Computing isogeny classes of typical principally polarized abelian surfaces over the rationals

Raymond van Bommel, Shiva Chidambaram, Edgar Costa, and Jean Kieffer

ABSTRACT. We describe an efficient algorithm which, given a principally polarized (p.p.) abelian surface A over $\mathbb{Q}$ with geometric endomorphism ring equal to $\mathbb{Z}$, computes all the other p.p. abelian surfaces over $\mathbb{Q}$ that are isogenous to A. This algorithm relies on explicit open image techniques for Galois representations, and we employ a combination of analytic and algebraic methods to efficiently prove or disprove the existence of isogenies. We illustrate the practicality of our algorithm by applying it to 1 440 894 isogeny classes of Jacobians of genus 2 curves.

1. Introduction

As a consequence of Faltings' finiteness theorems for abelian varieties [Fal83], the isogeny class of any abelian variety over a number field is finite. In the simplest case of elliptic curves over $\mathbb{Q}$, we have a good understanding of which shapes of isogeny classes can arise. Mazur's isogeny theorem for elliptic curves [Maz78] provides the list of primes ℓ appearing as degrees of isogenies over $\mathbb{Q}$, namely $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$. Furthermore, isogeny classes all have size at most 8 [Ken82]. In fact, the possible isogeny graphs can be explicitly listed [CL21, §6].

The standard approach to computing isogeny classes of elliptic curves over $\mathbb{Q}$ is the following. Given an elliptic curve E, it is enough to consider isogenies $E \to E'$ of prime degree ℓ where ℓ appears in Mazur's list. For each such ℓ, computing the possible image curves E' is a finite problem. The computation can be carried out either by factoring the ℓ-division polynomial of E and applying Vélu's formulas [Vél71], or more efficiently using explicit parametrizations or equations for the Hecke correspondence $X_0(\ell) \to X(1) \times X(1)$ [Elk98; CW05]. This method was used to generate the data currently contained in the L-functions and modular forms database (LMFDB)[1] [LMFDB].

As one moves away from the case of elliptic curves over $\mathbb{Q}$, very little is known on the theoretical side. Nevertheless, by carrying out explicit computations, one can hope to gain insight into the possible shapes of isogeny classes in higher dimensions. In this paper, we make a first step in this direction: we describe an algorithm to compute isogeny classes in the simplest higher-dimensional case, namely that of a

The first three authors were supported by Simons Foundation grant 550033. The fourth author was supported by Simons Foundation grant 550031.

[1] See `https://www.lmfdb.org/EllipticCurve/Q/Source`.

principally polarized (p.p.) abelian surface A over $\mathbb{Q}$. We also make the simplifying assumption that the geometric endomorphism ring of A is $\mathbb{Z}$, in other words, A is typical, although we plan to address more endomorphism ring types in future work.

Our overall strategy is to generalize the above method of computing isogeny classes to the case of abelian surfaces. However, several obstacles immediately arise:

(1) Isogenies no longer decompose into rational, prime-degree isogenies.
(2) There is no known analogue of Mazur's theorem for higher-dimensional abelian varieties.
(3) Division polynomials are too big to be efficiently computed, except for very small values of ℓ. The same is true of explicit equations for higher-dimensional analogues of the modular curve $X_0(\ell)$ studied in [Mil15a]: see [Mil15b] for examples for very small primes ℓ.

We address the first issue in Section 2, where we show that we only need to consider two types of isogenies of degree ℓ^2 and ℓ^4 respectively, where ℓ is a prime.

We circumvent the second issue in the following way. From any given typical abelian surface, Serre's open image theorem for Galois representations [Ser99] asserts that isogenies of the above types can exist over $\mathbb{Q}$ only for a finite number of primes ℓ (depending on the abelian surface). It is sufficient to consider these primes to enumerate the "neighbors" of A in the isogeny class. Further, Dieulefait [Die02] describes how to efficiently compute a finite superset of this list. We review this method in Section 3, and provide complete proofs for the reader's convenience.

To address the third issue, we advantageously replace purely algebraic methods by complex-analytic ones relying on the Siegel moduli space of complex p.p. abelian surfaces. Concretely, given an abelian surface A, we enumerate images of its period matrix under certain Hecke correspondences, and compute modular invariants at these points analytically. By keeping track of the correct scaling factors, we can actually compute these invariants as algebraic integers (embedded in $\mathbb{C}$), and thus provably recognize which of these tuples of complex invariants correspond to abelian surfaces defined over $\mathbb{Q}$. This algorithm is the subject of Section 4. It is significantly less expensive than writing down equations for modular varieties or factoring division polynomials, and is practical for isogeny degrees as large as $29^4 = 707\,281$, the largest value we encountered in our computations.

The output invariants only specify the $\overline{\mathbb{Q}}$-isomorphism class of the abelian surface A' isogenous to A. In Section 5, we explain how to obtain the correct $\mathbb{Q}$-isomorphism class using a well-known and completely algebraic process. First, Mestre's algorithm provides a genus 2 curve over $\mathbb{Q}$ whose Jacobian is isomorphic to A' over $\overline{\mathbb{Q}}$. We then identify which quadratic twist of that curve represents the desired $\mathbb{Q}$-isomorphism class.

The resulting algorithm has been implemented: our code and data is publicly available at `https://github.com/edgarcosta/genus2isogenies`. Numerical computations are performed using the C library HDME [Kie23], itself based on the Arb library [Joh17] for high-precision arithmetic with certified error bounds.

We finally discuss applications of our algorithm in Section 6. We first present an illustrative example where we found an isogeny of degree 31^2. We also report on the results of running our algorithm on a large dataset of Jacobians of genus 2 curves that includes the current LMFDB data [LMFDB]. This dataset consists of 1 743 737 curves split among 1 440 894 isogeny classes. By completing these isogeny classes, we find 600 948 new curves.

Acknowledgements. We thank Fabien Cléry for communicating us references on Siegel modular forms, Andrew Sutherland and Noam Elkies for providing us with interesting genus 2 curves to use as an input to our algorithm, and Bjorn Poonen for helpful conversations.

2. Classification of isogenies

In this section, we describe two fundamental isogeny types that are sufficient to exhaust isogeny classes of typical p.p. abelian surfaces. The essential ingredient in this classification is that every isogeny between p.p. abelian varieties is compatible with the given polarizations up to the action of an endomorphism fixed by the Rosati involution, as we detail below.

2.1. Isogenies between p.p. abelian varieties. Let k be a field. For simplicity, we assume thoughout that k has characteristic zero: this allows us to identify group schemes over k with the groups of their $\overline{k}$-points endowed with an action of $\mathrm{Gal}(\overline{k}/k)$. Unless otherwise specified, we only consider abelian varieties and isogenies that are defined over k. Two isogenies are considered isomorphic if they have the same domain and differ by an isomorphism on their targets.

Let A be an abelian variety over k, and denote its dual by $A^\vee$. A *polarization* on A is an isogeny $\lambda\colon A \to A^\vee$ of the shape $a \mapsto T_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ for some (not necessarily k-rational) ample line bundle $\mathcal{L}$ on A, where T_a is the translation by a in A. A polarization is called *principal* if it is an isomorphism.

From now on, we assume that A is principally polarized (p.p.), in other words A is endowed with a principal polarization λ_A. We then have a *Rosati involution* on $\mathrm{End}(A)$ given by $\varphi \mapsto \lambda_A^{-1} \circ \varphi^\vee \circ \lambda_A$. An endomorphism $\beta \in \mathrm{End}(A)$ is called *symmetric* if it is invariant under this involution. If β is symmetric, then the roots of its characteristic polynomial are real numbers [Mum70, Thm. 6 p. 208], and we further say that β is *totally positive* if these roots are positive.

For A as above and any integer n, there exists a canonical symplectic pairing $A[n] \times A[n] \to \mu_n$ known as the *Weil pairing*. More generally, if $\beta \in \mathrm{End}(A)$ is any endomorphism that is symmetric and totally positive, then $\lambda_A \circ \beta$ is another polarization of A [Mum70, (3) p. 190 and (IV) p. 209]. As in [Mum70, Def. p. 227], we can also define a symplectic pairing on $A[\beta] \times A[\beta]$ that we also refer to as the Weil pairing. We then have the following characterization of isogenies in terms of maximal isotropic subgroups of torsion subgroups $A[\beta]$; see also [EGM, Prop. 11.25].

Lemma 2.1. *Let (A, λ_A) be a p.p. abelian variety over k. Then there is a one-to-one correspondence between isomorphism classes of isogenies from A to other p.p. abelian varieties A', and pairs (β, G), where β is a totally positive symmetric endomorphism of A, and G is a subgroup of $A[\beta]$ which is defined over k and maximal isotropic with respect to the Weil pairing. Explicitly, an isogeny $\varphi\colon A \to A'$ correponds to the pair (β, G) such that* $\ker\varphi = G$ *and β is the unique endomorphism satisfying $\varphi^\vee \circ \lambda_{A'} \circ \varphi = \lambda_A \circ \beta$.*

Proof. First, we note that any isotropic subgroup of $A[\beta]$ has cardinality at most $\sqrt{\#A[\beta]}$, and is maximal if and only if equality holds [Mum70, Thm. 4 p. 233].

Let $(A', \lambda_{A'})$ be a p.p. abelian variety, and let $\varphi\colon A \to A'$ be an isogeny. Then there is a unique endomorphism β of A such that $\varphi^\vee \circ \lambda_{A'} \circ \varphi = \lambda_A \circ \beta$. This β is fixed by the Rosati involution, and corresponds via the bijection of [Mum70, Application III p. 208] to an ample line bundle on A, namely the pullback by φ of the ample line bundle on A' defining the polarization $\lambda_{A'}$. Thus β is totally positive. Moreover, the pairing on $A[\beta]$ becomes trivial on $\ker\varphi$ by [Mum70, (1) p. 228]. As $\deg(\varphi)^2 = \deg(\varphi)\deg(\varphi^\vee) = \deg(\beta)$, it follows that $\ker\varphi$ is a maximal isotropic subgroup of $A[\beta]$.

On the other hand, if β and G are given, then $\lambda_A \circ \beta$ is a polarization on A, and the quotient A/G is principally polarized by [Mum70, Cor. p. 231]. □

2.2. Fundamental isogeny types. Assume now that k is a number field. An abelian variety A over k is called *typical* if $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$. If A is typical, then only a small number of isogeny types suffice in order to enumerate its isogeny class.

Lemma 2.2. *Any isogeny between typical p.p. abelian varieties over a number field k can be decomposed into a chain of isogenies $\varphi\colon A \to A'$ defined over k whose kernels are maximal isotropic subgroups of either $A[\ell]$ or $A[\ell^2]$, where ℓ is a prime number (depending on φ).*

Proof. Let $\varphi\colon A \to A'$ be any isogeny. Since A is typical, by Lemma 2.1, there exists an integer $n \geq 1$ such that $K \coloneqq \ker\varphi \subset A[n]$ is maximal isotropic. Factor $n = \ell_1^{e_1} \cdot \ldots \cdot \ell_r^{e_r}$. Then $K \cap A[\ell_i^{e_i}]$ is maximal isotropic inside $A[\ell_i^{e_i}]$ for all $i = 1, \ldots, r$. Indeed, by [Mil86, Lemma 16.1] the subgroup is isotropic, and by checking the cardinality, one sees that the subgroup is maximal isotropic. As each subgroup $K \cap A[\ell_i^{e_i}]$ is defined over $\mathbb{Q}$, we can decompose φ as the composition of isogenies whose degrees are prime powers.

Now suppose that $n = \ell^e$ is a prime power, and that $e > 2$. Then we claim that

$$K' \coloneqq \ell K \cap A[\ell^{e-2}] = \ell K[\ell^{e-1}]$$

is a maximal isotropic subgroup of $A[\ell^{e-2}]$. We will then be able to decompose φ into two isogenies of lower degree, namely $A \to A/K'$ and $A/K' \to A/K$.

First, we prove that K' is isotropic: if $\langle\cdot,\cdot\rangle_{\ell^i}$ denotes the Weil pairing on $A[\ell^i]$ (for any $i \geq 1$), and $\ell x_1, \ell x_2$ for $x_1, x_2 \in K$ are arbitrary elements of K', we have that $\langle \ell x_1, \ell x_2\rangle_{\ell^{e-2}} = \langle x_1, x_2\rangle_{\ell^e} = 1$ by [Mil86, Lemma 16.1]. To see that K' is maximal, we determine its cardinality. Let r_1 and r_2 be the ranks of $K[\ell]$ and $K/K[\ell^{e-1}]$ as $\mathbb{Z}/\ell\mathbb{Z}$-modules. We have an exact sequence

$$0 \to K[\ell] \to K[\ell^{e-1}] \xrightarrow{\ell} K' \to 0$$

and $\#K[\ell^{e-1}] = \#K/\ell^{r_2}$. Hence

$$\#K' = \#K[\ell^{e-1}]/\#K[\ell] = \#K/\ell^{r_1+r_2} = \ell^{eg-r_1-r_2}.$$

On the other hand, we have $r_1 + r_2 \leq 2g$ because the Weil pairing on $A[\ell] \times A[\ell]$ vanishes on $K[\ell] \times \ell^{e-1}(K/K[\ell^{e-1}])$, and these subspaces have dimensions r_1 and r_2 over $\mathbb{Z}/\ell\mathbb{Z}$ respectively. Indeed, for $x \in K[\ell]$ and $y \in \ell^{e-1}(K/K[\ell^{e-1}])$, we can write x as $\ell^{e-1}x'$ for some $x' \in A[\ell^e]$ and y as $\ell^{e-1}y'$ for some $y' \in K$, and then

$$\langle x, y\rangle_\ell = \langle \ell^{e-1}x', \ell^{e-1}y'\rangle_\ell = \langle x', y'\rangle_{\ell^e}^{\ell^{e-1}} = \langle \ell^{e-1}x', y'\rangle_{\ell^e} = \langle x, y'\rangle_{\ell^e} = 0,$$

by [Mil86, Lemma 16.1] and the fact that K is isotropic.

