surface was an outlier for their method (the “sole exception” in the range of their computations).

We construct  $X$  as follows. First, we compute the period lattice of the modular abelian fourfold  $A_{61}$  (attached to  $S_2(\Gamma_0(61), \chi)$ ) to large precision. Adapting the methods of Costa–Mascot–Sijlsing–Voight [10], we then numerically split  $A_{61}$  as the square of a simple abelian surface with a  $(1, 2)$ -polarization—a *building block* in the language of Ribet and Pyle [31, 32]—providing a numerical candidate for  $A$ . We then glue with the elliptic curve  $E$  (in Theorem 1.1(b)) via analytic methods to find a curve of genus three over  $K$ , but with a terrible equation. Finally, we simplify the cover to obtain  $X \rightarrow E$  as in Theorem 1.1 and confirm that the Prym of this cover has everywhere good reduction as claimed.

**Contents.** The paper is organized as follows. In Section 2, we explain explicit methods to compute the period matrix of a modular abelian variety to large precision. In Section 3, we illustrate our adapted methods to numerically decompose a complex abelian variety with a focus on our example. In Section 4, we realize the resulting building block as a Prym explicitly; then in Sections 5 we simplify the equations for the curve  $X$  and verify the properties announced in Theorem 1.1.

**Acknowledgments.** The authors would like to thank Lassina Demb el e and the anonymous referees for comments. Sijlsing was supported by a Juniorprofessurprogramm “Endomorphismen algebraischer Kurven” of the Science Ministry of Baden-W urttemberg. Voight was supported by a Simons Collaboration grant (550029). This work was sparked during the conference *Arithmetic of Low-Dimensional Abelian Varieties* at the Institute for Computational and Experimental Research in Mathematics (ICERM) in June 2019; the authors would like to thank ICERM for their hospitality and support.

## 2. COMPUTING THE PERIOD MATRIX

In this section, we show how to compute the period matrix of our modular abelian variety to large precision. We begin by recalling how this variety shows up as a factor in the decomposition up to isogeny of the Jacobian of the modular curve  $X_1(61)$ . After this, we explain how to determine the periods of a newform of weight 2 in terms of its  $q$ -expansion. Finally, we show how to compute many coefficients of this  $q$ -expansion in reasonable time, so as to be able to compute the period matrix with very high accuracy. (The current implementation in MAGMA [6] allows computations to low precision; this is not enough for our purposes.)

**Conventions.** Before we begin, we set up a few conventions we use throughout. Let  $K$  be a field with algebraic closure  $K^{\text{al}}$ . For an abelian variety  $A$  over  $K$ , we denote by  $\text{End}(A)$  the endomorphisms of  $A$  defined over  $K$ ; if we wish to consider endomorphisms over a field extension  $L \supseteq K$ , we write  $A_L$  for the base change of  $A$  to  $L$  and write  $\text{End}(A_L)$  for endomorphisms over  $L$ .

**Setup.** Let  $k \in \mathbb{Z}_{\geq 0}$  and  $n, N \in \mathbb{Z}_{>0}$  be integers. We denote by  $\sigma_k(n) := \sum_{d|n} d^k$  the sum of the  $k$ -th powers of the positive divisors of  $n$ . In particular,  $\sigma_0(n)$  is the number of divisors of  $n$ .

Given a subgroup  $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ , let

$$\Gamma_H(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \text{ and } a, d \pmod{N} \in H \right\}.$$

By a **newform** of level  $\Gamma_H(N)$ , we mean a newform of level  $\Gamma_1(N)$  whose nebentypus character  $\varepsilon: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  satisfies  $H \leq \ker \varepsilon$ . Let  $\mathcal{N}_k(\Gamma_H(N))$  denote the finite set of newforms of weight  $k$  and level  $\Gamma_H(N)$ . This set is acted on (the left) by  $\text{Gal}_{\mathbb{Q}}$ , the absolute Galois group of  $\mathbb{Q}$ , via the coefficients of  $q$ -expansions at the cusp  $\infty$ : if  $f(q) = \sum_{n=1}^{\infty} a_n(f)q^n$  lies in  $\mathcal{N}_k(\Gamma_H(N))$ , so that in particular  $a_1 = 1$ , then the coefficients  $\{a_n(f)\}_n$  are algebraic integers, and for  $\tau \in \text{Gal}_{\mathbb{Q}}$  we have  $\tau f \in \mathcal{N}_k(\Gamma_H(N))$  with  $q$ -expansion  $(\tau f)(q) = \sum_n \tau(a_n(f))q^n$ . Let  $\text{Gal}_{\mathbb{Q}} \backslash \mathcal{N}_k(\Gamma_H(N))$  be the set of Galois orbits of  $\mathcal{N}_k(\Gamma_H(N))$ . For each  $f \in \mathcal{N}_k(\Gamma_H(N))$ , we denote by  $K_f := \mathbb{Q}(\{a_n(f)\}_n)$  the number field generated by the coefficients of  $f$ . The field  $K_f$  contains the values of the nebentypus character  $\varepsilon_f$  of  $f$ ; furthermore the nebentypus of  $\tau(f)$  is  $\varepsilon_{\tau(f)} = \tau \circ \varepsilon_f$  for all  $\tau \in G_{\mathbb{Q}}$ .

Let  $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$  denote the completed upper half-plane. Recall that for  $N \in \mathbb{Z}_{>0}$  and  $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ , the modular curve  $X_H(N) := \Gamma_H(N) \backslash \mathcal{H}^*$  attached to the congruence subgroup  $\Gamma_H(N)$  is defined over  $\mathbb{Q}$ , and its Jacobian  $J_H(N)$  decomposes up to isogeny over  $\mathbb{Q}$  as

$$(2.1) \quad J_H(N) \sim \prod_{M|N} \prod_{f \in \mathcal{N}_2(\text{Gal}_{\mathbb{Q}} \backslash \Gamma_{H_M}(M))} A_f^{\sigma_0(N/M)},$$

where  $H_M \leq (\mathbb{Z}/M\mathbb{Z})^\times$  denotes the image of  $H$  in  $(\mathbb{Z}/M\mathbb{Z})^\times$ . Moreover, for each Galois orbit  $f \in \text{Gal}_{\mathbb{Q}} \backslash \mathcal{N}_2(\Gamma_H(N))$ , the abelian variety  $A_f$  is simple over  $\mathbb{Q}$  with  $\dim A_f = [K_f : \mathbb{Q}]$ , and  $A_f$  has endomorphism algebra  $\text{End}(A_f) \otimes \mathbb{Q} \simeq K_f$ .

Let  $\mathbb{T}$  be the Hecke algebra of weight 2 and level  $\Gamma_H(N)$ . Roughly speaking,  $A_f$  can be thought of as the piece of  $J_H(N)$  on which  $\mathbb{T}$  acts with the same eigenvalue system as  $f$ .

More precisely,  $A_f$  is defined by

$$(2.2) \quad A_f := J_1(N)/I_f J_1(N),$$

where  $I_f := \{T \in \mathbb{T} : Tf = 0\}$  is the annihilator of  $f$  under  $\mathbb{T}$ , so that for instance the image of  $T_n|_{A_f} \in \text{End}(A_f)$  under the isomorphism  $\text{End}(A_f) \otimes \mathbb{Q} \simeq K_f$  is the coefficient  $a_n(f) \in K_f$ . In particular, up to isogeny, the matrix

$$\begin{pmatrix} & & \vdots & & \\ \cdots & \int_{\gamma_j} \tau(f)(z) dz & \cdots & & \\ & & \vdots & & \end{pmatrix}$$

whose rows are indexed by the newforms  $\tau(f)$  in the Galois orbit of  $f$  and whose columns are indexed by a  $\mathbb{Z}$ -basis  $(\gamma_j)_j$  of

$$H_1(X_H(N), \mathbb{Z})[I_f] = \{\gamma \in H_1(X_H(N), \mathbb{Z}) : T\gamma = 0 \text{ for all } T \in I_f\}$$

is a period matrix of  $A_f$ .

It is therefore possible to extract a period matrix of  $A_f$  out of a period matrix of the modular curve  $X_H(N)$ . While it may seem excessive to work with the periods of the whole Jacobian  $J_H(N)$  instead of  $A_f$ , this approach presents the advantage of making it easy to compute explicitly in the  $\mathbb{T}$ -module  $H_1(X_H(N), \mathbb{Z})$  using modular symbols.

**Our modular Jacobian factor.** In what follows, we use LMFDB [26] labels for our classical modular forms. In our case, we observe that the Galois orbit of newforms attached to  $A_{61}$  is

$$f := \text{61.2.b.a} = q + \alpha q^2 + (\alpha^2 + 3)q^3 + O(q^4)$$

where  $\alpha^4 + 8\alpha^2 + 13 = 0$ ; the four newforms in this orbit correspond to the four embeddings of  $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ , and their nebentypus is the quadratic character  $\chi_{61}$ . Thus  $N = 61$  and  $H = \ker \chi_{61}$ , the subgroup of squares of  $(\mathbb{Z}/61\mathbb{Z})^\times$ .

