GLUING GENUS 1 AND GENUS 2 CURVES ALONG ℓ-TORSION

PITCHAYUT SAENGRUNGKONGKA AND NOAH WALSH

ABSTRACT. Let Y be a genus 2 curve over $\mathbb{Q}$. We provide a method to systematically search for possible candidates of prime $\ell \geq 3$ and a genus 1 curve X for which there exists genus 3 curve Z over $\mathbb{Q}$ whose Jacobian is up to quadratic twist (ℓ, ℓ, ℓ)-isogenous to the product of Jacobians of X and Y, building off of the work by Hanselman, Schiavone, and Sijsling for $\ell = 2$. We find several such pairs (X, Y) for prime ℓ up to 13. We also improve their numerical gluing algorithm, allowing us to successfully glue genus 1 and genus 2 curves along their 13-torsion.

1. INTRODUCTION

The study of curves is a central topic in arithmetic geometry. Exhaustive lists of curves have long been a useful tool in number theory, starting with the Antwerp tables that contains elliptic curves up to conductor 200 [BK75], continuing with Cremona's tables of elliptic curves [Cre06], and persisting today with the collections of elliptic curves and genus 2 curves in the LMFDB [LMFDB].

For higher genus curves, a large number of curves can be constructed by gluing curves of smaller genera. For any two curves X and Y of genera g_X and g_Y, the process of gluing produces a curve Z of genus $g_X + g_Y$ such that the Jacobian of Z, denoted $\mathrm{Jac}(Z)$, is isogenous to the product $\mathrm{Jac}(X) \times \mathrm{Jac}(Y)$. In other words, $\mathrm{Jac}(Z)$ is a quotient of $\mathrm{Jac}(X) \times \mathrm{Jac}(Y)$ by G, where G is a finite subgroup of the product of the n-torsion subgroups $\mathrm{Jac}(X)[n]$ and $\mathrm{Jac}(Y)[n]$ for some fixed positive integer n. When that happens, we say that this gluing is ***along n-torsion***.

Given generic curves X and Y, there are many possible choices of subgroups G that give rise to gluings over $\mathbb{C}$, and one can construct those gluings analytically by considering $\mathrm{Jac}(X)$ and $\mathrm{Jac}(Y)$ as complex tori. However, for arithmetic applications, we are interested in curves defined over non-algebraically closed fields, such as $\mathbb{Q}$. If we take curves X and Y at random, then it is very likely there will be no gluing Z that is defined over $\mathbb{Q}$. We are interested in systematically producing pairs of curves that admit a gluing over $\mathbb{Q}$. These curves often have interesting properties that deviate from generic behavior, such as torsion structure, endomorphism ring, and Sato-Tate groups.

1.1. **Previous Work.** The simpler case of gluing two curves of genus 1 (i.e., $1 + 1 = 2$) has been studied in many aspects.

(i) **Criteria for gluings to exist.** Frey and Kani [FK91] show how to derive the necessary conditions for two curves to be gluable to each other along n-torsion, namely, if E_1 and E_2 are gluable, then there exists an antisymplectic, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism $E_1[n] \to E_2[n]$.

(ii) **Find all gluable pairs.** Next, we are interested in the following problem: given a list of elliptic curves (e.g., all elliptic curves in the L-functions and modular forms database, LMFDB [LMFDB]), systematically search for all pairs that are gluable. When $n = \ell$ is prime, Cremona and Freitas [CF22] gave a complete algorithm for detecting all such antisymplectic isomorphisms and applied their methods to all pairs of elliptic curves in the LMFDB.

(iii) **Parametrize all gluable pairs.** We can go one step further from (ii) and ask if one can parameterize all pairs of elliptic curves that are gluable. For a fixed elliptic curve E_1, the space of all elliptic curves E_2 that are gluable is one-dimensional and is a twist of the modular curve $X(n)$. For $n \in \{2, 3, 4, 5\}$, the genus of $X(n)$ is 0, and so the space can be parametrized by one rational variable. The details have been worked out by Rubin and Silverberg in [RS01], [RS95], and [Sil97]. Fisher [Fis14] works out formulas for $n \in \{7, 11\}$, but in that case there are finitely many E_2's for a fixed E_1. There are also efforts to parametrize *pairs* of gluable elliptic curve along n-torsion for higher n: Fisher [Fis20, Corollary 1.3] shows that there are infinitely many pairs of gluable curves for all $n \leq 10$.

(iv) **Computing gluing.** One way to compute gluings over $\mathbb{Q}$ is to do it analytically over $\mathbb{C}$. In simpler cases, we also have explicit formulas. Howe, Leprévost, and Poonen [HLP00, Proposition 4] gave an explicit formula for gluing along 2-torsion and used it to construct genus 2 curves with large rational torsion subgroups. More recently, Bröker et. al. [BHLS15, Section A.1] also gives a formula for gluing along 3-torsion. As ℓ grows larger, the formulas quickly becomes unwieldy.