Since K' is isotropic for the Weil pairing on $A[\ell^{e-2}]$ and $r_1 + r_2 \leq 2g$, we must have $r_1 + r_2 = 2g$ and K' is maximal isotropic in $A[\ell^{e-2}]$. □

From now on, we focus on the case of typical p.p. abelian surfaces. Let ℓ be a prime. We say that an isogeny $\varphi : A \to A'$ is

- a *1-step ℓ-isogeny*, if $\ker(\varphi)$ is maximal isotropic in $A[\ell]$, and

- a *2-step ℓ-isogeny*, if $\ker(\varphi)$ is maximal isotropic in $A[\ell^2]$ and isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$ as an abstract abelian group.

Note that the terminology "2-step ℓ-isogeny" is slightly abusive, as the endomorphism β associated with φ via Lemma 2.1 is actually ℓ^2 in that case.

Proposition 2.3. *Any isogeny between typical p.p. abelian surfaces over a number field k can be decomposed into a chain of 1-step ℓ-isogenies, 2-step ℓ-isogenies, and multiplication-by-ℓ endomorphisms for a series of primes ℓ, all defined over k.*

PROOF. By Lemma 2.2, we only need to consider an isogeny φ whose kernel K is maximal isotropic inside $A[\ell^2]$. Then $\#K = \ell^4$, so K is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^4$, $(\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$ or $(\mathbb{Z}/\ell^2\mathbb{Z})^2$. In the first case, the isogeny φ is multiplication by ℓ. In the second case, φ is 2-step. In the third case, the group $K \cap A[\ell] = \ell K$ is a maximal isotropic subgroup of $A[\ell]$: it is isotropic by [Mil86, Lemma 16.1], and maximal for cardinality reasons. We can thus decompose φ into two 1-step isogenies $A \to A/\ell K$ and $A/\ell K \to A/K$. □

Remark 2.4. A 2-step isogeny factors as a composition of two 1-step isogenies over $\overline{k}$, but these 1-step isogenies are not necessarily defined over k. Here is a more detailed look into this situation. If K is the kernel of a 2-step ℓ-isogeny, then ℓK is a rational 1-dimensional subspace of $A[\ell]$. We can extend ℓK in $\ell + 1$ ways to get a maximal isotropic subgroup of $A[\ell]$ contained in K. These $\ell + 1$ ways to factor the 2-step isogeny as a composition of two 1-step isogenies are permuted by $\mathrm{Gal}(\overline{k}/k)$.

2.3. Computing an isogeny class. From now on, we assume that $k = \mathbb{Q}$. In the following sections, we will detect the existence of 1- or 2-step ℓ-isogenies from A to another p.p. abelian surface by studying the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $A[\ell]$. Let $\mathcal{L}_1$ (resp. $\mathcal{L}_2$) be the set of primes ℓ such that $A[\ell]$ admits a 1-dimensional (resp. 2-dimensional and isotropic) Galois-stable subspace. Then the existence of a rational 1-step (resp. 2-step) isogeny implies that $\ell \in \mathcal{L}_2$ (resp. $\mathcal{L}_1$).

Summarizing, we use the following algorithm to compute the isogeny class of a typical p.p. abelian surface A over $\mathbb{Q}$, defined as the set of isomorphism classes of p.p. abelian surfaces A' such that there exists an isogeny $\varphi : A \to A'$ defined over $\mathbb{Q}$. These abelian surfaces all are the Jacobian of a genus 2 curve over $\mathbb{Q}$ by [Lau01, Appendix, Thm. 4], and this is how we encode both the input and output.

Algorithm 2.5. *Input:* a genus 2 curve C over $\mathbb{Q}$ such that $A = \mathrm{Jac}(C)$.
Output: the list of all p.p. abelian surfaces over $\mathbb{Q}$ that are isogenous to A.

Step 1. Use Dieulefait's tests to find finite supersets of $\mathcal{L}_2$ and $\mathcal{L}_1$ (see §3).
Step 2. For each ℓ in these sets, compute invariants for all abelian surfaces A' over $\mathbb{Q}$ obtained as the image of a 1-step (resp. 2-step) ℓ-isogeny with domain A (see §4).
Step 3. Reconstruct each such A' as the Jacobian of a genus 2 curve over $\mathbb{Q}$ by applying Mestre's algorithm and identifying the correct twist (see §5).
Step 4. Repeat this process on all the newly obtained abelian surfaces as needed.

3. Rational ℓ-torsion subgroups

Let A be a typical p.p. abelian surface over $\mathbb{Q}$, and let N be its conductor (see [BK94, §6] for the definition of the conductor and further background). Let d be the maximal integer such that $d^2 | N$. Let S denote the set of primes of bad reduction for A, i.e. the set of primes dividing N.

For each prime $\ell \geq 2$, let $\rho_\ell \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}(4, \mathbb{Z}_\ell)$ denote the Galois representation on the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_{n \geq 1} A[\ell^n] \simeq \mathbb{Z}_\ell^4,$$

where we fix a symplectic basis of $T_\ell(A)$ for this last isomorphism. The Néron–Ogg–Shafarevich criterion [ST68] states that ρ_ℓ is unramified away from ℓ and S; in other words, if $p \notin S \cup \{\ell\}$ is a prime, then the inertia group I_p at p has trivial image under ρ. The prime-to-ℓ part of the conductor of ρ_ℓ equals N when ℓ is a prime of good reduction [GRR72, Exposé IX, §4]. For each prime p of good reduction, we let $Q_p(x) := x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2 \in \mathbb{Z}[x]$ denote the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_p)$, which is independent of $\ell \neq p$. The complex roots of $Q_p(x)$ all have absolute value $\sqrt{p}$.

Considering all the ℓ-adic representations at the same time, we obtain the adelic Galois representation $\rho \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}(4, \widehat{\mathbb{Z}})$ attached to A. Serre's open image theorem [Ser99] asserts that the image of ρ is an open subgroup of $\mathrm{GSp}(4, \widehat{\mathbb{Z}})$, or equivalently has finite index in it. Consequently, the mod-ℓ Galois representation $\overline{\rho}_\ell := \rho_\ell \bmod \ell$, attached to the Galois action on $A[\ell]$, is surjective for all primes ℓ outside a finite set.

Dieulefait [Die02] describes an algorithm to explicitly determine a finite set of primes containing all primes ℓ at which $\overline{\rho}_\ell$ is not surjective, using the classification of maximal subgroups of $\mathrm{GSp}(4, \mathbb{F}_\ell)$. For each type of maximal subgroup, one can give necessary conditions on ℓ for the image of $\overline{\rho}_\ell$ to be contained in a subgroup of this type, and these conditions are satisfied by finitely many primes ℓ. The algorithm has been implemented in SageMath [Sage] by the work of [BBKKMSV23].

In this work, we are only interested in two types of maximal subgroups, namely the stabilizers of lines and two-dimensional isotropic subspaces in $\mathbb{F}_\ell^4$ [BBKKMSV23, Lemma 2.3(1)]. Keeping notation from §2.3, we call $\mathcal{L}_1$ (resp. $\mathcal{L}_2$) the finite set of primes ℓ for which the image of $\overline{\rho}_\ell$ stabilizes a line (resp. a 2-dimensional isotropic subspace). A 1-step ℓ-isogeny with domain A exists over $\mathbb{Q}$ if and only if $\ell \in \mathcal{L}_2$. Moreover, if a 2-step ℓ-isogeny with domain A exists over $\mathbb{Q}$, then $\ell \in \mathcal{L}_1$ as per Remark 2.4. We now describe the associated Dieulefait criteria [Die02, §3.1, §3.2] in more detail, assuming from now on that A has good reduction at ℓ.

3.1. Computing a finite superset of $\mathcal{L}_1$. Dieulefait's tests consist in studying the factorization of characteristic polynomials $Q_p(x)$ over finite fields, for a given list of primes p. We include this list as part of the input of the following algorithm.

Algorithm 3.1. *Input:*

- a genus 2 curve C over $\mathbb{Q}$ such that $A = \mathrm{Jac}(C)$,
- the conductor N of A,
- and a non-empty finite set P of primes of good reduction for C.

Output: a finite superset of $\mathcal{L}_1$.

Step 1. Compute the maximal integer d such that $d^2 \mid N$.

Step 2. Compute $Q_p \in \mathbb{Z}[x]$ for $p \in P$ by computing the number of points on C over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

Step 3. Compute $M = \gcd_{p \in P} \mathrm{Res}\big(Q_p(x), x^{f(p)} - 1\big)$, where $f(p)$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$.

Step 4. Return the list of prime divisors of M.

Proposition 3.2. *Algorithm 3.1 returns a finite superset of $\mathcal{L}_1$.*

PROOF. Suppose that there exists a 1-dimensional subrepresentation (π, V) of $\overline{\rho}_\ell$, induced by a stable line $V \subset A[\ell]$. Let $V^\perp$ denote the subgroup of $A[\ell]$ that pairs trivially with V under the Weil pairing. By Galois equivariance of the Weil pairing, the 1-dimensional quotient representation on $A[\ell]/V^\perp$ is given by $\pi^{-1}\chi_\ell$, where χ_ℓ is the mod-ℓ cyclotomic character. By results of Raynaud [Ray74, Cor. 3.4.4] and Serre [Ser72, §1.9], we know that π restricted to the inertia group I_ℓ at ℓ is either trivial or equal to χ_ℓ.

In any case, there exists a character ε, unramified away from N, such that the semisimplification $\overline{\rho}_\ell^{ss}$ admits both ε and $\varepsilon^{-1}\chi_\ell$ as direct summands. Hence the conductor of $\overline{\rho}_\ell$ is divisible by the square of the conductor of ε, in other words $\mathrm{cond}(\varepsilon)$ divides d. Class field theory then implies that ε is a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$. For each prime $p \in L$, since $f(p)$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$, we have $\varepsilon(\mathrm{Frob}_p)^{f(p)} = 1$. Therefore, $\varepsilon(\mathrm{Frob}_p)$ is a root of the characteristic polynomial of $\overline{\rho}_\ell(\mathrm{Frob}_p)$ and also of the polynomial $x^{f(p)} - 1$ over $\mathbb{F}_\ell$. Thus ℓ divides $\mathrm{Res}(Q_p(x), x^{f(p)} - 1)$ and hence ℓ divides M.

Since the complex roots of $Q_p(x)$ have absolute value $\sqrt{p}$, they are distinct from the roots of $x^{f(p)} - 1$ which have absolute value 1. So the resultants and thus M are guaranteed to be non-zero and the computed superset is finite. ☐

Remark 3.3. Building on results of Grothendieck [GRR72, Exposé IX, Prop. 3.5] and Larson–Vaintrob [LV14, Thm. 7.2], the authors of [BBKKMSV23] introduce the following strengthening of the above technique (Alg. 3.3). For $p \in P$, let $r = \gcd(f(p), 120)$. Let R_p be the polynomial whose roots are the r-th powers of the roots of Q_p. Then each $\ell \in \mathcal{L}_1$ must divide $p\,R_p(1)$. The original criterion by Dieulefait, as presented above, was however sufficient for our purposes.

3.2. Computing a finite superset of $\mathcal{L}_2$. In the case of $\mathcal{L}_2$, the computation of a finite superset might fail if the list of auxiliary primes p is too small, leading to the following algorithm.

Algorithm 3.4. *Input:*

- a genus 2 curve C over $\mathbb{Q}$ such that $A = \mathrm{Jac}(C)$,
- the conductor N of A,
- and a non-empty finite set P of primes of good reduction for C.

Output: a finite superset of $\mathcal{L}_2$, or `false`.

Step 1. Compute d.
Step 2. For $p \in P$, compute $Q_p = x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2 \in \mathbb{Z}[x]$.
Step 3. For $p \in P$, compute the polynomials

$$R_{1,p}(x) \coloneqq (b_p x - 1 - p^2x^2)(px+1)^2 - a_p^2 p x^2 \quad \text{and}$$
$$R_{2,p}(x) \coloneqq (b_p x - p - px^2)(x+1)^2 - a_p^2 x^2.$$

Step 4. For $i = 1$ and 2, compute $M_i = \gcd_{p \in P} \mathrm{Res}\big(R_{i,p}(x), x^{f(p)} - 1\big)$, where $f(p)$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$. Let $M = M_1 M_2$.
Step 5. If M is nonzero, return the list of prime divisors of M, else return `false`.

Proposition 3.5. *Algorithm 3.4 returns either* `false` *or a finite superset of $\mathcal{L}_2$.*

PROOF. Suppose that $\overline{\rho}_\ell$ admits a 2-dimensional isotropic subrepresentation denoted by (π, V). The quotient representation on $A[\ell]/V$ is given by $\chi_\ell \otimes (\pi^{-1})^t$.

By [Ray74, Cor. 3.4.4] and [Ser72, §1.9], we obtain as above that either $\det(\pi) = \varepsilon\chi_\ell^2$ or $\det(\pi) = \varepsilon\chi_\ell$ for some character ε unramified away from N. The direct sum decomposition $\overline{\rho}_\ell^{ss} \simeq \pi \oplus \chi_\ell \otimes (\pi^{-1})^t$ then implies that $\mathrm{cond}(\varepsilon)$ still divides d.