This Galois orbit [61.2.b.a](#) happens to be the only one with quadratic nebentypus, whereas there are two Galois orbits with trivial nebentypus, namely

$$\text{61.2.a.a} = q - q^2 - 2q^3 + O(q^4)$$

whose coefficient field is  $\mathbb{Q}$ , and

$$\text{61.2.a.b} = q + \beta q^2 + (-\beta^2 + 3)q^3 + O(q^4)$$

whose coefficient field is  $\mathbb{Q}(\beta)$  where  $\beta^3 - \beta^2 - 3\beta + 1 = 0$ . Since 61 is prime and since there are no cuspforms of weight 2 and level 1, the decomposition (2.1) informs us that  $J_H(61)$  is isogenous to the product of an elliptic curve corresponding to [61.2.a.a](#), an abelian 3-fold corresponding to [61.2.a.b](#), and our 4-fold  $A_{61}$  corresponding to [61.2.b.a](#). It also follows that the modular curve  $X_H(61)$  has genus 8, which is reasonable for practical computations.

In order to compute the period lattice of  $A_{61}$ , we must first isolate the rank-8 sublattice  $H_1(X_H(61), \mathbb{Z})[I]$  of the rank-16 lattice  $H_1(X_H(61), \mathbb{Z})$ , where  $I \leq \mathbb{T}$  is the annihilator of [61.2.b.a](#). We can obtain this sublattice as

$$H_1(X_H(61), \mathbb{Z})[I] = \bigcap_{T \in I} \ker(T|_{H_1(X_H(61), \mathbb{Z})}).$$

We observe that the Hecke operator  $T_2^4 + 8T_2^2 + 13$  lies in  $I$ , since  $T_2 f = a_2(f)f = \alpha f$  and  $\alpha^4 + 8\alpha^2 + 13 = 0$ ; furthermore, the kernel of this operator acting on  $H_1(X_H(61), \mathbb{Z})$  happens to have rank 8, so that it agrees with the sublattice  $H_1(X_H(61), \mathbb{Z})[I]$ .

*Remark 2.3.* The fact that the hunt for this sublattice was so short-lived is not a coincidence. Indeed, since 61 is prime and since there is no cuspform of weight 2 and level 1, all the eigenforms of level 61 are new, so that  $\mathbb{T} \otimes \mathbb{Q}$  is a semi-simple  $\mathbb{Q}$ -algebra by the multiplicity-one theorem. It is therefore étale, so that most of its elements generate it as a  $\mathbb{Q}$ -algebra; in fact, an element of  $\mathbb{T} \otimes \mathbb{Q}$  is a generator if and only if its eigenvalues on each of the Galois conjugates of [61.2.a.a](#), [61.2.a.b](#), and [61.2.b.a](#) are all distinct. In particular, it is not surprising to find that  $\mathbb{T} \otimes \mathbb{Q} = \mathbb{Q}[T_2]$ , so that  $I \otimes \mathbb{Q}$  is generated by  $T_2^4 + 8T_2^2 + 13$ , which explains why taking the kernel of this operator led us directly to the correct sublattice.

**Twisted winding elements.** We now recall a formula that we will use to compute the periods  $\int_\gamma f(z) dz$  of a newform  $f \in \mathcal{N}_2(\Gamma_H(N))$  for  $\gamma$  ranging over a  $\mathbb{Z}$ -basis of  $H_1(X_H(N), \mathbb{Z})$ .

Since  $f$  is an eigenform, it is actually enough to compute these integrals for  $\gamma$  ranging over a generating set of  $H_1(X_H(N), \mathbb{Z})$  as a  $\mathbb{T}$ -module, since

$$\int_{T\gamma} f(z) dz = \int_\gamma (Tf)(z) dz = \lambda_T(f) \int_\gamma f(z) dz$$

for all  $T \in \mathbb{T}$ , where  $\lambda_T(f)$  is such that  $Tf = \lambda_T(f)f$ .

Our strategy consists in integrating term-by-term the  $q$ -expansion of  $f$  along modular symbols chosen so that the resulting series has good convergence properties. We choose to use the so-called *twisted winding elements*, that is to say modular symbols of the form

$$s_\chi = \sum_{a \bmod m} \bar{\chi}(-a) \{\infty, a/m\}$$

where  $\chi$  is a primitive Dirichlet character whose modulus  $m$  is coprime to  $N$ .

Indeed, let  $\varepsilon_f$  be the nebentypus of  $f$ , and  $\lambda_f \in \mathbb{C}^\times$  be the Fricke pseudo-eigenvalue of  $f$ , i.e.

$$(2.4) \quad f \left| \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \right. = \lambda_f \sum_{n=1}^{\infty} \overline{a_n(f)} q^n;$$

if  $N$  is squarefree, the exact value of  $\lambda_f$  can be read off the coefficients  $a_n(f)$  of  $f$  [[30](#), Theorem 2.2.1]; in any case, a numerical approximation of  $\lambda_f$  can be obtained by evaluating (2.4) at a particular point of the upper half plane. A computation [[30](#), Proposition 3.2.3] based on the fact that the twist  $f \otimes \chi := \sum_{n=1}^{\infty} a_n(f) \chi(n) q^n$  of  $f$  by  $\chi$  is modular of level  $m^2 N$  and on the identity

$$\int_{\infty}^0 = \int_{\infty}^{\frac{i}{m\sqrt{N}}} + \int_{\frac{i}{m\sqrt{N}}}^0$$

yields the formula

$$(2.5) \quad \int_{s_\chi} f(z) dz = \frac{m}{2\pi i} \sum_{n=1}^{\infty} \frac{1}{n} \left( \frac{\chi(n) a_n(f)}{\mathfrak{g}(\chi)} - \chi(-N) \varepsilon_f(m) \lambda_f \frac{\overline{\chi(n) a_n(f)}}{\mathfrak{g}(\bar{\chi})} \right) R^n$$

where  $R := e^{-2\pi/m\sqrt{N}}$  and  $\mathbf{g}(\chi)$  denotes the Gauss sum

$$\mathbf{g}(\chi) := \sum_{a \in \mathbb{Z}/m\mathbb{Z}} \chi(a) e^{2a\pi i/m}$$

of  $\chi$  (and the same with  $\bar{\chi}$ ).

In view of the Deligne bound  $a_n(f) \ll n^{\frac{1}{2}+\varepsilon}$ , it is necessary to sum numerically the series (2.5) up to  $n \approx \frac{m\sqrt{N} \log 10}{2\pi} D$  in order to compute this integral with  $D$  correct decimal digits. For instance, the homology of the curve  $X_H(61)$  introduced above happens to be generated as a  $\mathbb{T}$ -module by the  $s_\chi$  for  $\chi$  ranging over the set of primitive characters of modulus  $m \leq 7$ ; therefore, in order to compute the period lattice of  $A_{61}$  with 1000 digits of accuracy, we need to compute the coefficients  $a_n(f)$  for  $n$  up to approximately 20000. We show how this can be done in reasonable time below.

*Remark 2.6.* For safety, we actually computed the coefficients  $a_n(f)$  and summed the series up to  $n \leq 24000$ . This 20% increase is quite arbitrary, but at this point we do not need to have a very tight control over the accuracy of our computations. Note that since we sum the series (2.5) using floating-point arithmetic and since its terms are roughly geometrically decreasing in magnitude, summing them in reverse (from  $n = 24000$  to  $n = 1$ ) increases numerical stability.

**High-accuracy  $q$ -expansions.** Classical algorithms, such as that based on modular symbols or that based on trace formulas for Hecke operators, compute the coefficients  $a_n(f)$  of a newform for  $n \leq B$  in complexity which is at least quadratic in  $B$ . Since we are aiming for  $B = 24000$ , these algorithms are not suitable for our purpose. We therefore turn to the method presented by Mascot [29, 3.1], which can compute the first  $B$  coefficients  $a_n(f)$  in complexity which is quasi-linear in  $B$ .

This method is based on the observation that any two rational functions  $u$  and  $v$  on an algebraic curve  $X$  are necessarily algebraically dependent, since the transcendence degree of the function field of  $X$  is only 1. There must therefore exist a polynomial  $\Phi(x, y)$  satisfying  $\Phi(u, v) = 0$ . Besides, this polynomial can be taken to have degree at most  $\deg v$  in  $x$  and  $\deg u$  in  $y$ ; indeed, a given value of  $u$  generically corresponds to  $\deg u$  points of  $X$ , which in turn yield at most  $\deg u$  values of  $v$ .

Let  $f \in \mathcal{N}_k(\Gamma_H(N))$ , let  $K_f$  be its coefficient field, and let  $\mathcal{O}_f$  be the ring of integers of  $K_f$ . Our method thus consists in using such a relation between the inverse of the  $j$ -invariant

$$(2.7) \quad u := 1/j = \frac{E_4^3 - E_6^2}{(12E_4)^3} \in q\mathbb{Z}[[q]]$$

where

$$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n, \quad E_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)q^n,$$

and the rational function  $v := f/u' \in \mathcal{O}_f[[q]]$  where  $u' := q du/dq$ .

The first  $B$  coefficients of  $u$  can be computed in quasi-linear complexity in  $B$  using the sieve of Eratosthenes and fast series arithmetic, and we can then determine the first  $B$  coefficients of  $v$  and hence of  $f = vu'$  by Newton iteration using  $\Phi(u, v) = 0$ .