If $\det(\pi) = \varepsilon\chi_\ell^2$, then for every prime p of good reduction, we have the following factorization of $Q_p(x)$ into a product of two related quadratic polynomials modulo ℓ:

$$Q_p(x) = \big(x^2 - rx + p^2\varepsilon(p)\big)\Big(x^2 - \frac{r}{p\varepsilon(p)}x + \varepsilon^{-1}(p)\Big).$$

If $\det(\pi) = \varepsilon\chi_\ell$, then for all such p, we have

$$Q_p(x) = \big(x^2 - rx + p\varepsilon(p)\big)\Big(x^2 - \frac{r}{\varepsilon(p)}x + p\varepsilon^{-1}(p)\Big).$$

By comparing coefficients and eliminating r, one observes that the first kind of factorization happens if and only if $\varepsilon(p)$ is a root of the integral polynomial $R_{1,p}(x)$ introduced in Algorithm 3.4 over $\mathbb{F}_\ell$ for all p. Similarly, the second kind of factorization happens if and only if $\varepsilon(p)$ is a root of $R_{2,p}(x)$ over $\mathbb{F}_\ell$ for all p. Thus, there is an $i \in \{1, 2\}$ such that for all p of good reduction, $\mathrm{Res}\big(R_{i,p}(x), x^{f(p)} - 1\big) = 0 \bmod \ell$. We deduce that ℓ always divides $M = M_1M_2$. □

We now show that Algorithm 3.4 returns a superset of $\mathcal{L}_2$ provided that P contains enough primes. In practice, failures are not an issue even for a small list P.

Proposition 3.6. *For B large enough and $P = \{p \le B \colon p \text{ is a good prime for } C\}$, Algorithm 3.4 returns a finite list of primes, in other words both M_1 and M_2 are nonzero.*

Proof. We first prove that $M_1 \neq 0$. For $p = 1 \bmod d$, we have

$$\mathrm{Res}(R_{1,p}(x), x^{f(p)} - 1) = R_{1,p}(1) = (b_p - 1 - p^2)(p + 1)^2 - a_p^2 p.$$

Using the bounds $|a_p| \le 4\sqrt{p}$ and $|b_p| \le 6p$ coming from the fact that the roots of $Q_p(x)$ have absolute value $\sqrt{p}$, it follows that $R_{1,p}(1) < 0$ if p is large enough, and thus $M_1 \neq 0$ for large B.

Second, we prove that $M_2 \neq 0$. Consider all polynomials over $\mathbb{F}_\ell$ which, over $\overline{\mathbb{F}}_\ell$, admit a factorization of the form

$$(x^2 - rx + p\eta)(x^2 - \tfrac{r}{\eta}x + p\eta^{-1}),$$

where $\eta \in \overline{\mathbb{F}}_\ell$ is a d-th root of unity and $r \in \overline{\mathbb{F}}_\ell$. When ℓ is sufficiently large, these polynomials do not account for all characteristic polynomials of matrices in $\mathrm{GSp}(4, \mathbb{F}_\ell)$. By Serre's open image theorem, we can further assume that the representation $\overline{\rho}_\ell$ is surjective. For such an ℓ, by the Chebotarev density theorem, there must exist infinitely many p such that $Q_p(x)$ does not factor over $\overline{\mathbb{F}}_\ell$ in the above shape, and thus $\ell \nmid \mathrm{Res}(R_{2,p}(x), x^{f(p)} - 1)$. Therefore $M_2 \neq 0$ if B is sufficiently large. □

Remark 3.7. Showing that $M_2 \neq 0$ for a sufficiently large B is non-trivial: indeed, if the reduction of A modulo p is isogenous to the square of an elliptic curve over $\mathbb{F}_p$, then $\mathrm{Res}(R_{2,p}(x), x^{f(p)} - 1) = 0$.

Remark 3.8. An improvement of a similar flavor to Remark 3.3 is also available here: see [BBKKMSV23, §3.1.3].

3.3. Other tests for irreducibility. The output of Algorithms 3.1 and 3.4 usually consists of very short lists of primes, but might still contain extraneous primes $\ell \notin \mathcal{L}_1 \cup \mathcal{L}_2$. In order to further weed out some of these primes, one can compute $Q_p(x)$ for a larger set of primes p, and eliminate any prime ℓ with the property that one of these polynomials is irreducible modulo ℓ. In our computations, we considered all primes $p \leq 500$ of good reduction for C.

4. Invariants of isogenous abelian surfaces

In this section, we describe an efficient algorithm solving the following problem: given a typical p.p. abelian surface A over $\mathbb{Q}$ and a prime number ℓ, compute the complete list of p.p. abelian surfaces A' over $\mathbb{Q}$ such that A and A' are linked by a rational 1- or 2-step ℓ-isogeny.

Devising a polynomial-time algorithm for this task is straightforward: we can write down equations for the torsion subgroups $A[\ell]$ or $A[\ell^2]$, look for rational subgroups of the correct shape by factoring these polynomials over $\mathbb{Q}$, and apply algorithms to compute quotients of p.p. abelian surfaces by isotropic subgroups [CE15; LR23]. Such an algorithm would however be hopelessly slow in practice.

A more efficient approach is to use modular equations for p.p. abelian surfaces, which are higher-dimensional analogues of elliptic modular polynomials: see [BL09] for their definition in the case of 1-step isogenies, and [Mil15a] for an efficient algorithm to compute them. Evaluating modular equations at A provides tuples of modular invariants (for instance Igusa–Clebsch invariants) of abelian surfaces isogenous to A, possibly defined over a number field. This evaluation can be done within a reasonable complexity, namely $\widetilde{O}(\ell^6 h)$ bit operations[2] in the case of 1-step ℓ-isogenies, where h is the height of the invariants of A [Kie22b]. This algorithm works by computing the invariants of isogenous abelian surfaces as complex numbers, packaging them into a polynomial, and recognizing its coefficients as rational numbers. Then a rational isogeny from A exists exactly when this polynomial has a rational root (see Proposition 4.7 below).

Here we take this method one step further: we compute these invariants over $\mathbb{C}$, and directly recognize when they are attached to a p.p. abelian surface defined over $\mathbb{Q}$. In a sense, we detect rational roots of modular equations without computing the number fields that other roots generate. When doing so, the cost is further lowered to $\widetilde{O}\big((n+1)\ell^d h\big)$ bit operations, where $d = 3$ (resp. 4) in the case of 1-step (resp. 2-step) isogenies, and n is the number of roots "close to" being rational, in a precise sense explained below. (We usually have $n = 0$, sometimes $n = 1$, and rarely more.) Crucially, this analytic method allows for certification. The modular invariants we compute provably correspond to p.p. abelian surfaces rationally isogenous to A, and provably miss none of them.

The computations over $\mathbb{C}$ make use of structure theorems for Siegel modular forms in dimension 2 and explicit formulas for Hecke correspondences, recalled in §4.1 and §4.2. Next, we explain why detecting rational isogenies reduces to detecting invariants defined over $\mathbb{Q}$ (§4.3), and how to compute these invariants as algebraic integers, which is the crucial idea behind certification (§4.4). Finally, in §4.5 and §4.6, we describe the algorithm and sketch its complexity analysis.

[2] We use the notation $\widetilde{O}(N)$ to denote $O\big(N \log^k(N)\big)$ for some value of k.

4.1. Siegel modular forms. Over $\mathbb{C}$, every p.p. abelian surface A can be written as a complex torus $\mathbb{C}^2/(\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2)$, where τ belongs to the Siegel upper half space $\mathbb{H}_2$, consisting of complex 2×2 symmetric matrices with positive definite imaginary part. Such a τ is called a (small) *period matrix* of A. The group $\mathrm{GSp}(4, \mathbb{R})^+$ consisting of general symplectic matrices with positive similitude factor acts on $\mathbb{H}_2$ as follows:

$$\gamma\tau = (a\tau + b)(c\tau + d)^{-1}, \quad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ in } 2 \times 2 \text{ blocks.}$$

For later use, we also write

$$\gamma^*\tau = c\tau + d.$$

The period matrix of A is unique up to the action of the modular group $\mathrm{Sp}(4, \mathbb{Z})$, so the quotient $\mathrm{Sp}(4, \mathbb{Z})\backslash\mathbb{H}_2$ is precisely the coarse moduli space of complex p.p. abelian surfaces. In fact, this coarse moduli space $\mathcal{A}_2$ exists as a quasi-projective variety defined over $\mathbb{Q}$, and $\mathcal{A}_2(\mathbb{C})$ can be identified with $\mathrm{Sp}(4, \mathbb{Z})\backslash\mathbb{H}_2$.

A (scalar-valued) *Siegel modular form* on $\mathbb{H}_2$ of weight $k \in \mathbb{Z}_{\geq 0}$ (and level 1) is a complex-analytic map $f : \mathbb{H}_2 \to \mathbb{C}$ satisfying $f(\gamma\tau) = \det(\gamma^*\tau)^k f(\tau)$ for all $\tau \in \mathbb{H}_2$ and $\gamma \in \mathrm{Sp}(4, \mathbb{Z})$. See [Gee08] for more background on these objects. Siegel modular forms admit Fourier expansions: writing $\tau \in \mathbb{H}_2$ as

$$\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix}$$

and $q_j = \exp(2\pi i \tau_j)$ for $1 \leq j \leq 3$, the Fourier expansion of a Siegel modular form belongs to the power series ring $\mathbb{C}[q_3, q_3^{-1}][[q_1, q_2]]$.

By the Baily–Borel theorem, Siegel modular forms with rational Fourier coefficients yield projective embeddings of $\mathcal{A}_2$ that are defined over $\mathbb{Q}$, and can thus be used as rational coordinates on this moduli space. Igusa [Igu62] proved the following fundamental theorem.

Theorem 4.1. *The graded $\mathbb{C}$-algebra of Siegel modular forms on $\mathbb{H}_2$ of even weight is free with four generators M_4, M_6, M_{10}, M_{12} of weights $4, 6, 10, 12$ with integral Fourier coefficients.*

In this paper, we normalize these generators so that their Fourier expansions are primitive and M_{10}, M_{12} are cusp forms. This defines them uniquely up to sign. We can fix these signs by specifying their first few Fourier coefficients:

$$\begin{aligned} M_4(\tau) &= 1 + 240(q_1 + q_2) + O\big(q_1^2, q_2^2, q_1q_2\big), \\ M_6(\tau) &= 1 - 504(q_1 + q_2) + O\big(q_1^2, q_2^2, q_1q_2\big), \\ M_{10}(\tau) &= \big(q_3 - 2 + q_3^{-1}\big)q_1q_2 + O(q_1^2, q_2^2), \qquad \text{and} \\ M_{12}(\tau) &= \big(q_3 + 10 + q_3^{-1}\big)q_1q_2 + O\big(q_1^2, q_2^2\big). \end{aligned}$$

We find this normalization more convenient than the ones usually considered in the literature. In terms of Igusa's notation in [Igu62], we have

$$M_4 = \psi_4, \quad M_6 = \psi_6, \quad M_{10} = 4\chi_{10}, \quad \text{and} \quad M_{12} = 12\chi_{12}.$$

In terms of the modular forms h_k for $k \in \{4, 6, 10, 12\}$ from [Str14, §7.1], we have

$$M_4 = 2^{-2}h_4, \quad M_6 = 2^{-2}h_6, \quad M_{10} = -2^{-12}h_{10}, \quad \text{and} \quad M_{12} = 2^{-15}h_{12}. \tag{4.2}$$

From Theorem 4.1, we deduce that for each $\tau \in \mathbb{H}_2$, at least one of the values $M_k(\tau)$ for $k \in \{4, 6, 10, 12\}$ does not vanish.

Igusa [Igu79] further determined an explicit set of fourteen generators for the graded ring of Siegel modular forms with integral Fourier coefficients, which contains the above forms M_k. The following easy corollary of Igusa's result will play an essential role in this paper.

Proposition 4.3 ([Kie22b, §2.1]). *Let f be a Siegel modular form on $\mathbb{H}_2$ of even weight k with integral Fourier coefficients. Then $12^k f \in \mathbb{Z}[M_4, M_6, M_{10}, M_{12}]$.*

If f is a Siegel modular form of weight k with rational Fourier coefficients, then we can also give f an algebraic meaning as follows [FC90, Def. 1.1 p. 137]. Let A be a p.p. abelian surface over a number field L embedded in $\mathbb{C}$, and let ω be a basis of the 1-dimensional L-vector space $\wedge^2\Omega^1(A)$. Then $f(A,\omega)$ is a well-defined element of L, and satisfies $f(A, t\omega) = t^{-k} f(A,\omega)$ for all $t \in L^\times$.

The relation between $f(A,\omega)$ and the values of f on the Siegel half space $\mathbb{H}_2$ is the following [FC90, p. 141]. Let $\tau \in \mathbb{H}_2$ be a period matrix of A, and choose an isomorphism $\eta\colon A(\mathbb{C}) \to \mathbb{C}^2/(\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2)$. The basis of differential forms $(2\pi i\, dz_1, 2\pi i\, dz_2)$ induces a natural basis of $\wedge^2\Omega^1$ on the complex torus; call this basis $\omega(\tau)$. There is a unique $r \in \mathbb{C}^\times$ such that $\omega = r \cdot \eta^*\omega(\tau)$. Then $f(A,\omega) = r^{-k} f(\tau)$; one can check that this quantity $f(A,\omega)$ does not depend on the choice of τ or η.

Let now A be a p.p. abelian surface over $\mathbb{Q}$, and choose a basis ω of $\wedge^2\Omega^1(A)$. Then the weighted projective point

$$\big(M_4(A,\omega) : M_6(A,\omega) : M_{10}(A,\omega) : M_{12}(A,\omega)\big) \in \mathbb{P}^{4,6,10,12}(\mathbb{Q}) \tag{4.4}$$

is independent of ω, since scaling ω by $t^{-1} \in \mathbb{Q}^\times$ scales the above coordinates by $(t^4, t^6, t^{10}, t^{12})$. We call this projective point the *modular invariants* of A. This projective point has a unique representative $(m_4, m_6, m_{10}, m_{12}) \in \mathbb{Z}^4$ that is reduced in the sense that no prime p satisfies $p^k \mid m_k$ for all $k \in \{4, 6, 10, 12\}$; by a slight abuse of language, we also call this tuple of integers the modular invariants of A.

If A is the Jacobian of a genus 2 curve C defined over $\mathbb{Q}$, then the modular invariants of A can be computed as follows. Let $(I_2 : I_4 : I_6 : I_{10}) \in \mathbb{P}^{2,4,6,10}(\mathbb{Q})$ be the Igusa–Clebsch invariants of C as defined in [Str14, §2.1]; these invariants are also denoted by $(A : B : C : D)$ in [Igu62] and $(A' : B' : C' : D')$ in [Mes91]. Then, as a consequence of (4.2), the modular invariants of A are

$$(m_4 : m_6 : m_{10} : m_{12}) = \big(2^{-2} I_4 : 2^{-3}(I_2 I_4 - 3I_6) : -2^{-12} I_{10} : 2^{-15} I_2 I_{10}\big). \tag{4.5}$$

In particular, on the input of C, the modular invariants of A can easily be computed from the expression of $I_2, \ldots, I_{10}$ as polynomials in the coefficients of C.

4.2. Hecke correspondences. Consider a period matrix $\tau \in \mathbb{H}_2$ attached to a p.p. abelian surface A over $\mathbb{C}$. Then the period matrices of abelian surfaces linked to A by an isogeny of a given type can be computed by letting certain symplectic matrices act on τ. This precisely corresponds to analytic formulas for the action of Hecke operators on spaces of Siegel modular forms [CG15, §10], [Kri90, Chap. VI, §5]. The case of 1-step isogenies corresponds to the Hecke operator usually denoted by $T(\ell)$, and 2-step isogenies correspond to the Hecke operator $T_1(\ell^2)$. Concretely, we define the following collections of matrices:

(1) $S(\ell)$ consists of the $\ell^3 + \ell^2 + \ell + 1$ matrices of the form

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & b & c \\ 0 & 0 & \ell & 0 \\ 0 & 0 & 0 & \ell \end{pmatrix}, \quad \begin{pmatrix} \ell & 0 & 0 & 0 \\ -a & 1 & 0 & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & \ell \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & a & 0 \\ 0 & \ell & 0 & 0 \\ 0 & 0 & \ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \ell & 0 & 0 & 0 \\ 0 & \ell & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where a, b, c run through $\{0, \ldots, \ell - 1\}$;

(2) $S(\ell^2)$ consists of the $\ell^4 + \ell^3 + \ell^2 + \ell$ matrices of the following form:

$$\begin{pmatrix} \ell & 0 & 0 & a\ell \\ -b & 1 & a & ab+d \\ 0 & 0 & \ell & b\ell \\ 0 & 0 & 0 & \ell^2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & d & -a \\ 0 & \ell & -\ell a & 0 \\ 0 & 0 & \ell^2 & 0 \\ 0 & 0 & 0 & \ell \end{pmatrix}, \quad \begin{pmatrix} \ell^2 & 0 & 0 & 0 \\ -a\ell & \ell & 0 & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & \ell \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \ell & 0 & 0 & 0 \\ 0 & \ell^2 & 0 & 0 \\ 0 & 0 & \ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where a, b run through $\{0, \ldots, \ell - 1\}$ and d runs through $\{0, \ldots, \ell^2 - 1\}$; as well as

$$\begin{pmatrix} \ell & 0 & a & b \\ 0 & \ell & b & c \\ 0 & 0 & \ell & 0 \\ 0 & 0 & 0 & \ell \end{pmatrix}$$

where a, b, c run through $\{0, \ldots, \ell - 1\}$ with the additional conditions that $ac = b^2$ and $(a, b, c) \neq (0, 0, 0)$.

The set $S(\ell)$ (resp. $S(\ell^2)$) consists of matrices in $\mathrm{GSp}(4, \mathbb{R})^+$ with integral coefficients, zero lower left block, and with the property that the determinant of their lower right block divides ℓ^2 (resp. ℓ^3).

Proposition 4.6. *Let $\tau \in \mathbb{H}_2$, let $A = \mathbb{C}^2/(\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2)$ be the p.p. complex abelian surface attached to τ, and let ℓ be a prime number.*

(1) The matrices $\gamma\tau$ for $\gamma \in S(\ell)$ are period matrices for the abelian surfaces A/K where K runs through the maximal isotropic subgroups of $A[\ell]$.
(2) The matrices $\gamma\tau$ for $\gamma \in S(\ell^2)$ are period matrices for the abelian surfaces A/K where K runs through the maximal isotropic subgroups of $A[\ell^2]$ isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2 \times (\mathbb{Z}/\ell^2\mathbb{Z})$.

Proof. First, we consider 1-step isogenies. Consider the subgroup $\Gamma^0(\ell)$ of $\mathrm{Sp}_4(\mathbb{Z})$ defined as

$$\Gamma^0(\ell) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(4, \mathbb{Z}) : b = 0 \pmod{\ell} \right\}.$$

The map

$$\tau \mapsto \big(\mathbb{C}^2/(\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2), (\mathbb{Z}^2 \oplus \tfrac{1}{\ell}\tau\mathbb{Z}^2)/(\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2)\big)$$

is a bijection between $\Gamma^0(\ell)\backslash\mathbb{H}_2$ and the set of isomorphism classes of pairs (A, K), where A is a p.p. abelian surface over $\mathbb{C}$ and $K \subset A[\ell]$ is maximal isotropic for the Weil pairing. (This is proved in an analogous way to [BL09, Thm. 3.2], which uses the subgroup $\Gamma_0(\ell)$ instead.) The quotient surface A/K admits $\frac{1}{\ell}\tau$ as a period matrix. The period matrices we wish to enumerate are therefore the $\frac{1}{\ell}\gamma\tau$, where γ runs through a (finite) set of representatives of $\Gamma^0(\ell)\backslash \mathrm{Sp}(4, \mathbb{Z})$.

We can rewrite these matrices using the action of $\mathrm{GSp}(4, \mathbb{Q})^+$, noting that for all $\gamma \in \mathrm{Sp}(4, \mathbb{Z})$,

$$\big(\mathrm{Diag}(1, 1, \ell, \ell)\gamma\big) \cdot \tau = \tfrac{1}{\ell}(\gamma\tau).$$

This leads us to the formalism of Hecke operators in terms of double cosets: we have

$$\Gamma^0(\ell) = \mathrm{Sp}(4, \mathbb{Z}) \cap \mathrm{Diag}(1, 1, \ell, \ell)^{-1} \, \mathrm{Sp}(4, \mathbb{Z}) \, \mathrm{Diag}(1, 1, \ell, \ell),$$

so the map $\gamma \mapsto \mathrm{Diag}(1, 1, \ell, \ell)\gamma$ induces a bijection

$$\Gamma^0(\ell)\backslash \mathrm{Sp}(4, \mathbb{Z}) \to \mathrm{Sp}(4, \mathbb{Z})\backslash \mathrm{Sp}(4, \mathbb{Z}) \, \mathrm{Diag}(1, 1, \ell, \ell) \, \mathrm{Sp}(4, \mathbb{Z}).$$

By [CG15, Prop. 10.1], the set $S(\ell)$ is a set of representatives for the coset space on the right hand side (we acted on some representatives by elements of $\mathrm{Sp}_4(\mathbb{Z})$ to simplify them). This proves (1).

The 2-step case is similar. The reduction map $\mathrm{Sp}(4, \mathbb{Z}) \to \mathrm{Sp}(4, \mathbb{Z}/\ell^2\mathbb{Z})$ is surjective (see [BL09, §3]), and we define $\Gamma^0(\ell^2)$ as the preimage in $\mathrm{Sp}(4, \mathbb{Z})$ of the stabilizer of the maximal isotropic subgroup $\langle (0,\ell,0,0),(0,0,1,0),(0,0,0,\ell)\rangle$ in $(\mathbb{Z}/\ell^2\mathbb{Z})^4$. The map

$$\tau \mapsto \big(\mathbb{C}^2/(\mathbb{Z}^2\oplus\tau\mathbb{Z}^2), (\mathbb{Z}\oplus\tfrac{1}{\ell}\mathbb{Z})\oplus\tau(\tfrac{1}{\ell^2}\mathbb{Z}\oplus\tfrac{1}{\ell}\mathbb{Z}))/(\mathbb{Z}^2\oplus\tau\mathbb{Z}^2)\big)$$

is a bijection between $\Gamma^0(\ell^2)\backslash\mathbb{H}_2$ and the set of isomorphism classes of pairs (A,K), where A is a p.p. abelian surface over $\mathbb{C}$ and $K\subset A[\ell^2]$ is a maximal isotropic subgroup for the Weil pairing and isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2\times\mathbb{Z}/\ell^2\mathbb{Z}$. A period matrix for the quotient abelian surface A/K is then $\operatorname{Diag}(1,\ell,\ell^2,\ell)\,\tau$. As above, a reformulation in terms of double cosets will be convenient. We have

$$\Gamma^0(\ell^2) = \operatorname{Sp}(4,\mathbb{Z})\cap\operatorname{Diag}(1,\ell,\ell^2,\ell)^{-1}\operatorname{Sp}(4,\mathbb{Z})\operatorname{Diag}(1,\ell,\ell^2,\ell),$$

so the map $\gamma\mapsto\operatorname{Diag}(1,\ell,\ell^2,\ell)\gamma$ induces a bijection

$$\Gamma^0(\ell^2)\backslash\operatorname{Sp}(4,\mathbb{Z})\to\operatorname{Sp}(4,\mathbb{Z})\backslash\operatorname{Sp}(4,\mathbb{Z})\operatorname{Diag}(1,\ell,\ell^2,\ell)\operatorname{Sp}(4,\mathbb{Z}).$$

Combining [CG15, Prop. 10.5] with [Kri90, Chap. VI, Lem. 5.2], we find that $S(\ell^2)$ is exactly a set of representatives for the coset space on the right hand side. □

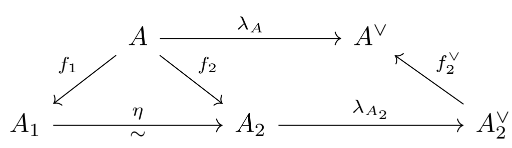
4.3. Rational invariants versus rational isogenies. Our algorithm will enumerate period matrices $\gamma\tau$ using Proposition 4.6 and evaluate the modular forms M_k at these points. If $\gamma\tau$ corresponds to an abelian surface A' that is isogenous to A over $\mathbb{Q}$, then $\big(M_4(\gamma\tau):M_6(\gamma\tau):M_{10}(\gamma\tau):M_{12}(\gamma\tau)\big)$ must be rational as a weighted projective point, i.e. up to complex scaling with the correct weights. In fact, the converse statement also holds.

Proposition 4.7. *Let A be a typical p.p. abelian surface over $\mathbb{Q}$, let τ be a period matrix of A, let ℓ be a prime number, and let $i\in\{1,2\}$. Then*

(1) As γ runs through $S(\ell^i)$, the projective points $\big(M_4(\gamma\tau):\cdots:M_{12}(\gamma\tau)\big)$ in $\mathbb{P}^{4,6,10,12}(\mathbb{C})$ are all distinct.

(2) Fix $\gamma\in S(\ell^i)$, and assume that there exists a scalar $\lambda\in\mathbb{C}^\times$ such that $\lambda^k M_k(\gamma\tau)\in\mathbb{Q}$ for each $k\in\{4,6,10,12\}$. Then $\gamma\tau$ is a period matrix of a p.p. abelian surface A', defined over $\mathbb{Q}$, such that there exists an i-step isogeny $A\to A'$ of degree ℓ^{2i} defined over $\mathbb{Q}$.

Proof. We first prove (1) by contradiction. If these projective points happen to be equal for some $\gamma_1\neq\gamma_2$, then we have a (non-commutative) diagram



where f_1,f_2 are isogenies with distinct kernels, and η is an isomorphism. Then the compositions $\eta\circ f_1\circ\lambda_A^{-1}\circ f_2^\vee\circ\lambda_{A_2}$ and $f_2\circ\lambda_A^{-1}\circ f_2^\vee\circ\lambda_{A_2}$ yield elements of $\operatorname{End}((A_2)_{\overline{\mathbb{Q}}})=\mathbb{Z}$ of the same degree ℓ^{2i}. They must therefore be equal up to sign. Thus $\eta\circ f_1=\pm f_2$ and $\ker f_1=\ker f_2$, a contradiction.

For (2), let K be the subgroup of A attached to γ. If K is not defined over $\mathbb{Q}$, then the Galois orbit of K consists of several subgroups of A, and the associated quotients have the same modular invariants, contradicting (1). Therefore K and the associated isogeny are defined over $\mathbb{Q}$. □

4.4. Certification. By Proposition 4.7, evaluating modular invariants and detecting when they are rational suffices to detect rational isogenies. In practice however, we will have to manipulate these complex numbers up to some finite precision. While rational invariants can still be detected heuristically and the isogeny might be proved to exist by other methods, certifying the non-existence of a rational isogeny is not immediate.