In order to increase the efficiency of this computation, we run it modulo a large enough prime number  $p$  which splits completely in the coefficient field  $K_f$  of  $f$ . More precisely,

let  $(\omega_j)_{j \leq [K_f:\mathbb{Q}]}$  be a  $\mathbb{Z}$ -basis of  $\mathcal{O}_f$ , so that each element of  $\mathcal{O}_f$  may be uniquely written as  $\sum_j \lambda_j \omega_j$  with  $\lambda_j \in \mathbb{Z}$  for all  $j$ . The matrix

$$\begin{pmatrix} & \vdots & \\ \cdots & \tau(\omega_j) & \cdots \\ & \vdots & \end{pmatrix}$$

whose rows (resp. columns) are indexed by the complex embeddings  $\tau : K_f \hookrightarrow \mathbb{C}$  (resp. the integers  $1 \leq j \leq [K_f:\mathbb{Q}]$ ) is square, and invertible since the square of its determinant is the discriminant of  $K_f$ . Let  $(c_{j,\tau})_{j,\tau}$  be the coefficients of its inverse, and define

$$C := \max_j \sum_{\tau} |c_{j,\tau}|.$$

Then for all  $r > 0$  and for any element  $\theta = \sum_j \lambda_j \omega_j \in \mathcal{O}_f$ , we have

$$(2.8) \quad |\tau(\theta)| \leq r \text{ for all } \tau : K_f \hookrightarrow \mathbb{C} \implies |\lambda_j| \leq Cr \text{ for all } j.$$

Since for all  $n \in \mathbb{Z}_{\geq 1}$ , the coefficient  $a_n(f) \in \mathcal{O}_f$  has absolute value at most  $\sigma_0(n)\sqrt{n}$  under every embedding  $\tau : K_f \hookrightarrow \mathbb{C}$ , if we require that

$$(2.9) \quad p \geq 1 + 2C \max_{n \leq B} \sigma_0(n)\sqrt{n},$$

then for all  $n \leq B$  we can recover the exact value of  $a_n(f) = \sum_j \lambda_{j,n} \omega_j$  from the  $\lambda_{j,n} \pmod p$ , since we will always have  $p \geq 2|\lambda_{j,n}| + 1$ .

Our method is summarized in Algorithm 2.10; for more detail, see Mascot [29, 3.1], [30, 3.3].

---

**Algorithm 2.10.** High-accuracy  $q$ -expansion in quasi-linear time

---

**Input:** A newform  $f$  and  $B \in \mathbb{Z}_{\geq 1}$ .

**Output:** The coefficients  $a_n(f)$  for  $n \leq B$ .

**Algorithm:**

1. Evaluate the degrees of the rational functions  $u = 1/j$  and  $v = f/u'$  (where  $u' = q \, dq/du$ ) on the modular curve  $X_H(N)$  in terms of the index  $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H(N)]$  and of the ramification of the  $j$ -invariant map.
2. Use Riemann-Roch to find a bound  $b \in \mathbb{Z}_{\geq 1}$  such that any linear combination of the  $u^m v^n$  with  $m \leq \deg v$  and  $n \leq \deg u$  whose first  $b$   $q$ -expansion coefficients vanish is necessarily the 0 function.
3. Compute the coefficients  $a_n(f)$  for  $n \leq b$  using one of the quadratic algorithms mentioned above.
4. Pick a prime  $p$  satisfying (2.9) and which splits completely in  $K_f$ , and compute the first  $B$  coefficients of  $u \pmod p$  using fast series arithmetic in  $\mathbb{F}_p[[q]]$ .
5. For each prime  $\mathfrak{p} \mid p$  of  $K_f$ , in parallel:
  - a. By linear algebra, find coefficients  $a_{m,n} \in \mathbb{F}_{\mathfrak{p}}$  such that the first  $b$  coefficients of

$$\sum_{m \leq \deg v} \sum_{n \leq \deg u} a_{m,n} u^m v^n$$

are all 0 mod  $\mathfrak{p}$ , and define

$$\Phi_{\mathfrak{p}}(x, y) = \sum_{m \leq \deg v} \sum_{n \leq \deg u} a_{m,n} x^m y^n \in \mathbb{F}_{\mathfrak{p}}[x, y].$$

- b. Use Newton iteration in  $\mathbb{F}_{\mathfrak{p}}[[q]]$  over the second variable of the equation  $\Phi_{\mathfrak{p}}(u, v) = 0 \pmod{\mathfrak{p}}$  to find the first  $B$  coefficients of  $v \pmod{\mathfrak{p}}$ .
6. Use CRT over the primes  $\mathfrak{p}$  to determine the first  $B$  coefficients of  $v \pmod{p\mathcal{O}_f}$ .
7. Express the first  $B$  coefficients of  $f = vu' \pmod{p\mathcal{O}_f}$  on the  $\mathbb{Z}/p\mathbb{Z}$ -basis  $(\omega_j)_{j \leq [K_f:\mathbb{Q}]}$  of  $\mathcal{O}_f/p\mathcal{O}_f$ , and deduce their exact value thanks to Deligne's bounds.

*Remark 2.11.* Although the complexity of this method is quasilinear in  $B$ , the initial computation of the  $a_n(f)$  for  $n \leq b$  and the linear algebra required to find the coefficients  $a_{m,n}$  of  $\Phi_{\mathfrak{p}}(x, y)$  represent a significant overhead if the degrees of  $u$  and  $v$  are large. In our case, it is more efficient to proceed as follows:

- (i) Compute the first  $B$  coefficients of the newform  $f_0 = \text{61.2.a.a} = q - q^2 - 2q^3 + O(q^4)$  introduced above using algorithm 2.10. This is faster than for  $f$ , since  $f_0$  has trivial nebentypus, so that instead of  $X_H(61)$ , we can work on the curve  $X_0(61)$ , where the degree of  $u = 1/j$  is smaller.
- (ii) Compute the first  $B$  coefficients of  $f$  using a variant of Algorithm 2.10 based on a relation between the functions  $u = 1/j$  and  $v = (f/f_0)^2$ . Since the nebentypus of  $f$  has order 2, this can again be done on the curve  $X_0(61)$ .

In general, if we wanted the coefficients of more modular forms (e.g., the other newform 61.2.a.b of trivial nebentypus), it is better to proceed inductively by replacing the  $j$ -invariant with forms that have already been computed (such as  $f_0$  and  $f$ ), since this leads to polynomials  $\Phi_{\mathfrak{p}}(x, y)$  of much lower degree [30, 3.3].

Using this method, we can obtain the coefficients  $a_n(f)$  for  $n \leq 24000$  as elements of  $K_f = \mathbb{Q}(\alpha)$ , where  $\alpha^4 + 8\alpha^2 + 13 = 0$ . We then deduce the complex coefficients of each of the newforms  $\tau(f)$  in the Galois orbit of  $f$  by applying each of the complex embeddings of  $K_f$  to these coefficients. It then remains to evaluate the integrals  $\int_{s_{\chi}} \tau(f)(z) dz$  using (2.5), and then to extract the periods of our abelian 4-fold  $A_{61}$ , as explained at the beginning of this section.

### 3. ISOLATING THE BUILDING BLOCK

The result of the algorithms in the previous sections is a  $4 \times 8$  period matrix  $\Pi \in M_{4,8}(\mathbb{C})$  with respect to some basis of the homology of the corresponding abelian 4-fold  $A_{61}$ . In this section, we find the period sublattice corresponding to an abelian surface as isogeny factor.

**Finding a polarization.** The homology basis used for the period computations in the previous section need not, in general, be symplectic. Indeed, the computation of the intersection pairing on the homology of a modular curve is currently implemented only for the case of  $X_0(N)$ . Therefore, we start this section by briefly describing how to numerically recover a polarization for  $\Pi$ .

*Remark 3.1.* Dembélé–Kumar [12, §4.1.1, Method 1] showed that when the character is quadratic (as in our case), the Atkin–Lehner involution splits the modular abelian variety,



giving a polarization whose degree is a power of 2. In cases where the resulting polarization is not principal, they search (in the Hecke algebra) for a suitable principal polarization, so the method we give can be seen as a more general version of this approach.

More generally, let  $\Pi \in M_{g,2g}(\mathbb{C})$  be a period matrix, with corresponding abelian variety  $A = V/\Lambda$ , where  $V = \mathbb{C}^g$  and  $\Lambda = \Pi\mathbb{Z}^{2g}$ . Having  $\Pi$  at our disposal yields an identification of the homology group  $H_1(A, \mathbb{Z})$  with  $\mathbb{Z}^{2g}$ . Multiplication by  $i$  on  $A$  yields an endomorphism  $J$  of  $H_1(A, \mathbb{R})$ , which we similarly identify with the unique matrix  $J \in M_{2g}(\mathbb{R})$  obtained from the equality [2, §6.1]

$$(3.2) \quad i\Pi = \Pi J.$$

Via the above identification and the Riemann relations [5, 4.2.1], finding a polarization for  $A$  comes down to finding an alternating matrix  $E \in M_{2g}(\mathbb{Z})$  satisfying  $J^t E J = E$  (where  ${}^t$  denotes transpose) and the positive definiteness condition  $i\Pi E^{-1} \Pi^* > 0$  (where  $*$  denotes the conjugate transpose).

We first focus on the linear equations

$$(3.3) \quad \begin{aligned} E^t &= -E \\ J^t E J &= E. \end{aligned}$$

Let  $m = g(2g - 1)$ . We choose a  $\mathbb{Z}$ -basis of size  $m$  of alternating matrices  $M_{2g}(\mathbb{Z})_{\text{alt}}$  (e.g., indexed by entries above the diagonal). Numerically solving the equations (3.3) then reduces to finding common approximate zeros of a number of linear forms  $\ell_1, \dots, \ell_m : \mathbb{Z}^m \rightarrow \mathbb{R}$ . We determine a  $\mathbb{Z}$ -basis of vectors  $v$  for which all  $\ell_i(v)$  are numerically negligible by LLL-reducing the lattice spanned by the rows of the matrix

$$(3.4) \quad \left( \begin{array}{c|ccc|c} I_m & C\ell_1 & \cdots & C\ell_m \\ \hline \end{array} \right).$$

Here  $I_m$  is the  $m$ -by- $m$  identity matrix, and the other columns correspond to the linear forms  $\ell_i$  multiplied by a sufficiently large scalar  $C \in \mathbb{R}_{\gg 0}$ . The first elements of the resulting LLL-reduced basis will give approximate solutions of (3.3), and we preserve those that do so to large enough precision to get a  $\mathbb{Z}$ -basis of numerical solutions for (3.3).

Having found a  $\mathbb{Z}$ -basis of solutions of (3.3), we take small linear combinations until we find an element  $E$  of determinant 1 such that the Hermitian matrix  $i\Pi E^{-1} \Pi^*$  is positive definite. We summarize our steps in Algorithm 3.5.

---

**Algorithm 3.5.** Numerically recovering principal polarizations

---

**Input:** A period matrix  $\Pi \in M_{g,2g}(\mathbb{C})$ , not necessarily with respect to a symplectic basis.

**Output:** An alternating matrix  $E \in M_{2g}(\mathbb{Z})$  defining a principal polarization for the abelian variety corresponding to  $\Pi$ .

**Algorithm:**

1. Use LLL to find a  $\mathbb{Z}$ -basis  $\{E_1, \dots, E_d\}$  of solutions of (3.3) in  $M_{2g}(\mathbb{Z})_{\text{alt}}$ .
  2. Take a (random)  $\mathbb{Z}$ -linear combination  $E = \sum_{i=1}^d c_i E_i$ , with  $c_i \in \mathbb{Z}$ .
  3. If  $\det(E) = 1$  and  $i\Pi E^{-1} \Pi^*$  is positive definite, return  $E$ ; else, return to Step 2.
- 

In this way, we quickly recover a principal polarization  $E$  on  $\Pi$ .

*Remark 3.6.* More generally, this method can be used to search for polarizations of any desired type.

For our modular abelian fourfold  $A = A_{61}$ , whose period matrix  $\Pi \in M_{4,8}(\mathbb{C})$  was computed in the previous section, we carry out Algorithm 3.5 and recover (numerically) a principal polarization on  $A$ .

**Finding small idempotents.** With a polarization in hand, we numerically decompose the abelian variety  $A = A_{61}$ , following Costa–Mascot–Sijlsing–Voight [10]: we compute numerically that  $\text{End}(A_{\mathbb{C}})$  is an order of index 13 in  $M_2(\mathbb{Z}[\sqrt{3}])$ . Using methods similar to those above, we find a  $\mathbb{Z}$ -basis  $\{(T_1, R_1), \dots, (T_8, R_8)\}$  for the pairs  $(T, R)$  with  $T \in M_4(\mathbb{C})$  and  $R \in M_8(\mathbb{Z})$  such that numerically

$$(3.7) \quad T\Pi = \Pi R.$$

Specifically,  $R_1 = 1$ , and the remaining matrices  $R_i$  are

$$\begin{pmatrix} -1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 & 1 & -1 & 2 & 0 \\ 1 & 0 & 0 & 0 & -1 & 1 & 0 & 2 \\ -1 & 0 & -1 & 0 & -1 & -1 & -1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ -1 & 0 & -1 & -1 & -1 & -2 & -1 & -2 \\ -1 & 0 & -1 & 0 & -1 & -1 & -1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} -2 & 0 & -1 & 0 & 0 & -2 & -1 & -2 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 \\ -1 & -1 & -1 & -2 & -1 & 0 & 0 & 0 \\ 0 & -1 & -2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & -1 & 2 & 1 & 2 \\ -1 & -1 & -1 & 0 & -1 & 0 & -1 & 0 \\ -1 & -1 & 0 & 1 & 1 & -2 & 0 & 0 \\ 1 & 2 & 2 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -2 & -1 & 0 & -1 & -2 \\ -10 & -1 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & -2 & 0 & 0 & -1 & -3 \end{pmatrix}, \\ \begin{pmatrix} -1 & 0 & 0 & -1 & 0 & -2 & -1 & -2 \\ 0 & 0 & -1 & -2 & -1 & 1 & -2 & -1 \\ 0 & -1 & -1 & 1 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & -1 & -1 & 0 & -1 & -1 \\ -1 & 0 & 0 & 1 & 0 & 1 & 1 & 2 \\ -1 & -1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & -1 & 0 & 0 & -1 & -2 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -2 & -1 & -1 & -1 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -1 & 0 & 0 & 1 \\ 2 & 0 & 2 & 1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 \\ -2 & 0 & -2 & -2 & -1 & -2 & -1 & -3 \\ 1 & 0 & 1 & 1 & 0 & 1 & -1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & -2 & 1 & 1 & -2 & -3 \\ -3 & -1 & -2 & -1 & -1 & -2 & -2 & -3 \\ 2 & -1 & 0 & -1 & -1 & 2 & 0 & 1 \\ -1 & 1 & -1 & 1 & -1 & 0 & 1 & 1 \\ -1 & -1 & -1 & 0 & -2 & 1 & 0 & 2 \\ 1 & -1 & 2 & 1 & 0 & 0 & -1 & 1 \\ -1 & 2 & 0 & 0 & 2 & -1 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & -2 & 0 & -2 & -2 & -3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & -1 & 0 & -1 \\ -3 & -1 & -1 & 1 & -1 & 3 & 1 & 3 \\ 0 & 0 & 1 & 2 & 1 & 1 & 2 & 2 \\ 2 & -1 & 1 & 1 & 1 & -3 & 1 & -1 \\ -1 & 0 & -2 & -2 & -2 & 2 & -2 & 0 \end{pmatrix}.$$

The matrices  $R_i$  are a  $\mathbb{Z}$ -basis for the numerical endomorphism ring  $\text{End}(A_{\mathbb{C}}) \subset M_8(\mathbb{Z})$ ; we look for small idempotents therein as follows. Inspired by algorithms for computing an isomorphism with the matrix ring [16, 22], we equip  $M_8(\mathbb{Z})$  with the Frobenius norm (sum of squares of entries)  $N: M_8(\mathbb{Z}) \rightarrow \mathbb{Z}$ , a positive definite quadratic form; then idempotents (and, more generally, zerodivisors) are likely to be short vectors with respect to this norm. This very quickly identifies scores of idempotents

$$(3.8) \quad R_2 + 1, R_4 + 1, R_2 - R_3 + 1, R_8, \dots$$

and we select one that gives us the simplest looking decomposition.

**Inducing the polarization.** Let  $(T, R)$  be a small idempotent in  $\text{End}(A_{\mathbb{C}}) \otimes \mathbb{Q}$  as constructed above. We can then find an isogeny factor of  $A$  in two ways:

- (i) Taking the kernel of  $T$  yields a linear subspace of  $W$  of  $\mathbb{C}^g$  in which  $W \cap \Pi\mathbb{Z}^{2g}$  is a lattice. Choosing bases, we get a new period matrix  $\Pi'$  as well as a pair abusively still denoted  $(T, R)$  such that  $T\Pi' = \Pi R$ . The matrix  $T$  represents the *inclusion* of  $W \cong \mathbb{C}^{\dim(W)}$  into  $V \cong \mathbb{C}^g$ .
- (ii) Alternatively, taking the image of  $T$  yields a linear subspace of  $W$  of  $\mathbb{C}^g$  in which  $T\Pi\mathbb{Z}^{2g}$  is a lattice. Choosing bases, we get a new period matrix  $\Pi'$  as well as a pair abusively still denoted  $(T, R)$  such that  $T\Pi = \Pi'R$ . The matrix  $T$  represents the *projection* from  $V \cong \mathbb{C}^g$  to  $W \cong \mathbb{C}^{\dim(W)}$ .

Note that the dimensions of the abelian varieties  $W$  in approaches (i) and (ii) above are complementary in the sense that they sum to  $g$ .