A key idea to achieve certification is to leverage the fact that we manipulate modular forms with integral Fourier coefficients to compute algebraic integers instead of just complex numbers. This technique is inspired from the description of denominators for modular equations in [Kie22b], and allows us to rule out non-rational isogenies. As a byproduct, we are also able to certify the existence of rational isogenies using computations over $\mathbb{C}$ only.

Concretely, let A, τ and ℓ be as in Proposition 4.7, and denote the modular invariants of A as defined in §4.1 by $(m_4, m_6, m_{10}, m_{12}) \in \mathbb{Z}^4$. Then there exists a scalar $\lambda \in \mathbb{C}^\times$, uniquely determined up to sign (but dependent on τ), such that

$$\lambda^k M_k(\tau) = m_k \text{ for all } k \in \{4, 6, 10, 12\}. \tag{4.8}$$

Let f be a Siegel modular form of even weight k with integral Fourier coefficients. For $\gamma \in S(\ell^i)$, we define

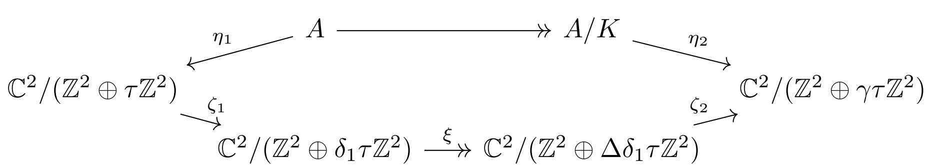
$$N(f, \gamma) \coloneqq (12\lambda)^k (\ell^d \det(\gamma^* \tau)^{-1})^k f(\gamma\tau). \tag{4.9}$$

with $d = 2$ if $i = 1$, and $d = 3$ if $i = 2$. (The central factor $\ell^d \det(\gamma^*\tau)^{-1}$ is a power of ℓ independent of τ.) We will show that the $N(f, \gamma)$ are in fact algebraic integers.

The first step is to reinterpret the complex numbers $N(f, \gamma)$ algebraically. Let ω be a basis of $\wedge^2 \Omega^1(A)$ such that $M_j(A, \omega) = m_j$ for all $j \in \{4, 6, 10, 12\}$, and let K be the subgroup of A corresponding to γ via the correspondence of Proposition 4.6. The subgroup K is not necessarily defined over $\mathbb{Q}$; let L be its field of definition, which is a number field embedded in $\mathbb{C}$. Then pulling back differential forms along the quotient isogeny $A \to A/K$ induces a bijection between the L-vector spaces $L \otimes_{\mathbb{Q}} \Omega^1(A)$ and $\Omega^1(A/K)$. Under this bijection, ω corresponds to an L-basis ω' of $\wedge^2 \Omega^1(A/K)$.

Lemma 4.10. *With the above notation, we have* $N(f, \gamma) = 12^k f(A/K, \omega')$.

Proof. By [BL04, Rem. 8.1.4], for every $\tau' \in \mathbb{H}_2$ and $\gamma \in \mathrm{Sp}(4, \mathbb{Z})$, the map $z \mapsto (\gamma^*\tau')^{-t} z$ defines an isomorphism between the abelian surfaces $\mathbb{C}^2/(\mathbb{Z}^2 \oplus \tau'\mathbb{Z}^2)$ and $\mathbb{C}^2/(\mathbb{Z}^2 \oplus (\gamma\tau')\mathbb{Z}^2)$. Keeping the notation from above the lemma, we write $\gamma = \delta_2 \Delta \delta_1$ where $\delta_1, \delta_2 \in \mathrm{Sp}(4, \mathbb{Z})$ and Δ is either $\mathrm{Diag}(1, 1, \ell, \ell)$ or $\mathrm{Diag}(1, \ell, \ell^2, \ell)$ depending on i. We then consider the commutative diagram



where ζ_1 (resp. ζ_2) is the isomorphism $z \mapsto (\delta_1^*\tau)^{-t} z$ (resp. $z \mapsto (\delta_2^*(\Delta\delta_1\tau))^{-t} z$), double-tipped arrows denote natural quotient maps, η_1 is an isomorphism of complex tori, and η_2 is another isomorphism that is determined by the choice of η_1. We recall that $\omega(\tau)$ denotes the element $2\pi i dz_1 \wedge 2\pi i dz_2$ of $\wedge^2\Omega^1\big(\mathbb{C}^2/(\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2)\big)$, where z_1, z_2 are the coordinates of $\mathbb{C}^2$. Let $r \in \mathbb{C}^\times$ be chosen such that $\omega' = r\,\eta_2^*\,\omega(\gamma\tau)$ as differential forms on A/K. We have $f(A/K,\omega') = r^{-k} f(\gamma\tau)$. Using the bottom line of the diagram, we find that

$$\omega(\tau) = \det(\delta_1^*\tau)\cdot\det\big(\delta_2^*(\Delta\delta_1\tau)\big)\cdot(\zeta_2\circ\xi\circ\zeta_1)^*\,\omega(\gamma\tau).$$

We can rewrite this equality using the following cocycle relation:

$$\gamma^*\tau = (\delta_2\Delta\delta_1)^*\tau = \delta_2^*(\Delta\delta_1\tau)\cdot\Delta^*(\delta_1\tau)\cdot\delta_1^*\tau.$$

As $\det\Delta^*(\delta_1\tau) = \ell^d$, we have

$$\omega(\tau) = \ell^{-d}\det(\gamma^*\tau)\cdot(\zeta_2\circ\xi\circ\zeta_1)^*\,\omega(\gamma\tau)$$

We deduce that $\omega = r\,\ell^d\det(\gamma^*\tau)^{-1}\eta_1^*\omega(\tau)$ as differential forms on A, and thus $\lambda = \pm r^{-1}\ell^{-d}\det(\gamma^*\tau)$. From (4.9), we finally obtain

$$N(f,\gamma) = 12^k r^{-k} f(\gamma\tau) = 12^k f(A/K,\omega'). \qquad \square$$

Theorem 4.11. *Let A be a p.p. abelian surface defined over $\mathbb{Q}$, let $\tau\in\mathbb{H}_2$ be a period matrix of A, let ℓ be a prime, and let $i\in\{1,2\}$. For a Siegel modular form f on $\mathbb{H}_2$ of even weight with integral Fourier coefficients and $\gamma\in S(\ell^i)$ (cf. §4.2), we define $N(f,\gamma)$ as in equation (4.9). Then*

(1) For each such modular form f, the set $\{N(f,\gamma) : \gamma\in S(\ell^i)\}$ is a Galois-stable set of algebraic integers. Moreover, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on this set corresponds to the Galois action on subgroups of $A[\ell^i]$ via the correspondence of Proposition 4.6.

(2) If $\gamma\in S(\ell^i)$ corresponds to a subgroup K of A that is defined over $\mathbb{Q}$, then

$$\big(N(M_4,\gamma) : N(M_6,\gamma) : N(M_{10},\gamma) : N(M_{12},\gamma)\big)\in\mathbb{P}^{4,6,10,12}(\mathbb{Q})$$

are the modular invariants of the quotient A/K in the sense of §4.1.

Proof. By Lemma 4.10, the complex numbers $N(f,\gamma)$ are in fact algebraic, form a Galois-stable set, and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on them corresponds to the Galois action on subgroups of A. We now show that the $N(f,\gamma)$ are algebraic integers. To this end, we construct the monic polynomial

$$P(X) = \prod_{\gamma\in S(\ell^i)}\big(X - N(f,\gamma)\big).$$

Let $n = \deg(P) = \#S(\ell^i)$. Expanding the product, we observe as in [Kie22b, Prop. 2.4] that for each $0\le j\le n$, the coefficient of X^{n-j} in P takes the form

$$(12\lambda)^{kj}\cdot g_j(\tau),$$

where g_j is a Siegel modular form of weight kj with integral Fourier coefficients. By Proposition 4.3, the modular form $12^{kj}g_j$ is an element of $\mathbb{Z}[M_4,M_6,M_{10},M_{12}]$ of weight kj. Therefore

$$(12\lambda)^{kj}g_j(\tau)\in\mathbb{Z}[m_4,m_6,m_{10},m_{12}] = \mathbb{Z}.$$

Thus P has integral coefficients, which concludes the proof of (1).

Item (2) is a direct consequence of Lemma 4.10: we showed the existence of a basis ω of the $\mathbb{Q}$-vector space $\wedge^2\Omega^1(A/K)$ such that $N(M_k,\gamma) = 12^k M_k(A/K,\omega)$ for all $k\in\{4,6,10,12\}$, and absorbing the scalar factors 12^k does not modify the projective point. $\square$

4.5. Outline of the algorithm. Now that the theoretical background is set, we describe the concrete computations over $\mathbb{C}$ that we perform to list the rational 1- or 2-step isogenies from a given typical p.p. abelian surface A over $\mathbb{Q}$. We take the modular invariants of A as input. If A is given as the Jacobian of a genus 2 curve over $\mathbb{Q}$ as in Algorithm 2.5, then its modular invariants can be determined by polynomial formulas in terms of the coefficients of the curve, as explained in §4.1. Similarly, the output will consists of modular invariants of isogenous abelian surfaces: we refer to Section 5 for the subsequent reconstruction of genus 2 curve equations.

In the whole algorithm, we use interval arithmetic to keep track of precision losses: each complex number is encoded as a ball that provably contains the exact value. Of course, we need to assume more than mere correctness of the underlying arithmetic for our algorithms to work, as we will not get far if every operation returns the whole of $\mathbb{C}$. A minimal assumption in this subsection is that any given computation with exact input will output a complex ball whose radius tends to zero as its *working precision* tends to infinity. This will ensure that our algorithms terminate. In fact, we have a precise control on the precision losses incurred during the computations: we postpone this discussion to the complexity analysis in §4.6.

There are two main stages in the algorithm. First, we use low-precision computations to filter out symplectic matrices $\gamma \in S(\ell)$ or $S(\ell^2)$ whose associated $N(f, \gamma)$, seen as a ball, does not contain any rational integer. By Theorem 4.11, these matrices γ do not correspond to rational isogenies with domain A. One expects that all remaining subgroups correspond to rational isogenies. Second, we use high-precision computations to either certify or disprove that the remaining subgroups are defined over $\mathbb{Q}$. We will use two black boxes, namely the computation of a period matrix from modular invariants and the evaluation the Siegel modular forms M_k at a point of $\mathbb{H}_g$; we also refer to §4.6 for a discussion of these steps. In the first stage, we proceed as follows.

Algorithm 4.12. *Input:*

- the modular invariants m_4, m_6, m_{10}, m_{12} of a p.p. abelian surface A over $\mathbb{Q}$,
- a prime number ℓ, and $i \in \{1, 2\}$ indicating either 1-step or 2-step isogenies.

Output:

- a period matrix τ of A (to low precision),
- a list L of symplectic matrices that provably contains all $\gamma \in S(\ell^i)$ associated with a rational subgroup of $A[\ell^i]$ for this choice of τ,
- for each $\gamma \in L$ and $k \in \{4, 6, 10, 12\}$, a candidate value $m'_k(\gamma) \in \mathbb{Z}$ for the algebraic integer $N(M_k, \gamma)$ satisfying $|N(M_k, \gamma) - m'_k(\gamma)| \leq 2^{-10}$;
- for each $\gamma \notin L$ and $k \in \{4, 6, 10, 12\}$, a ball containing $N(M_k, \gamma)$ of radius at most 2^{-10}.

Step 1. Compute a low-precision approximation of a period matrix τ of A, see Theorem 4.17.

Step 2. Evaluate the modular forms $M_4, \ldots, M_{12}$ at τ, and deduce an approximation of the scaling factor λ as defined in §4.4.

Step 3. For each $\gamma \in S(\ell^i)$ and each $k \in \{4, 6, 10, 12\}$, evaluate $N(M_k, \gamma)$. If the radius of one of these approximations is larger than 2^{-10}, double the working precision and restart.

Step 4. Let L be the list of all γ such that each of the balls $N(M_k, \gamma)$ for $k \in \{4, 6, 10, 12\}$ contains an integer $m'_k(\gamma)$, and return the output listed above.

At the end of Algorithm 4.12, for each $\gamma \in L$, the integers $m'_k(\gamma)$ are the only possible values for the modular invariants of the isogenous abelian surface if it is indeed defined over $\mathbb{Q}$. One could stop here and certify the existence of an isogeny by other methods. In order to certify that these likely isogenies indeed exist using computations over $\mathbb{C}$ only, we proceed as follows.

Lemma 4.13. *Keep the notation of Algorithm 4.12. Let* $k \in \{4, 6, 10, 12\}$*, let* $m \in \mathbb{Z}$*, and let* $S_0 \subset S(\ell^i)$ *be a nonempty subset such that* $|N(M_k, \gamma) - m| \leq 1$ *for all* $\gamma \in S_0$*, and* $N(M_k, \gamma) \neq m$ *for all* $\gamma \in S(\ell^i) \backslash S_0$*. Let*

$$B = \prod_{\gamma \in S(\ell^i) \backslash S_0} |N(M_k, \gamma) - m|.$$

Then for each $\gamma \in S_0$*, the inequality* $|N(M_k, \gamma) - m| < \dfrac{1}{B}$ *holds if and only if* $N(M_k, \gamma) = m$*.*

Proof. Let $S_1 \subset S_0$ be the subset of matrices γ such that the equality $N(M_k, \gamma) = m$ holds, and consider the polynomial

$$P = \prod_{\gamma \in S(\ell^i)} \big(X - N(M_k, \gamma) + m\big) \in \mathbb{Z}[X], \quad \text{by Theorem 4.11.}$$

The coefficient of X^j in P is zero for $0 \leq j \leq \#S_1 - 1$, and the coefficient of $X^{\#S_1}$ is, up to sign,

$$\prod_{\gamma \in S(\ell^i) \backslash S_0} \big(N(M_k, \gamma) - m\big) \cdot \prod_{\gamma \in S_0 \backslash S_1} \big(N(M_k, \gamma) - m\big).$$

By construction, this integer is nonzero, hence at least 1 in absolute value. Thus, for every $\gamma \in S_0 \backslash S_1$, we have as claimed

$$|N(M_k, \gamma) - m| \geq \frac{1}{B}. \qquad \square$$

Algorithm 4.14. *Input:* the input and output of Algorithm 4.12.
Output: the modular invariants of all the p.p. abelian surfaces linked to A by an i-step ℓ-isogeny, as a list of integer-valued tuples $(m'_4, m'_6, m'_{10}, m'_{12})$.

Step 1. For each $\gamma_0 \in L$ and $k \in \{4, 6, 10, 12\}$, let $S_0 \subset L$ to be the set of all matrices γ such that $m'_k(\gamma) = m'_k(\gamma_0)$, and compute a low-precision upper bound for the quantity B as in Lemma 4.13. Let B_0 be their maximum value ranging over all γ_0 and k.

Step 2. Choose a higher working precision (more on this below). Recompute the period matrix τ, as well as $N(M_k, \gamma)$ for each $\gamma \in L$ and $k \in \{4, 6, 10, 12\}$.

Step 3. For each $\gamma \in L$ and $k \in \{4, 6, 10, 12\}$, check whether $N(M_k, \gamma)$ still contains the candidate value $m'_k(\gamma)$. If not, remove γ from L. If yes, check whether the inequality
$$|N(M_k, \gamma) - m'_k(\gamma)| < \frac{1}{B_0}$$
holds; if this cannot be decided, double the working precision and go back to Step 2.

Step 4. Output the list of tuples $(m'_4(\gamma), \ldots, m'_{12}(\gamma))$ for the remaining $\gamma \in L$.

As soon as all the radii of the balls containing $N(M_k, \gamma)$ are less than $\frac{1}{2B_0}$, there will be no further doubling of the working precision in Step 3, thus Algorithm 4.14 terminates. Lemma 4.13 guarantees that the algorithm is correct.

Remark 4.15. In practice, increasing the working precision by p bits results in output intervals whose radius is multiplied by roughly 2^{-p}. Therefore a good guess for the choice of high precision in Step 2 of Algorithm 4.14 is to add $\lceil \log_2(B_0) \rceil$ bits to the current working precision at the end of Algorithm 4.12. We then expect that no further precision increases are needed in Step 3.

4.6. Implementation details and complexity analysis. We conclude this section with a complexity analysis of the isogeny algorithm in terms of ℓ, i and the height of the integers m_k for $k \in \{4, 6, 10, 12\}$. First, we give an asymptotic upper bound on the absolute values $|N(M_k, \gamma)|$: this will specify the necessary working precisions in Algorithms 4.12 and 4.14. Then, we review previous works on the computation of period matrices and the evaluation of modular forms in quasi-linear time in terms of the required precision, filling in the two black boxes of §4.5.

We may fix a compact subset $\mathcal{G} \subset \mathbb{H}_2 \cup \{\infty\}$, where ∞ denotes the cusp at infinity, such that the period matrix τ in Step 1 of Algorithm 4.12 always belongs to $\mathcal{G}$. For instance, we can take $\mathcal{G}$ to be the set of points at a distance at most 2^{-10} from the Siegel fundamental domain $\mathcal{F}$ (see [Str14, §6.2]), plus the point ∞. Recall that the modular forms M_k are bounded in a neighborhood of ∞, never vanish simultaneously on $\mathbb{H}_2$, and that M_4 and M_6 take the value 1 at ∞. Thus there exist two absolute constants $0 < C_1 < C_2 < +\infty$ such that $M_k \leq C_2$ uniformly on $\mathcal{G}$ for each $k \in \{4, 6, 10, 12\}$, and $\max\big\{|M_k(\tau)| : k \in \{4, 6, 10, 12\}\big\} \geq C_1$ for each $\tau \in \mathcal{G}$.

Lemma 4.16. *In Algorithm 4.12, assume that $\tau \in \mathcal{G}$, and let*

$$h = \log \max\{|m_4|, \ldots, |m_{12}|\}.$$

Then in Step 2 of that algorithm, we have $\log|\lambda| = O(h)$. In Step 3, we have $\log|N(M_k, \gamma)| = O(h + \log \ell)$ for each $\gamma \in S(\ell^i)$ and $k \in \{4, 6, 10, 12\}$. Both implied constants are absolute.

Proof. For the first part, we have $\log|\lambda| \leq \frac{1}{4}(h - \log C_1)$. For the second part, we need to estimate $|M_k(\gamma\tau)|$. The matrix $\gamma\tau \in \mathbb{H}_2$ will not usually belong to $\mathcal{G}$, but its imaginary part is nevertheless "bounded below": if $a, b, 0, d$ denote the 2×2 blocks of γ, we have $\operatorname{Im}(\gamma\tau) = a \operatorname{Im}(\tau) d^{-1}$, so $\det \operatorname{Im}(\gamma\tau) \geq C_3/\ell^2$ where C_3 is an absolute constant. Let now $\eta \in \mathrm{Sp}(4, \mathbb{Z})$ be such that $\eta\gamma\tau \in \mathcal{G}$, and let $r = \det(\eta^*(\gamma\tau))$. Then by [Kli90, Proof of Prop. 1.1], we have

$$\det(\operatorname{Im}(\eta\gamma\tau)) = |r|^{-2} \det(\operatorname{Im}(\gamma\tau))$$

so $|r|^{-2} \leq C_4 \ell^2$, where C_4 is an absolute constant. Finally we have

$$\log|M_k(\gamma\tau)| = \log|r^{-k} M_k(\eta\gamma\tau)| = O(\log \ell)$$

where the implied constant is absolute. □

With these estimates in hand, we focus on the two key computations left aside in §4.5. From the data of modular invariants in $\mathbb{Z}$, a corresponding period matrix $\tau \in \mathcal{F}$ can be efficiently computed using arithmetic-geometric means, an algorithm described in [Dup06, Chap. 9] and proved correct in [Kie22a]. (In the first low-precision step, we could also use numerical integration [MN19], but the dependency of this algorithm on h has not been made explicit.)

Theorem 4.17 ([Kie22b, §4.1])**.** *There exists an algorithm which, given the modular invariants $m_4, \ldots, m_{12} \in \mathbb{Z}$ of a typical p.p. abelian surface A over $\mathbb{Q}$ and $p \geq 1$,* *computes an approximation of a period matrix $\tau \in \mathcal{F}$ of A up to an error of 2^{-p} within a running time of $\widetilde{O}(p+h)$ binary operations, where $h = \log\max\{|m_4|, \ldots, |m_{12}|\}$.*

In order to evaluate the modular forms M_k at a point $\gamma\tau \in \mathbb{H}_2$, we compute a matrix $\eta \in \mathrm{Sp}(4,\mathbb{Z})$ such that $\eta\gamma\tau$ is close to the fundamental domain $\mathcal{F}$ and evaluate $M_k(\eta\gamma\tau)$. The latter can be rewritten as polynomials in terms of theta constants at $\eta\gamma\tau$: see [Str14, §7.1] for explicit formulas. Following [Kie22b, §4.3], we can control the cost of the reduction step in terms of the quantity

$$\Lambda(\gamma\tau) = \log\max\{2, |\gamma\tau|, \det(\mathrm{Im}(\gamma\tau))^{-1}\},$$

where $|\gamma\tau|$ denotes the largest absolute value of an entry of $\gamma\tau$. As a consequence of [Str14, Cor. 7.8], we have $|\tau| = O(h)$, so $\Lambda(\gamma\tau) = O(\log h + \log\ell)$ where the implied constant is absolute. After the reduction step, the evaluation of theta constants on $\mathcal{F}$ can be done in uniform quasi-linear time using arithmetic-geometric means and Newton's method. The following result summarizes this approach.

Theorem 4.18 ([Kie22b, §4.3])**.** *There exists an algorithm and an absolute constant C_5 such that the following holds. Let $\tau \in \mathbb{H}_2$ and $p \geq 1$. Then, given an approximation of τ to precision $p + C_5\Lambda(\tau)$, the algorithm computes a matrix $\gamma \in \mathrm{Sp}(4,\mathbb{Z})$ such that $\log|\gamma| = O(\Lambda(\tau))$, a matrix $\tau' \in \mathcal{F}$ such that $|\tau' - \gamma\tau| \leq 2^{-p}$, and an approximation of the squares of theta constants at $\gamma\tau$ up to an error of 2^{-p}. Its running time is $\widetilde{O}(\Lambda(\tau)^2 + p)$ binary operations.*

We can now prove the complexity bound stated at the beginning of Section 4.

Corollary 4.19. *Let A be a typical p.p. abelian surface over $\mathbb{Q}$ with modular invariants $m_4, \ldots, m_{12}$, and let $h = \log\max\{|m_4|, \ldots, |m_{12}|\}$. Let ℓ be a prime, let $i \in \{1,2\}$, and let n be the size of the list L returned by Algorithm 4.12 on this input. Then one can run Algorithms 4.12 and 4.14 to detect i-step ℓ-isogenies with domain A using a total of $\widetilde{O}\big((n+1)\ell^d h\big)$ binary operations, where $d = 3$ when $i = 1$ and $d = 4$ when $i = 2$.*

Proof. By Lemma 4.16, in Step 3 of Algorithm 4.12, we need to evaluate $M_k(\gamma\tau)$ to $O(h + \log\ell)$ bits of precision for each $\gamma \in S(\ell^i)$. By Theorems 4.17 and 4.18, this can be done within $\widetilde{O}(\ell^d h)$ binary operations, as $\#S(\ell^i) = O(\ell^d)$. Similarly, in Algorithm 4.14, we have $\log|B_0| = O(\ell^d(h + \log\ell))$, so we need to evaluate $M_k(\gamma\tau)$ to $O\big(\ell^d(h+\log\ell)\big)$ bits of precision for each $\gamma \in L$. This can be done in $\widetilde{O}(n\ell^d h)$ binary operations. □

5. Reconstructing genus 2 curves

5.1. Mestre's algorithm. Given a quadruple of Igusa–Clebsch invariants $I = (I_2 : I_4 : I_6 : I_{10})$ over $\mathbb{Q}$, there always exists a genus 2 curve over $\overline{\mathbb{Q}}$ having these invariants, but it cannot always be defined over $\mathbb{Q}$. This phenomenon is known as Mestre's obstruction. Given I, Mestre [Mes91] constructs a conic L over $\mathbb{Q}$ together with an effective divisor D of degree 6 on this conic with the following properties. If $L(\mathbb{Q}) \neq \emptyset$ and hence $L \cong \mathbb{P}^1$, then there exists a genus 2 curve over $\mathbb{Q}$ with invariants I whose Weierstrass points correspond to the points in D. If $L(\mathbb{Q}) = \emptyset$, there is no genus 2 curve over $\mathbb{Q}$ having these invariants. This reconstruction algorithm has been implemented in many computer algebra systems and the reader is referred to [Mes91] for more details about the method.

In our setting, Mestre's obstruction does not arise, and $L(\mathbb{Q})$ is always nonempty. Indeed, by Proposition 4.7, we only manipulate typical p.p. abelian surfaces defined over $\mathbb{Q}$. By [Lau01, Appendix, Thm. 4], these surfaces all are Jacobians of genus 2 curves defined over $\mathbb{Q}$.

Mestre's algorithm usually produces curves with very large coefficients. Their sizes can be reduced by applying [SC03], which has been implemented in [PARI/GP] and [Magma]. Note that even this reduced model is not necessarily unique.

5.2. Identifying the correct twists. Having constructed a curve C' over $\mathbb{Q}$ from the invariants output by Algorithm 4.14, we have no guarantee yet that $\mathrm{Jac}(C)$ will be isogenous to $\mathrm{Jac}(C')$ over $\mathbb{Q}$: we can only say that $\mathrm{Jac}(C')$ is a twist of the abelian surface isogenous to $\mathrm{Jac}(C)$. Since $\mathrm{End}(\mathrm{Jac}(C')_{\overline{\mathbb{Q}}}) = \mathbb{Z}$, the only possible twists of $\mathrm{Jac}(C')$ are quadratic twists, and correspond to quadratic twists of the curve C' itself. Therefore, there will be a unique twist C'' of C' (up to isomorphism over $\mathbb{Q}$) such that $\mathrm{Jac}(C)$ is isogenous to $\mathrm{Jac}(C'')$.

We use the following method to find C''. For a genus 2 curve C and a prime of good reduction ℓ of $\mathrm{Jac}(C)$, we denote by $a_\ell(C) \in \mathbb{Z}$ the trace of Frobenius on the reduction on $\mathrm{Jac}(C)$ modulo ℓ.

Algorithm 5.1. *Input:* curves C and C' of genus 2 over $\mathbb{Q}$ with typical Jacobians, such that some twist of $\mathrm{Jac}(C')$ is isogenous to $\mathrm{Jac}(C)$.
Output: the unique twist C'' of C' such that $\mathrm{Jac}(C)$ is isogenous to $\mathrm{Jac}(C'')$.