**Proposition 3.9.** *In approach (i), the restriction of  $E$  to  $W$  is represented by the matrix  $E' := R^t E R$ , and  $E'$  defines a polarization for  $\Pi'$ .*

*Proof.* It is clear that  $E'$  is alternating. The complex structure  $J$  restricts to give the complex structure on  $W$ , in the sense that because  $T\Pi' = \Pi R$  we have

$$(3.10) \quad \Pi R J' = T \Pi' J' = i T \Pi' = i \Pi R = \Pi J R,$$

so that  $R J' = J R$ . Therefore  $E'$ , as the restriction of  $E$  under  $R$ , is again compatible with  $J'$ , or more precisely

$$(3.11) \quad J'^t E' J' = J'^t R^t E R J' = R^t J^t E J R = R^t E R = E'.$$

Similarly, since  $E'$  is the restriction of  $E$  under  $R$ , the corresponding Hermitian form on  $W$  remains positive definite, which is equivalent to  $i\Pi'E'^{-1}\Pi'^* > 0$  (as in Birkenhake–Lange [5, Proof of Lemma 4.2.3]).  $\square$

**Proposition 3.12.** *In approach (ii), an integer multiple of  $E' := (R E^{-1} R^t)^{-1}$  induces a polarization on  $\Pi'$ .*

*Proof.* This follows from the previous proposition by double duality. The projection  $(T, R)$  induces a dual map  $(T^\vee, R^\vee) : (A')^\vee \rightarrow A^\vee$  on the corresponding dual abelian varieties. Recall that we can identify  $A^\vee = V^\vee/\Lambda^\vee$ , where  $V^\vee := \text{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$  is the set of antilinear maps from  $V$  to  $\mathbb{C}$  and where  $\Lambda^\vee$  is the dual of  $\Lambda$  under the canonical pairing between  $V$  and  $V^\vee$ . The original pairing  $E$  gives rise to a map  $V \rightarrow V^\vee$  sending the lattice  $\Lambda$  into its antilinear dual  $\Lambda^*$ . In other words, we have

$$(3.13) \quad E(\Lambda \otimes \mathbb{Q}) = \Lambda^\vee \otimes \mathbb{Q}.$$

Therefore a suitable multiple of the inverse map  $E^{-1} : V^\vee \rightarrow V$  maps  $\Lambda^\vee$  into its dual  $\Lambda$ . This defines a polarization on  $A^\vee$ ; it is compatible with the complex structure because  $E$  is, and it is positive definite for the same reason. We can transfer this polarization to  $A^\vee$  by the previous proposition, using the inclusion  $(T^\vee, R^\vee)$  dual to the projection  $(T, R)$ . Note that  $R^\vee = R^t$  by duality. Dualizing a second time, we get our induced polarization on  $A'$  after again taking a suitable integral multiple if needed.  $\square$

*Remark 3.14.* If the morphism  $(T, R)$  in the previous proposition corresponds to a map of curves of degree  $d$  under the Torelli map, then  $E'$  is in fact  $d$  times the principal polarization on  $\Pi'$  by Birkenhake–Lange [5, Lemma 12.3.1]. However, the above notion of an induced polarization applies whether  $(T, R)$  comes from a map of curves or not.

We apply approach (ii) to the chosen polarization  $E$  and idempotent  $(T, R)$  for our period matrix  $\Pi \in M_{4,8}(\mathbb{C})$  and obtain a matrix  $\Pi_2 \in M_{2,4}(\mathbb{C})$  with a polarization  $E_2$  of type  $(1, 2)$ , which defines an abelian surface  $A_2$ . Note that the above approaches are essentially equivalent by duality; we slightly preferred the second as it comes with a projection map  $A \rightarrow A_2$ .

#### 4. COMPUTING AN EQUATION FOR THE COVER

The  $(1, 2)$ -polarized abelian surface  $A_2$  defined by  $\Pi_2$  and  $E_2$  in the previous section was obtained from a numerical idempotent of  $\Pi$  defined over the base field  $K = \mathbb{Q}(\sqrt{61})$ . Therefore the abelian surface  $A_2$  is also defined over  $K$ . However, the polarization  $E_2$  is not principal, so we do not obtain in this way a Jacobian of a genus 2 curve over  $K$ . In this section, we show how to realize  $A_2$  as the Prym variety associated to a map  $X \rightarrow A_1$  from a genus 3 curve to a genus 1 curve.

Along the way, we will continue our numerical computations and retain our sensitivity to fields of definition; at the end, we will rigorously certify our construction.

To obtain a principal polarization, one can first try to take a maximal isotropic subgroup of the kernel of the isogeny  $A \rightarrow A^\vee$  defined by  $E_2$ . This kernel is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and carries a non-trivial Weil pairing; there are therefore 3 such maximal isotropic groups. Calculating the corresponding principally polarized quotients of  $A_2$ , one obtains that all of them give rise to indecomposable polarizations and therefore correspond to algebraic curves under Torelli. However, calculating the corresponding Igusa invariants, or alternatively reconstructing after Guàrdia [19] (implemented at [35]) shows that all of them define the same cubic Galois extension  $L$  of  $K$ , namely that defined by the polynomial  $x^3 - \sqrt{61}x^2 + 4x + 2$ .

This cubic polynomial also shows the way out. We will glue  $A_2$  with an elliptic curve  $A_1$  over  $K$  to realize  $A_2$  as the Prym of genus-3 double cover of  $A_1$  over  $K$ . This is a slight generalization of the same gluing operation when both  $A_2$  and  $A_1$  have a principal polarization, which will be considered in detail in the upcoming work by Hanselman [20] (for code, see Hanselman–Sijtsling [21]).

Via the aforementioned cubic polynomial, we consider the elliptic curve

$$(4.1) \quad A_1: y^2 = x^3 - \sqrt{61}x^2 + 4x + 2.$$

Let  $\Pi_2$  be a period matrix for the 2-dimensional abelian variety  $A_2$  with respect to which the polarization  $E_2$  is represented by the alternating form

$$(4.2) \quad E_2 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

The elliptic curve  $A_1$  will have a principal polarization represented by the standard symplectic matrix  $E_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ , and with corresponding period matrix  $\Pi_1$  say.

Consider the period matrix

$$(4.3) \quad \Pi'_3 = \begin{pmatrix} \Pi_2 & 0 \\ 0 & \Pi_1 \end{pmatrix},$$

with corresponding abelian variety  $A'_3$ ; it admits a polarization represented by

$$(4.4) \quad E'_3 = \begin{pmatrix} E_2 & 0 \\ 0 & 2E_1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

Let  $G := \ker(E'_3) < \frac{1}{2}\Lambda'/\Lambda'$ , where  $\Lambda' = H_1(A'_3, \mathbb{Z}) \cong \Pi'_3\mathbb{Z}^6$ . Then  $G$  is equipped with the basis corresponding to the final four columns of  $E'_3$ , and under the corresponding identification

$$(4.5) \quad G \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2$$

the Weil pairing on  $G$  is the product pairing. By Birkenhake–Lange [5, 2.4.4], the quotients of  $A'_3$  on which the polarization  $E'_3$  induces a principal polarization are in bijection with the maximal isotropic subgroups  $H < G$ —there are 15 such subgroups.

**Proposition 4.6.** *Suppose that  $A'_3$  and  $G$  are defined over  $K$ . Then there exists a maximal isotropic subgroup  $H < G$  that is defined over  $K$ . In particular, the quotient  $A'_3/H$  is defined over  $K$ .*

*Proof.* The first factor in (4.5) corresponds to the kernel of the polarization  $E_2$  on  $A_2$ . By the discussion at the beginning of this section, we know the structure of this group as a Galois module: the elements of order 2 are cyclically permuted by a generator of the Galois extension  $L$  of  $K$  defined by  $x^3 - \sqrt{61}x^2 + 4x + 2$ . This is the very same Galois module structure as that on the second factor in (4.5), which corresponds to  $A_1[2]$ .

We can therefore obtain a Galois-stable isotropic subgroup  $H < G$  by starting with a pair  $(x_1, x_2)$  with  $x_1 \neq 0$  and  $x_2 \neq 0$  and taking the image under Galois, after which we adjoin 0:

$$(4.7) \quad H := \{(0, 0), (x_1, x_2), (\sigma(x_1), \sigma(x_2)), (\sigma^2(x_1), \sigma^2(x_2)) = (x_1 + \sigma(x_1), x_2 + \sigma(x_2))\}.$$

Since  $\sigma_i(x_1)$  and  $\sigma_j(x_1)$  pair to 1 for  $i \neq j$  and similarly for  $x_2$ , this subgroup is indeed isotropic, because the product pairing on  $G$  assumes the values  $0 + 0 = 0$  and  $1 + 1 \equiv 0 \pmod{2}$ . By construction,  $H$  is defined over  $K$ .

The second part of the proposition follows immediately.  $\square$

Given a maximal isotropic subgroup  $H$  of  $G$ , say with generators  $h_1$  and  $h_2$ , we take inverse images  $\tilde{h}_1$  and  $\tilde{h}_2$  in  $\frac{1}{2}\Lambda'$ . This yields a lattice

$$(4.8) \quad \Lambda = \Lambda' + \mathbb{Z}\tilde{h}_1 + \mathbb{Z}\tilde{h}_2.$$

that contains  $\Lambda'$ . Choosing a basis of  $\Lambda$ , and keeping the basis for  $\Lambda'$  used heretofore, we find a matrix  $R_3 \in M_6(\mathbb{Z})$  such that  $\Lambda R_3 = \Lambda'$ . By construction,  $E'_3$  induces a principal polarization on the abelian variety corresponding to the period matrix

$$(4.9) \quad \Pi_3 = \Pi'_3 R_3^{-1}.$$

Note that we have a projection map corresponding to the pair  $(I_3, R_3)$  in the equality  $I_3\Pi'_3 = \Pi_3R_3$ . Under this map, the induced principal polarization on  $\Pi_3$  corresponds to the polarization class from Proposition 3.12.

While we can in principle identify the subgroup  $H$  in terms of the columns of  $E'_3$  by using the Abel–Jacobi map from [27], we just tried all 15 subgroups, as in Algorithm 4.10.

---

**Algorithm 4.10.** Finding a principally polarized quotient over  $K$  that is a Jacobian

---

**Input:** The period matrices  $\Pi_2$  and  $\Pi_1$  for the factors  $A_2$  and  $A_1$  over  $K$ , with polarizations  $E_2$  and  $E_1$  of type  $(1, 2)$  and  $(1)$  respectively, along with the associated matrices  $\Pi'_3$  and  $E'_3$  as in (4.3) and (4.4).

**Output:** A matrix  $\Pi_3 = \Pi'_3R_3^{-1}$  on which  $E'_3$  induces a principal polarization  $E_3$  such that  $\Pi_3$  numerically corresponds to a genus-3 curve  $X$  over  $K$ , along with  $E_3$  and the invariants of  $X$ .

**Algorithm:**

1. Determine the 15 isotropic subgroups  $H$  of  $G = \ker(E'_3) \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2$  with the product Weil pairing.
  2. For a given  $H$  as in Step 1, lift generators  $h_1$  and  $h_2$  to elements  $\tilde{h}_1$  and  $\tilde{h}_2$  of  $\frac{1}{2}\Lambda'/\Lambda'$ .
  3. Construct  $\Lambda = \Lambda' + \mathbb{Z}\tilde{h}_1 + \mathbb{Z}\tilde{h}_2$ , choose a basis of  $\Lambda$ , and find  $R_3 \in M_6(\mathbb{Z})$  such that  $\Lambda R_3 = \Lambda'$ .
  4. Let  $\Pi_3 = \Pi'_3R_3^{-1}$ , and let  $E_3 = R_3^{-t}E'_3R_3^{-1}$ .
  5. Using the methods of [24, §2] and LLL, check if the principally polarized abelian variety defined by  $\Pi_3$  and  $E_3$  corresponds to an algebraic curve  $X$ , and if so, whether the invariants of  $X$  are numerically in  $K$ . If so, return  $\Pi_3$ ,  $E_3$ , and the corresponding invariants. Otherwise proceed to the next  $H$  in Step 1.
- 

Invoking this calculation using 1000 decimal digits, only one isotropic subgroup numerically gave rise to invariants over  $K$ ; we obtain in this way a period matrix  $\Pi_3$  whose abelian variety  $A_3 := \mathbb{C}^3/\Pi_3\mathbb{Z}^6$  is equipped with the principal polarization  $E_3$ .

Finally, using the main result in Lercier–Ritzenthaler–Sijtsling [25] (recognizing invariants), we constructed a plane quartic equation defining a genus 3 curve whose Jacobian (numerically) matches the abelian surface  $A_3$ .

## 5. SIMPLIFYING, TWISTING, AND VERIFYING THE COVER

The methods from the previous section furnish us with an equation  $F(x, y, z) = 0$  defining a smooth plane quartic curve  $X \subset \mathbb{P}^2$  over  $K$  whose Jacobian putatively contains the abelian surface  $A = A_2$  and the elliptic curve  $E = A_1$  in Theorem 1.1 as isogeny factors over  $\mathbb{Q}^{\text{al}}$ . Since this reconstruction from invariants is only up to  $\mathbb{Q}^{\text{al}}$ -isomorphism, this Jacobian may not yet contain the given factors over  $K$ . Moreover, the implementation of these methods does not yet optimize the equations involved when working over proper extensions of  $\mathbb{Q}$ ; indeed, the first homogeneous defining polynomial  $F$  is of a rather terrible form, whose coefficients are thousands upon thousands of decimal digits long. In this section, we simplify, twist, and then verify that the cover is as claimed.

**Simplification.** Since the ring of integers of  $K$  has class number 1, a first step is to remove superfluous primes from the discriminant by generalizing methods of Elsenhans [14]. This approach makes the equation somewhat smaller, but its size is still thousands of digits.

Although we constructed  $X$  from a period matrix  $\Pi$ , the reconstruction methods involved only uses invariants and does not furnish the period matrix of  $\text{Jac}(X)$  in terms of  $\Pi$ . Fortunately, using integration algorithms due to Neurohr [28], we can simply recompute the period matrix of  $\text{Jac}(X)$  from scratch. Then, with the techniques of Bruin–Sijtsling–Zotine [7] one can find the numerical geometric automorphism group  $\text{Aut}(X_{\mathbb{C}})$  of the curve  $X$  along with its tangent representation on the ambient  $\mathbb{P}^2$ . It turns out that  $\text{Aut}(X_{\mathbb{C}}) \simeq \mathbb{Z}/2\mathbb{Z}$ , and in particular the nontrivial involution  $\iota$  generating  $\text{Aut}(X_{\mathbb{C}})$  is putatively defined over  $K$  itself.

Let  $T \in \text{GL}_3(K)$  be a matrix representing  $\iota$ , i.e.,  $F \cdot T = \lambda F$  under the substitution acting on the right. Since  $X$  is canonically embedded, we can read off the matrix  $T$  from its tangent representation. Moreover, we can write  $T = UDU^{-1}$ , where  $D$  is a diagonal matrix with diagonal entries  $(-\mu, \mu, \mu)$  say. Then for  $H = F \cdot U$  we have  $H \cdot D = F \cdot UD = \lambda F \cdot U = \lambda H$ , so that  $H(-x, y, z) = \lambda H(x, y, z)$ . In this way, we recognize an exact automorphism and reduce to the case where

$$(5.1) \quad F(x, y, z) = G(x^2, y, z),$$

with  $G$  homogeneous in  $x, y, z$  of weights 2, 1, 1. Now the equation  $G(x, y, z) = 0$  defines a genus-1 curve  $E$ , which is the quotient of  $X$  by its involution  $\iota$  and which is still defined over  $K$ . The map  $X \rightarrow E$  is ramified over the divisor of zeros  $D$  of  $x$  on  $E$ .

We then calculate the  $j$ -invariant of the binary quartic  $q(y, z)$  corresponding to the genus-1 curve  $E$ . An elliptic curve  $E_0$  with the same  $j$ -invariant over  $K$  is defined by

$$(5.2) \quad E_0: u^2 = p_0(t)$$

over  $K$ , where

$$(5.3) \quad p_0(t) := (10\nu + 34)(t^3 + \nu t^2 + (1 - \nu)t + 1)$$

where  $\nu := (1 + \sqrt{61})/2 \in K$  satisfies  $\nu^2 = \nu + 15$ . The conductor of  $E_0$  is (64). As luck would have it, the binary quartic  $q$  is equivalent over  $K$  to the quartic  $z^4 p_0(y/z)$  corresponding to the polynomial  $p_0$ , yielding an isomorphism  $E \xrightarrow{\sim} E_0$ . Pushing the divisor  $D$  along this isomorphism, one obtains a divisor  $D_0$  on  $E_0$ . Again luck is on our side and the divisor  $D_0 - 4\infty$  on  $E_0$  is principal; the corresponding degree-2 cover  $X_0$  of  $E_0$  is defined by the affine equations

$$(5.4) \quad X_0: \begin{cases} (10\nu + 34)u^2 = t^3 + \nu t^2 + (1 - \nu)t + 1 \\ (-2\nu + 9)w^2 = 2u + (-7\nu - 24)t^2 + (4\nu + 14)t - 2\nu - 7 \end{cases}$$

Eliminating  $u$  using the second equation and substituting in the first, replacing  $w \leftarrow x$  and  $t \leftarrow y$ , and homogenizing yields the defining homogeneous quartic

$$(5.5) \quad \begin{aligned} F_0(x, y, z) = & (-195\nu + 859)x^4 + (-64\nu + 282)x^2y^2 + (-5\nu + 24)y^4 \\ & + (148\nu - 652)x^2yz + (-16\nu + 68)y^3z + (-74\nu + 326)x^2z^2 \\ & + (96\nu - 422)y^2z^2 + (-148\nu + 652)yz^3 + (-47\nu + 207)z^4. \end{aligned}$$

We are blessed for one final time because  $F_0$  defines a non-singular curve  $X_0 \subset \mathbb{P}^2$  with the same Dixmier–Ohno invariants as the original terrible curve  $X$ . (This is not automatic, as a degree 2 cover of a genus-1 curve is not determined by its ramification locus only, in contrast to the case of genus-0 curves.) In any event, we have finally obtained a simplified equation  $X_0$ .