Step 1. Compute a set $\mathcal{B}$ of primes containing the bad primes of C and C'. Let

$$G = \langle -1 \rangle \times \langle b : b \in \mathcal{B} \rangle \subset \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

Step 2. Find auxiliary primes $\ell_1, \ldots, \ell_k$ such that the Frobenius traces $a_{\ell_i}(C)$ are nonzero and the map

$$\mu \colon G \to \{\pm 1\}^k, \quad x \mapsto \left(\left(\frac{x}{\ell_i} \right) \right)_{1 \le i \le k}$$

is injective.

Step 3. Identify the unique element $g \in G$ for which the twist C'' of C' by g satisfies $a_{\ell_i}(C'') = a_{\ell_i}(C)$ for every $1 \le i \le k$, and return C''.

Proposition 5.2. *Algorithm 5.1 terminates and is correct.*

Proof. First, we will prove the existence of the auxiliary primes $\ell_1, \ldots, \ell_k$. By [CDSS17, Theorem 1] and the fact that $\mathrm{Jac}(C)$ is typical, the equality $a_\ell(C) = 0$ holds only for a density 0 subset of primes. Write $\mathcal{B} \cup \{-1\} = \{b_1, \ldots, b_k\}$. For each $1 \le i \le k$, by quadratic reciprocity, we can find congruence conditions on ℓ guaranteeing that $\left(\frac{b_i}{\ell}\right) = -1$ and $\left(\frac{b_j}{\ell}\right) = 1$ for each $j \neq i$. By Dirichlet's prime number theorem and the fact that only a density 0 subset of the primes are excluded, there exists a prime ℓ_i (in fact infinitely many) satisfying these congruence conditions and such that $a_{\ell_i}(C) \neq 0$. With this choice of $\ell_1, \ldots, \ell_k$, the map μ is injective.

Next, we recall the Néron–Ogg–Shafarevich criterion [ST68]: an abelian surface A has good reduction at a prime p if and only if for all primes $\ell \neq p$, the Galois representation $T_\ell(A)$ is unramified at p. Hence, if A has good reduction at p and A' is the quadratic twist of A by a squarefree integer D divisible by p, then A' has bad reduction at p. Indeed, the Galois representation $T_\ell(A')$ is obtained from $T_\ell(A)$ by tensoring with the quadratic character associated with $\mathbb{Q}(\sqrt{D})$, which is ramified at p. On the other hand, any abelian surface isogenous to A must have the same primes of bad reduction.

As a consequence, the correct twist $\mathrm{Jac}(C'')$ of $\mathrm{Jac}(C')$ is given by a squarefree integer D that can only be divisible by primes of bad reduction of $\mathrm{Jac}(C)$ or $\mathrm{Jac}(C')$. These form a subset of $\mathcal{B}$, so the correct twist is among those enumerated by G. By the choice of the auxiliary primes $\ell_1, \ldots, \ell_k$, the tuples of Frobenius traces $(a_{\ell_1}, \ldots, a_{\ell_k})$ take distinct values for all the twists enumerated by G, so there is a unique output in Step 3. ☐

Algorithm 5.1 has an exponential complexity in terms of the number of bad primes of C and C', but this number is small in practice.

Remark 5.3. In the case of elliptic curves, an analogue of Algorithm 5.1 would not be needed. Indeed, if E is an elliptic curve over $\mathbb{Q}$ with automorphism group $\{\pm 1\}$, then the modular invariants of E in $\mathbb{P}^{4,6}(\mathbb{Q})$ determine the $\mathbb{Q}$-isomorphism class of E, as twisting E by d multiplies its invariants by d^2 and d^3. Thus we would obtain the correct twist as a direct result of the computations over $\mathbb{C}$.

In genus 2 however, quadratic twists have the same modular invariants: this comes from the fact that twisting an abelian surface A by d acts on $\Omega^1(A)$ as $\mathrm{Diag}(\sqrt{d}, \sqrt{d})$, hence on $\wedge^2 \Omega^1(A)$ as multiplication by d, which is a rational number. Nevertheless, one would still be able to compute the correct twist directly (and thus circumvent Algorithm 5.1) by considering vector-valued Siegel modular forms, or equivalently by keeping track of big period matrices. This goes beyond the scope of this paper, and Algorithm 5.1 was sufficient for our experiments.

6. Examples

We now give explicit illustrations of the methods developed above. First, we discuss an example of a 1-step 31-isogeny; then, we report on the results of running our algorithm on a large dataset of Jacobians of genus 2 curves that includes the current LMFDB data [LMFDB]. The prime $\ell = 31$ is the largest prime for which the Galois representation on $A[\ell]$ is not surjective among all the abelian surfaces A in this dataset [BBKKMSV23].

All computations were ran on a server with an AMD EPYC 7713 2GHz CPU and Sage 9.7 [Sage], Magma 2.28-2 [Magma], GP/PARI 2.15.0 [PARI/GP], and `pydhme v0.0.6` installed.[3]

6.1. A 1-step 31-isogeny.

Consider the hyperelliptic curve

$$C\colon y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45.$$

The conductor of $\mathrm{Jac}(C)$ is $7^2 \cdot 31^2$. Combining this with the study of local Euler factors at $p \in \{3, 5, 11\}$, we see that $\mathcal{L}_1 = \emptyset$ and $\mathcal{L}_2 \subseteq \{31\}$ in the notation of §3.

The Igusa–Clebsch invariants $(I_2 : I_4 : I_6 : I_{10})$ of C in $\mathbb{P}^{2,4,6,10}(\mathbb{Q})$ are

$$(-324608 : 7340502400 : -589129410429504 : 5306537926135312384),$$

from which we can deduce that $\mathrm{Jac}(C)$ has the following modular invariants:

$$(m_4, m_6, m_{10}, m_{12}) = (1909600, 2582145496, 45252529, -59231181184).$$

[3] A Sage interface for [Kie23] is available at `https://github.com/edgarcosta/pyhdme/`.

We apply Algorithm 4.12 with $\ell = 31$ and $i = 1$. After computing a period matrix

$$\tau \approx \begin{pmatrix} 1.69708i & 0.31188 + 0.84854i \\ 0.31188 + 0.84854i & -0.18812 + 2.09922i \end{pmatrix}$$

in the Siegel fundamental domain with 300 bits of precision, we conclude that there is a unique coset representative

$$\gamma = \begin{pmatrix} 1 & 0 & 0 & 7 \\ 0 & 1 & 7 & 23 \\ 0 & 0 & 31 & 0 \\ 0 & 0 & 0 & 31 \end{pmatrix} \in S(31)$$

such that $N(M_4, \gamma)$ contains an integer. Indeed, we have

$$\begin{aligned} &|N(M_4,\gamma) - \alpha^2 \cdot 318972640| < 7.8 \times 10^{-47} \\ &|N(M_6,\gamma) - \alpha^3 \cdot 1225361851336| < 5.5 \times 10^{-39} \\ &|N(M_{10},\gamma) - \alpha^5 \cdot 10241530643525839| < 1.6 \times 10^{-29} \\ &|N(M_{12},\gamma) + \alpha^6 \cdot 307105165233242232724| < 4.6 \times 10^{-22} \end{aligned}$$

where $\alpha = 2^2 \cdot 3^2 \cdot 31$. We then employ Algorithm 4.14, working with 4 128 800 bits of precision, to certify that an abelian surface with projective invariants

$$(318972640, 1225361851336, 10241530643525839, -307105165233242232724)$$

is indeed isogenous to $\mathrm{Jac}(C)$ via a 1-step 31-isogeny.

Mestre's algorithm and a reduction algorithm (§5.1) yield the hyperelliptic curve

$$y^2 = -1624248x^6 + 5412412x^5 - 6032781x^4 + 876836x^3 - 1229044x^2 - 5289572x - 1087304.$$

Applying Algorithm 5.1 we learn that the desired curve C'' is the quadratic twist of this hyperelliptic curve by -83761, and is given by the equation

$$y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 + 406259311249x + 93951289752862$$

with discriminant $7^2 \cdot 31^3 \cdot 83761^{12}$.

The overall computation took 175 minutes of CPU time and used 6.5 gigabytes of ram, of which roughly 90% is spent certifying the existence of an isogeny between these two curves, i.e. in Algorithm 4.14.

Given C and C'', we can also independently produce a certificate for the existence of an isogeny of the correct degree [CMSV19]. It took about 6.5 CPU hours to produce the 2.8 megabyte certificate.

6.2. LMFDB and beyond. We now report on the application of our algorithms to a dataset of 1 743 737 genus 2 curves with trivial geometric endomorphism algebra. These are all the typical abelian surfaces in a dataset of approximately 5 million curves with conductor up to 2^{20} provided to us by Andrew Sutherland [Sut22]. This dataset expands the current set of genus 2 curves in the L-functions and modular forms database (LMFDB) [LMFDB].

The 1 743 737 curves are split among 1 440 894 isogeny classes, while the LMFDB subset contains 63 107 curves split among 62 600 isogeny classes. These isogeny classes have been identified using Frobenius traces only [BSSVY16, §4.3], a heuristic method whose results are confirmed by our computations.

We have applied our algorithms to one curve per isogeny class and found 600 948 new curves in total. Table 1 lists the degrees of the irreducible isogenies that we found (in other words we ignore 2-step isogenies arising as the composition of two rational 1-step isogenies), and Table 2 shows the sizes of the 1 440 894 isogeny classes. Most of the large classes only feature Richelot isogenies, i.e. 1-step 2-isogenies. In total, however, only 242 442 of the 600 948 new curves can be reached from the original dataset via Richelot isogenies.

d	Number of isogenies of degree d	d	Number of isogenies of degree d
2^2	419 157	7^4	246
2^4	693 519	11^4	9
3^2	11 568	13^2	20
3^4	29 742	13^4	9
5^2	415	17^2	4
5^4	2 440	31^2	1
7^2	154		

TABLE 1. Number of isogenies of each degree in the extended dataset.

k	Number of isogeny classes of size k	k	Number of isogeny classes of size k
1	1 032 456	12	52
2	116 847	14	102
3	197 253	16	1 555
4	54 543	18	706
5	15 547	20	120
6	14 323	22	99
7	430	24	6
8	5 594	28	4
9	35	30	8
10	1 214		

TABLE 2. Distribution of isogeny class sizes in the extended dataset.

Remark 6.1. It is worth noting that 195 806 of the 197 253 isogeny classes of size 3 and 15 523 of the 15 547 isogeny classes of size 5 are only made up of 2-step 2-isogenies, of degree 16. The isogeny graphs in these two cases are a triangle $\triangle$ and a bowtie $\bowtie$ respectively. Moreover, there is no isogeny class of size 2 made of a single 2-step 2-isogeny.

These observations can be explained as follows: the existence of a 2-step 2-isogeny $\varphi_1 \colon A_1 \to A_2$ always implies the existence of a triangle consisting of three 2-step 2-isogenies. Indeed, assume that $\ker f$ is generated by $e_1, 2e_2, 2f_2$, where (e_1, e_2, f_1, f_2) is a symplectic basis of $A_1[4]$. Then the subgroup generated by $e_1 + 2f_1, 2e_2, 2f_2$ is another rational maximal isotropic subgroup of $A_1[4]$, and gives rise to an isogeny $\varphi_2 \colon A_1 \to A_3$. Furthermore, one can show that there exists another 2-step 2-isogeny $\varphi_3 \colon A_2 \to A_3$ such that $\varphi_2 \circ [2] = \varphi_3 \circ \varphi_1$.

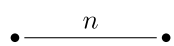
The whole computation took 111 days of CPU time and used 215 megabytes of RAM on average per class. Only 30 classes taking more than 10 minutes. In these

29 cases, we had to search for and potentially certify isogenies of large degree. For 6 of the classes, it took on average 18 minutes to prove the nonexistence of 1 and 2-step 29-isogenies; one of them has LMFDB label 976.a, and contains a Jacobian with a 29-torsion point. The remainder correspond to $23 = 9 + 9 + 4 + 1$ isogeny classes consisting of exactly two abelian surfaces linked by isogenies of degrees 11^4, 13^4, 17^2, and 31^2 respectively, as listed in Table 1. The only class that took more than 1.5 hours is the example discussed in §6.1, featuring the isogeny of degree 31^2.

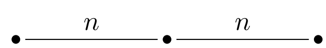
The largest degree of an irreducible isogeny was 13^4. For example, the class 349.a has two abelian surfaces connected by such an isogeny, namely the Jacobians of the two curves

$$349.a.349.1\colon y^2 + (x^3 + x^2 + x + 1)y = -x^3 - x^2$$
$$C\colon y^2 + y = x^5 - 363x^4 - 2517x^3 + 151106x^2 + 487525x - 16355862.$$

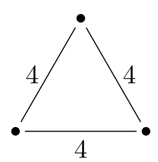
Table 3 continues our zoological study of isogeny graphs by listing all graphs on at most four vertices that we observed. We label an edge by ℓ (resp. ℓ^2) when it corresponds to a 1-step (resp. 2-step) ℓ-isogeny.