**Twisting.** It remains to find the correct twist of  $X_0$  (with respect to the involution on  $X_0$ ) that matches  $A_2$  as an isogeny factor *over*  $K$  (instead of merely over  $\mathbb{Q}^{\text{al}}$ ). Again, this step is needed because the algorithms in Lercier–Ritzenthaler–Sijtsling [25] only yield the correct geometric isomorphism class. We proceed as follows.

First, we consider the scheme over  $\mathbb{Z}$  cut out by (5.5) and the equation for  $\nu$ . By a Gröbner basis computation, we find that  $X_0$  has bad reduction only at the prime (2); so our desired twist will be by a 2-unit (in  $K^\times$ ). We begin by computing generators for the group  $U := \mathbb{Z}_K[1/2]^\times / \mathbb{Z}_K[1/2]^{\times 2}$  of 2-units of  $K$  modulo squares, a group with 2-rank 3.

To find the right twist, we loop over primes  $p \geq 5$  that split in  $K$  and by counting points compare the  $L$ -polynomial  $L_p(X, T) \in 1 + T\mathbb{Z}[T]$  of  $X$  and the absolute  $L$ -polynomial of  $f$

$$L_p(f, T) := (1 - a_p T + \chi(p)pT^2)(1 - \tau(a_p)T + \chi(p)T^2) \in 1 + T\mathbb{Z}[T],$$

where  $\langle \tau \rangle = \text{Gal}(K | \mathbb{Q})$ . We find always that  $L_p(f, \pm T) \mid L_p(X, T)$  for a unique choice of sign  $\varepsilon_p$ .

We then look for an element  $\delta \in U$  such that  $\left(\frac{\delta}{\mathfrak{p}}\right) = \varepsilon_p$  for each prime  $\mathfrak{p}$  above  $p$ : we find a unique match, namely  $\delta = -5\nu + 22$ , an element of norm  $-1$ . Twisting by this element (replacing  $x^2 \leftarrow \delta^{-1}x^2$ ) gives an equation all of whose good Euler factors match:

$$(5.6) \quad \begin{aligned} F(x, y, z) := & (5\nu + 17)x^4 - (14\nu + 48)x^2y^2 + (8\nu + 28)x^2yz \\ & - (4\nu + 14)x^2z^2 + (10\nu + 33)y^4 - (12\nu + 44)y^3z \\ & + (2\nu + 26)y^2z^2 + (4\nu - 16)yz^3 + (\nu - 6)z^4. \end{aligned}$$

**Verification.** We now conclude with the proof of our main result (Theorem 1.1); for convenience, we reproduce the statement.

**Theorem 5.7.** *Let  $X$  be the projective plane curve over  $K$  defined by the equation  $F(x, y, z) = 0$  as in (5.6). Then the following statements hold.*

- (a) *The curve  $X$  is smooth of genus 3 and has bad reduction at the prime (2) only.*
- (b) *The curve  $X$  admits an involution  $\iota: (x : y : z) \mapsto (-x : y : z)$  over  $K$ , and the quotient of  $X$  by  $\iota$  defines a map from  $X$  onto an elliptic curve  $E$  of conductor (64). An equation for  $E$  is given by*

$$-(10\nu + 34)y^2 = x^3 - \nu x^2 + (-\nu + 1)x - 1.$$

- (c) *Up to isogeny over  $K$ , we have  $\text{Jac}(X) \sim A \times E$ , where  $A$  is the Prym variety of the natural map  $\text{Jac}(X) \rightarrow \text{Jac}(E)$ , an abelian surface over  $K$  with everywhere good reduction.*
- (d) *All geometric endomorphisms of  $A$  are defined over  $K$ , and  $\text{End}(A) \simeq \mathbb{Z}[\sqrt{3}]$  so  $A$  is of  $\text{GL}_2$ -type over  $K$ . Moreover,  $A$  is isogenous to  $A'_{61}$  over  $K$ .*
- (e) *The abelian surface  $A$  has a polarization over  $K$  of type (1, 2), but no abelian surface isogenous to  $A$  over  $K$  admits a principal polarization over  $K$ .*

*Proof.* Part (a) was verified directly via a Gröbner basis computation as above: more precisely, we compute that the ideal  $N$  generated by  $F$  and its derivatives in  $\mathbb{Z}[\nu][x, y, z]$ , saturated at the irrelevant ideal  $(x, y, z)$ , has  $N \cap \mathbb{Z}[\nu] = (2)^{14}$ .

Part (b) is because  $F(x, y, z) = G(x^2, y, z)$ , and  $G(x, y, z)$  defines an elliptic curve, equipped with the point at infinity  $(\nu - 3 : 1 : 0)$ ; we then compute the given equation (arising up to



quadratic twist by construction). For the first part of (c), the splitting over  $K$  comes from the map in (b).

Next, we prove part (d) using the methods of Costa–Mascot–Sijtsling–Voight [10], which rigorously certifies that  $\text{End}(\text{Jac}(X)) = \text{End}(\text{Jac}(X^{\text{al}})) \simeq \mathbb{Z} \times \mathbb{Z}[\sqrt{3}]$ , where  $X^{\text{al}}$  denotes the base change to an algebraic closure  $K^{\text{al}}$  of  $K$ . More precisely, with respect to a  $K$ -basis of differentials, we certify that there is an endomorphism with tangent representation

$$(5.8) \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3/2 & (\nu - 4)/2 \\ 0 & (\nu + 3)/2 & -3/2 \end{pmatrix}$$

representing multiplication by  $\sqrt{3}$ .

To finish the proof of (c), frustratingly it is not clear how to algorithmically verify that the Prym has everywhere good reduction directly. (We could not find an implementation for the computation of regular models over number fields.) Instead, we look at Galois representations and apply the now standard method of Faltings–Serre, the relevant details of which we now sketch: see Dieulefait–Guerberoff–Pacetti [13, §4] and more generally Brumer–Pacetti–Poor–Tornara–Voight–Yuen [4, §2].

The 2-adic Tate module of the abelian surface factor yields a Galois representation

$$(5.9) \quad \rho_{A,2}: \text{Gal}_K \rightarrow \text{GL}_2(\mathbb{Z}_2[\sqrt{3}]),$$

where  $\text{Gal}_K := \text{Gal}(K^{\text{al}} | K)$  is the absolute Galois group of  $K$ ; since  $(2) = \mathfrak{l}^2$  ramifies in  $\mathbb{Z}[\sqrt{3}]$ , reducing modulo  $\mathfrak{l} = (1 + \sqrt{3})$  gives the mod  $\mathfrak{l}$  representation

$$\bar{\rho}_{A,\mathfrak{l}}: \text{Gal}_K \rightarrow \text{GL}_2(\mathbb{F}_2).$$

Counting points, we find that the conjugacy classes of Frobenius elements for either prime above 5 has order 3, so the image of  $\bar{\rho}_{A,\mathfrak{l}}$  has order 3 or 6, and correspondingly the fixed field of  $\ker \bar{\rho}_2$  is an extension of  $K$  of degree 3 or 6 ramified only at  $(2)$ . By computational class field theory, we verify there is in fact a *unique* such extension: it is the normal closure of the extension of  $K$  defined by the polynomial  $p_0(t)$  in (5.3), whose absolute field is defined by

$$(5.10) \quad x^6 + x^5 - 7x^4 + 14x^2 - 16x + 4;$$

the full normal extension  $L$  of  $\mathbb{Q}$  is defined by

$$(5.11) \quad x^{12} - 4x^{11} + 10x^{10} - 44x^9 + 174x^8 - 422x^7 + 618x^6 - 512x^5 + 170x^4 + 56x^3 - 58x^2 + 6x + 9.$$

We repeat the same calculation for the newform  $f \in S_2(\Gamma_0(61), \chi)$ : its base change  $f_K$  to  $K$  has level (1) and so gives a Galois representation  $\rho_{f_K,\mathfrak{l}}: \text{Gal}_K \rightarrow \text{GL}_2(\mathbb{Z}_2^{\text{al}})$  for which the characteristic polynomial of Frobenius lies in  $\mathbb{Z}_2[\sqrt{3}]$ . Reducing modulo  $\mathfrak{l}$  and semisimplifying gives  $\bar{\rho}_{f_K,\mathfrak{l}}^{\text{ss}}: \text{Gal}_K \rightarrow \text{GL}_2(\mathbb{F}_2^{\text{al}})$ ; since the traces belong to  $\mathbb{F}_2$ , up to equivalence the representation takes values in  $\mathbb{F}_2$  [36, Corollary 1], and as in the previous paragraph we confirm that it is surjective so absolutely irreducible so equal to its semisimplification: indeed, we must have  $\bar{\rho}_{A,\mathfrak{l}} \simeq \bar{\rho}_{f_K,\mathfrak{l}}$  by uniqueness. By a result of Carayol [8, Theoreme 2], up to equivalence the representation takes values in  $\mathbb{Z}_2[\sqrt{3}]$ , i.e., we have  $\rho_{f_K,\mathfrak{l}}: \text{Gal}_K \rightarrow \text{GL}_2(\mathbb{Z}_2[\sqrt{3}])$ .

We conclude by showing that  $\rho_{A,\mathfrak{l}} \simeq \rho_{f_K,\mathfrak{l}}$ , from which the remainder of part (c) follows as  $f_K$  has level (1). We compute  $\mathbb{Z}_L[1/2]^\times / \mathbb{Z}_L[1/2]^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^9$  and that the primes of  $L$  above 3, 5, 61, 97 generate the corresponding elementary 2-abelian extension of  $L$ . The

method of Faltings–Serre then provides that  $\rho_{A,\iota} \simeq \rho_{f_K,\iota}$  if and only if we have the equality of traces  $\text{tr } \rho_{A,\iota}(\text{Frob}_{\mathfrak{p}}) = \text{tr } \rho_{f_K,\iota}(\text{Frob}_{\mathfrak{p}})$  for the primes  $\mathfrak{p}$  of  $K$  above 3, 5, 61, 97, where  $\text{Frob}_{\mathfrak{p}} \in \text{Gal}_K$  denotes (a representative of) the conjugacy class of the  $\mathfrak{p}$ -Frobenius automorphism. Having checked equality of  $L$ -polynomials for these primes (indeed, we checked all primes of norm up to 200), the result follows.

Finally, having proven in the previous paragraph that  $A$  is modular, part (e) was proven for a particular abelian surface in the isogeny class of  $A$  by Dembélé–Kumar [12, Remark 3] (using a criterion of González–Guàrdia–Rotger [18]). We now show it extends to all abelian surfaces in the isogeny class. We have exhibited a  $(1, 2)$ -polarization  $\lambda: A \rightarrow A^\vee$ , where  $A^\vee$  denotes the dual abelian variety. Assume for purposes of contradiction that there exists an isogeny  $\varphi: A' \rightarrow A$  and a *principal* polarization  $\lambda'$  on  $A'$ , both over  $K$ . Then

$$\mu' := \varphi^\vee \circ \lambda \circ \varphi: A' \rightarrow (A')^\vee$$

is another polarization, with  $\deg(\mu') = 2 \deg(\varphi)^2$ . From work of González–Guàrdia–Rotger [18, Theorem 2.3, Theorem 2.10(ii)], we conclude that  $\mu'$  corresponds to a *totally positive* element of  $\text{End}(A')$  of norm  $\deg(\mu')$ . But  $\text{End}(A')$  is an order in  $\text{End}(A') \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{3})$ , and 2 is not a norm from this field—equivalently, the conic  $x^2 - 3y^2 = 2z^2$  has no rational points over  $\mathbb{Q}$ , or also equivalently, the corresponding quaternion algebra  $(2, 3 | \mathbb{Q}) \not\cong M_2(\mathbb{Q})$  is not split, having discriminant 6—a contradiction. (The element  $1 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$  has norm  $-2$ , and  $(2)$  represents the nontrivial element of the narrow class group of  $\mathbb{Z}[\sqrt{3}]$ .)  $\square$

## REFERENCES

- [1] V. A. Abrashkin, *Galois modules of group schemes of period  $p$  over the ring of Witt vectors*, translated from *Izv. Akad. Nauk SSSR Ser. Mat.* **51** (1987), no. 4, 691–736, 910, *Math. USSR-Izv.* **31** (1988), no. 1, 1–46.
- [2] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus-2 curves over the rational numbers*, *LMS J. Comput. Math.* **19** (Special Issue A) (2016), 235–254.
- [3] Armand Brumer and Kenneth Kramer, *Certain abelian varieties bad at only one prime*, *Algebra Number Theory* **12** (2018), no. 5, 1027–1071.
- [4] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen, *On the paramodularity of typical abelian surfaces*, *Algebra & Number Theory* **13** (2019), no. 5, 1145–1195.
- [5] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin, second edition, 2004.
- [6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, *J. Symbolic Comput.* **24** (1997), vol. 3–4, 235–265.
- [7] Nils Bruin, Jeroen Sijsling, and Alexandre Zotine, *Numerical computation of endomorphism rings of Jacobians*, *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, Open Book Series 2 (2019), 155–171.
- [8] Henri Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet,  $p$ -adic monodromy and the Birch and Swinnerton-Dyer conjecture* (Boston, MA, 1991), *Contemp. Math.*, vol. 165, Amer. Math. Soc., Providence, RI, 1994, 213–237.
- [9] W. Casselman, *On abelian varieties with many endomorphisms and a conjecture of Shimura’s*, *Invent. Math.* **12** (1971), 225–236.
- [10] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, *Math. Comp.* **88** (2019), 1303–1339.
- [11] Lassina Dembélé, *Abelian varieties with everywhere good reduction over certain real quadratic fields with small discriminant*, 2019, preprint.

- [12] Lassina Dembélé and Abhinav Kumar, *Examples of abelian surfaces with everywhere good reduction*, Math. Ann. **364** (2016), no. 3–4, 1365–1392.
- [13] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), no. 270, 1145–1170.
- [14] Andreas-Stephan Elsenhans, *Good models for cubic surfaces*, preprint at [https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red\\_5.pdf](https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf).
- [15] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, translated from Invent. Math. **73** (1983), no. 3, 349–366; *ibid.* **75** (1984), no. 2, 381, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, 9–27.
- [16] Tom Fisher, *How to trivialise an algebra*, 2007, <http://www.faculty.jacobs-university.de/mstoll/workshop2007/fisher2.pdf>.
- [17] Jean-Marc Fontaine, *Il n’y a pas de variété abélienne sur  $\mathbb{Z}$* , Invent. Math. **81** (1985), no. 3, 515–538.
- [18] Josep González, Jordi Guàrdia, and Victor Rotger, *Abelian surfaces of  $GL_2$ -type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287.
- [19] Jordi Guàrdia, *Jacobian nullwerte and algebraic equations*, J. Algebra **253** (2002), no. 1, 112–132.
- [20] Jeroen Hanselman, *Gluing curves along their torsion*, Ph.D. thesis, Universität Ulm, 2020, [https://oparu.uni-ulm.de/xmlui/bitstream/handle/123456789/33412/Hanselman\\_Thesis.pdf](https://oparu.uni-ulm.de/xmlui/bitstream/handle/123456789/33412/Hanselman_Thesis.pdf).
- [21] Jeroen Hanselman and Jeroen Sijsling, *gluing: Gluing curves of low genus along their torsion*, <https://github.com/JRSijsling/gluing>.
- [22] Ivanyos, Gábor, Lajos Rónyai, and Josef Schicho, *Splitting full matrix algebras over algebraic number fields*, J. Algebra **354** (2012), 211–223.
- [23] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals Math. Studies, vol. 108, Princeton University Press, 1985.
- [24] 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.
- [25] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Reconstructing plane quartics from their invariants*, Discrete Comput. Geom. (2018), <https://doi.org/10.1007/s00454-018-0047-4>.
- [26] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, <http://www.lmfdb.org>, 2019, [Online; accessed 30 July 2019].
- [27] Pascal Molin and Christian Neurohr, *Computing period matrices and the Abel-Jacobi map of superelliptic curves*, Math. Comp. **88** (2019), no. 316, 847–888.
- [28] Christian Neurohr, *Efficient integration on Riemann surfaces  $\mathcal{E}$  and applications*, Ph.D. thesis, Carl-von-Ossietzky-Universität Oldenburg, 2018.
- [29] Nicolas Mascot, *Computing modular Galois representations*, Rendiconti Circ. Mat. Palermo, vol. 62 no 3 (2013), 451–476.
- [30] Nicolas Mascot, *Companion forms and explicit computation of  $PGL_2$ -number fields with very little ramification*, Journal of Algebra, vol. 509 (2018) 476–506.
- [31] Nicolas Mascot, Jeroen Sijsling, and John Voight, *Prym calculation code*, <https://github.com/JRSijsling/prym>.
- [32] Elisabeth E. Pyle, *Abelian varieties over  $\mathbb{Q}$  with large endomorphism algebras and their simple components over  $\overline{\mathbb{Q}}$* , Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, 189–239.
- [33] Kenneth A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), no. 1, 143–162.
- [34] René Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. **325** (2003), no. 3, 413–448.
- [35] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, no. 1, Princeton University Press, Princeton, 1971.
- [36] Jeroen Sijsling, *curve\_reconstruction: Geometric and arithmetic reconstruction of curves from their period matrices*, [https://github.com/JRSijsling/curve\\_reconstruction](https://github.com/JRSijsling/curve_reconstruction).
- [37] Richard Taylor, *Representations of Galois groups associated to modular forms*, Proc. ICM (Zürich, 1994), vol. 2, Birkhäuser, Basel, 1995, 435–442.

SCHOOL OF MATHEMATICS, TRINITY COLLEGE DUBLIN, IRELAND

*E-mail address:* mascotn@tcd.ie

*URL:* <https://www.maths.tcd.ie/~mascotn/>

UNIVERSITÄT ULM, INSTITUT FÜR ALGEBRA UND ZAHLENTHEORIE, D-89068 ULM, GERMANY

*E-mail address:* jeroen.sijssling@uni-ulm.de

*URL:* <https://jrsijssling.eu/>

MATHEMATICS DEPARTMENT, DARTMOUTH COLLEGE, HANOVER, NH 03755

*E-mail address:* jvoight@gmail.com

*URL:* <http://www.math.dartmouth.edu/~jvoight/>