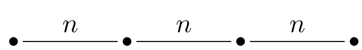


for $n \in \{2, 3, 5, 7, 13, 17, 31, 9, 25, 49, 121, 169\}$

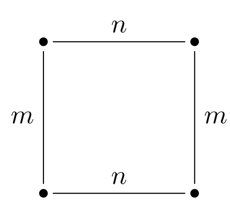


for $n \in \{3, 5, 7, 9\}$

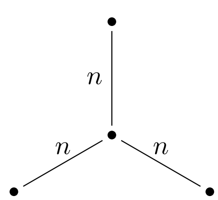




for $n \in \{3, 5\}$



for $(m, n) \in \{(2, 3), 2, 5), (2, 9), (2, 25), (3, 3), (5, 9), (9, 25)\}$



for $n \in \{2, 3\}$

Table 3. Observed isogeny graphs with 2 to 4 vertices.

The 1 440 894 isogeny classes represent 71 non-isomorphic graphs, the largest having size 30 (see `https://github.com/edgarcosta/genus2isogenies/tree/main/data/graphs_2e20`). In every class containing 18 or more abelian surfaces, the only irreducible isogenies are Richelot isogenies.

Despite the size of our dataset, this list of graphs is not complete. The following curve, suggested by Noam Elkies, gives rise to an isogeny graph consisting of 42 vertices connected by Richelot isogenies:

$$y^2 = (x+4)(x+11)(4x-1)(12x+13)(15x-4).$$

This curve has conductor $2^{24}\cdot 3^3\cdot 5^2\cdot 7^2\cdot 13\cdot 17^2$ and discriminant $2^{40}\cdot 3^{18}\cdot 5^6\cdot 7^6\cdot 13^4\cdot 17^4$. Its isogeny graph is displayed in Figure 1.

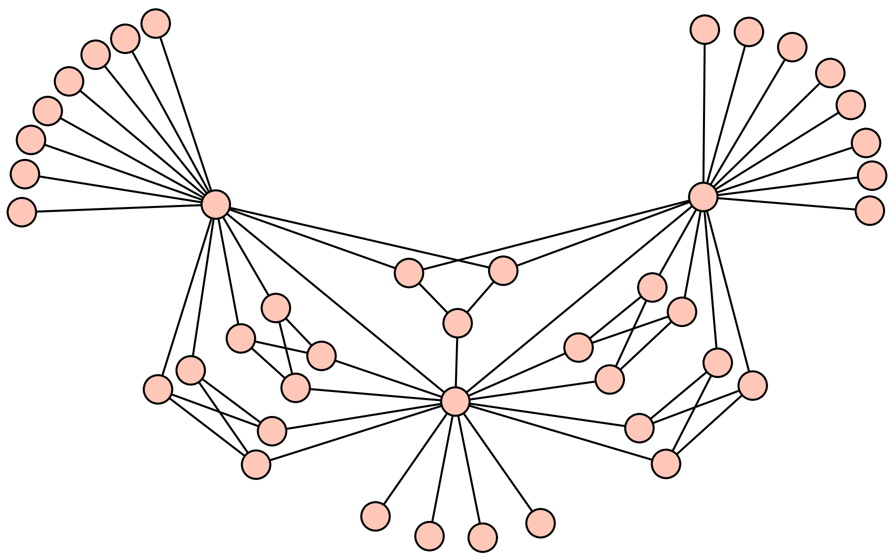


FIGURE 1. Isogeny graph with 42 vertices.

6.3. Sanity checks. Running such a large scale computation allows us to perform several sanity checks regarding the correctness of our implementation. For each isogeny found, we heuristically confirmed that the Jacobians were isogenous in two ways. First, we confirmed that all the traces of Frobenius agree for all primes up to 2^{16}, using [smalljac], that do not divide the discriminants of the curves involved. Second, independent analytic computations based on [CMSV19] have confirmed the isogeny degrees that we computed.

Regarding completeness of the isogeny classes, we ran two checks. As indicated above, we started from only one curve in each of the 1 440 894 (heuristic) isogeny classes in our dataset, and we checked that all the other curves in that class indeed appeared in our result. We also confirmed that our isogeny classes are closed under Richelot isogenies, using the function `RichelotIsogenousSurfaces` in [Magma] based on algebraic formulas specific to this case.

References

[BBKKMSV23] Barinder S. Banwait, Armand Brumer, Hyun Jong Kim, Zev Klagsbrun, Jacob Mayle, Padmavathi Srinivasan, and Isabel Vogt. "Computing non-surjective primes associated to Galois representations of genus 2 curves." 2023 (↑ 6, 7, 8, 21).

[BL04] C. Birkenhake and H. Lange. "Complex abelian varieties." Second. Springer, 2004 (↑ 14).

[BSSVY16] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki. "A database of genus-2 curves over the rational numbers." In: *LMS J. Comput. Math.* 19 (2016), pp. 235–254 (↑ 22).

[Magma] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language." In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265 (↑ 20, 21, 25).

[BL09] Reinier Bröker and Kristin Lauter. "Modular polynomials for genus 2." In: *LMS J. Comput. Math.* 12 (2009), pp. 326–339 (↑ 9, 12).

[BK94] Armand Brumer and Kenneth Kramer. "The conductor of an abelian variety." In: *Compositio Math.* 92.2 (1994), pp. 227–248 (↑ 5).

[CL21] Garen Chiloyan and Álvaro Lozano-Robledo. "A classification of isogeny-torsion graphs of $\mathbb{Q}$-isogeny classes of elliptic curves." In: *Trans. London Math. Soc.* 8.1 (2021), pp. 1–34 (↑ 1).

[CG15] Fabien Cléry and Gerard van der Geer. "Constructing vector-valued Siegel modular forms from scalar-valued Siegel modular forms." In: *Pure Appl. Math. Q.* 11.1 (2015), pp. 21–47 (↑ 11, 12, 13).

[CDSS17] Alina Carmen Cojocaru, Rachel Davis, Alice Silverberg, and Katherine E. Stange. "Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre)." In: *Int. Math. Res. Not. IMRN* 12 (2017), pp. 3557–3602 (↑ 20).

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. "Rigorous computation of the endomorphism ring of a Jacobian." In: *Math. Comp.* 88.317 (2019), pp. 1303–1339 (↑ 22, 25).

[CE15] Jean-Marc Couveignes and Tony Ezome. "Computing functions on Jacobians and their quotients." In: *LMS J. Comput. Math.* 18.1 (2015), pp. 555–577 (↑ 9).

[CW05] John E. Cremona and Mark Watkins. "Computing isogenies of elliptic curves." 2005 (↑ 1).

[Die02] Luis V. Dieulefait. "Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbf{Z}$." In: *Experimental Mathematics* 11.4 (2002), pp. 503–512 (↑ 2, 6).

[Dup06] Régis Dupont. "Moyenne arithmético-géométrique, suites de Borchardt et applications." PhD thesis. École Polytechnique. 2006 (↑ 18).

[EGM] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. "Abelian varieties." Unpublished book (↑ 3).

[Elk98] Noam D. Elkies. "Elliptic and modular curves over finite fields and related computational issues." In: *Computational perspectives* *on number theory (Chicago, IL, 1995)*. Vol. 7. AMS/IP Stud. Adv. Math. Amer. Math. Soc., Providence, RI, 1998, pp. 21–76 (↑ 1).

[Fal83] Gerd Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern." In: *Invent. Math.* 73.3 (1983), pp. 349–366 (↑ 1).

[FC90] Gerd Faltings and Ching-Li Chai. "Degeneration of abelian varieties." With an appendix by David Mumford. Springer-Verlag, Berlin, 1990 (↑ 11).

[Gee08] Gerard van der Geer. "Siegel modular forms and their applications." In: *The 1-2-3 of modular forms*. Universitext. Springer, Berlin, 2008, pp. 181–245 (↑ 10).

[GRR72] A. Grothendieck, M. Raynaud, and D. S. Rim. "Groupes de monodromie en géométrie algébrique. I." In: Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Springer-Verlag, Berlin-New York, 1972 (↑ 6, 7).

[Igu62] Jun-ichi Igusa. "On Siegel modular forms of genus two." In: *Amer. J. Math.* 84 (1962), pp. 175–200 (↑ 10, 11).

[Igu79] Jun-ichi Igusa. "On the ring of modular forms of degree two over $\mathbf{Z}$." In: *Amer. J. Math.* 101.1 (1979), pp. 149–183 (↑ 11).

[Joh17] Fredrik Johansson. "Arb: efficient arbitrary-precision midpoint-radius interval arithmetic." In: *IEEE Trans. Comput.* 66.8 (2017). `https://arblib.org/`, pp. 1281–1292 (↑ 2).

[smalljac] Kiran S. Kedlaya and Andrew V. Sutherland. "Computing L-series of hyperelliptic curves." In: *Algorithmic number theory*. Vol. 5011. Lecture Notes in Comput. Sci. Springer, Berlin, 2008, pp. 312–326 (↑ 25).

[Ken82] M. A. Kenku. "On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class." In: *J. Number Theory* 15.2 (1982), pp. 199–202 (↑ 1).

[Kie22a] J. Kieffer. "Sign choices in the AGM for genus two theta constants." In: *Pub. Math. Besançon* (2022), pp. 37–58 (↑ 18).

[Kie22b] Jean Kieffer. "Evaluating modular equations for abelian surfaces." 2022 (↑ 9, 11, 14, 15, 18, 19).

[Kie23] Jean Kieffer. "HDME: a C library for the evaluation of higher-dimensional modular equations." `https://github.com/j-kieffer/hdme`. 2023 (↑ 2, 21).

[Kli90] H Klingen. "Introductory lectures on Siegel modular forms." Cambridge University Press, 1990 (↑ 18).

[Kri90] Aloys Krieg. "Hecke algebras." In: *Mem. Amer. Math. Soc.* 87.435 (1990) (↑ 11, 13).

[LV14] Eric Larson and Dmitry Vaintrob. "Determinants of subquotients of Galois representations associated with abelian varieties." In: *J. Inst. Math. Jussieu* 13.3 (2014). With an appendix by Brian Conrad, pp. 517–559 (↑ 7).

[Lau01] Kristin Lauter. "Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields." In: *J. Algebraic Geom.* 10.1 (2001). With an appendix in French by J.-P. Serre, pp. 19–36 (↑ 5, 20).

[LMFDB] The LMFDB Collaboration. "The L-functions and modular forms database." http://www.lmfdb.org. 2022 (↑ 1, 2, 21, 22).

[LR23] David Lubicz and Damien Robert. "Fast change of level and applications to isogenies." In: *Res. Number Theory* 9.1 (2023), Paper No. 7, 28 (↑ 9).

[Maz78] B. Mazur. "Rational isogenies of prime degree (with an appendix by D. Goldfeld)." In: *Invent. Math.* 44.2 (1978), pp. 129–162 (↑ 1).

[Mes91] Jean-François Mestre. "Construction de courbes de genre 2 à partir de leurs modules." In: *Effective methods in algebraic geometry (Castiglioncello, 1990)*. Vol. 94. Progr. Math. Birkhäuser Boston, 1991, pp. 313–334 (↑ 11, 19).

[Mil15a] Enea Milio. "A quasi-linear time algorithm for computing modular polynomials in dimension 2." In: *LMS J. Comput. Math.* 18.1 (2015), pp. 603–632 (↑ 2, 9).

[Mil15b] Enea Milio. "Modular polynomials." https://members.loria.fr/EMilio/modular-polynomials/. [Online; accessed 2-May-2023]. 2015 (↑ 2).

[Mil86] J. S. Milne. "Abelian varieties." In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, New York, 1986, pp. 103–150 (↑ 4, 5).

[MN19] Pascal Molin and Christian Neurohr. "Computing period matrices and the Abel-Jacobi map of superelliptic curves." In: *Math. Comp.* 88.316 (2019), pp. 847–888 (↑ 18).

[Mum70] David Mumford. "Abelian varieties." Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, London, 1970 (↑ 3, 4).

[PARI/GP] *PARI/GP version* `2.15.0`. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2022 (↑ 20, 21).

[Ray74] Michel Raynaud. "Schémas en groupes de type $(p, \dots, p)$." In: *Bull. Soc. Math. France* 102 (1974), pp. 241–280 (↑ 7, 8).

[Sage] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.7)*. https://www.sagemath.org. 2022 (↑ 6, 21).

[Ser72] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." In: *Invent. Math.* 15.4 (1972), pp. 259–331 (↑ 7, 8).

[Ser99] Jean-Pierre Serre. "Oeuvres – Collected Papers IV: 1985–1998." Oeuvres. Springer Berlin Heidelberg, 1999, pp. 1–55 (↑ 2, 6).

[ST68] Jean-Pierre Serre and John Tate. "Good reduction of abelian varieties." In: *Ann. of Math. (2)* 88 (1968), pp. 492–517 (↑ 6, 20).

[SC03] Michael Stoll and John E. Cremona. "On the reduction theory of binary forms." In: *J. Reine Angew. Math.* 565 (2003), pp. 79–99 (↑ 20).

[Str14] Marco Streng. "Computing Igusa class polynomials." In: *Math. Comp.* 83.285 (2014), pp. 275–309 (↑ 10, 11, 18, 19).

[Sut22] Andrew V. Sutherland. "A database of genus 2 curves over $\mathbb{Q}$ with conductor less than 2^{20}." https://math.mit.edu/~drew/st2e20.txt. 2022 (↑ 22).

[Vél71] Jacques Vélu. "Isogénies entre courbes elliptiques." In: *C. R. Acad. Sci. Paris Sér. A-B* 273 (1971), A238–A241 (↑ 1).

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: bommel@mit.edu
URL: https://raymondvanbommel.nl

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: shivac@mit.edu
URL: https://math.mit.edu/~shivac

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: edgarc@mit.edu
URL: https://edgarcosta.org

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
Email address: kieffer@math.harvard.edu
URL: https://scholar.harvard.edu/kieffer