Genus 1 plus genus 2 gluing (i.e., $1 + 2 = 3$) has not been as widely studied. Ritzenthaler and Romagny [RR18] gave a formula for recovering the equation of the genus-2 factor of a genus-1 plus genus-2 gluing along 2-torsion, given that we know the genus-1 factor. Then, Hanselman, Schiavone, and Sijsling [HSS21] give a comprehensive algorithm and explicit formula for gluing along 2-torsion. They answer to some of the questions above for gluing genus 1 and 2 curves as follows.

- To answer (i), [HSS21, §1] provides a concrete criteria for a gluing along ℓ-torsion to exist, which we recall in Section 2.
- To answer (iv), [HSS21, §2.1] outlines the analytic algorithm to compute the gluing along ℓ-torsion, which was implemented in [HSS20]. In the case of $\ell = 2$, they also provide an explicit formula to glue genus 1 and 2 curves along 2-torsion.
- While they did not directly discuss (iii), for any fixed genus 2 curve Y such that there exists an elliptic curve X that admits gluing along ℓ-torsion, one can reduce the problem of finding all gluable elliptic curves X' to finding elliptic curves X' whose ℓ-torsion is isomorphic (as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module) to the ℓ-torsion of X. See Lemma 6.1 for more details.

Our work attempts to answer (ii) and gives improvement to existing methods in (iv).

1.2. **Our Results.** This paper considers the problem of gluing two curves of genus 1 and genus 2 along their ℓ-torsion to obtain a curve of genus 3 for prime ℓ. We focus on the case $\ell \geq 3$ that has not been as widely studied. There are two key results.

The first key result is that, given curve Y of genus 2, we demonstrate how to systematically and efficiently search for genus 1 curves X in the LMFDB and corresponding primes ℓ such that the curves are gluable along ℓ-torsion. More specifically, given a genus 2 curve Y, we first rule out all but finitely many of ℓ's. Then, for each such ℓ, we search for elliptic curves X such that there exists a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup $G \subset \mathrm{Jac}(X)[\ell] \times \mathrm{Jac}(Y)[\ell]$ such that the quotient

$$Q = \frac{\mathrm{Jac}(X) \times \mathrm{Jac}(Y)}{G} \tag{1.1}$$

is a principally-polarized abelian variety. The search process culminates in the workflow described in Section 6. We also provide an algorithm to rigorously verify the existence of such G in the generic case in Algorithm 4.14 and Algorithm 5.11. If Q is isomorphic to a Jacobian of some genus-3 curve Z (which happens generically, when Q is not a product of two or more Jacobians), then curves X and Y would produce a gluing Z. We use this result to glue a large number of curves in LMFDB and discover curves with interesting geometric endomorphism ring in Section 7.2.

The second key result is an improvement of the numerical gluing algorithm in [HSS21, Section 2.1] to obtain a more efficient algorithm, Algorithm 6.4. With this algorithm, we are able to reduce the time taken to the point that we are able glue along 13-torsion in 24 minutes in Example 7.4.

1.3. **Organization of the Article.** In Section 2, we describe the condition under which two curves are gluable as given in [HSS21]. Then, in Section 3, we explain how to use Frobenius elements to efficiently filter pairs of gluable curves. Section 4 explains how to utilize Serre's modularity conjecture to rigorously verify (in the generic case) part of the gluability condition. Section 5 adapts the symplectic test in [FK22] to verify the other part of gluability condition. We put all the pieces together and describe our current workflow in Section 6, which includes the speedup of the gluing algorithm. Finally, Section 7 list some examples produced from running our workflow on curves in the LMFDB.

1.4. **Notations.** For any prime p and an integer $n \neq 0$, let $\nu_p(n)$ be the p-adic valuation of n, i.e., the exponent of p in the prime factorization of n.

For any abelian variety A over a field k, $A[n]$ denotes the set of n-torsion points over its algebraic closure $\overline{k}$. For any curve X, we let N_X denote the conductor of X, and for any prime p not dividing N_X, let $a_{p,X}$ denote the trace of Frobenius at p of X. Additionally, we define $a_{p,X}$ to be equal to 1, -1, and 0 if X is an elliptic curve with split multiplicative, non-split multiplicative, and additive reduction modulo p, respectively.

Acknowledgements. This research was conducted through the MIT Department of Mathematics's Summer Program for Undergraduate Research (SPUR). The authors would like to thank our mentors Edgar Costa and Sam Schiavone for their guidance throughout the program. We also thank Eran Assaf and Shiva Chidambaram for helpful discussions. Finally, we thank Prof. David Jerison and Jonathan Bloom for organizing SPUR and for their thoughtful comments about our research.

2. Gluability Conditions

Let $n \geq 2$ be an integer. Let X and Y be smooth curves of any genus over a base field k with characteristic not dividing n. Informally, a gluing of X and Y is a curve Z with an isomorphism $\mathrm{Jac}(Z) \simeq (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$, where G is a subgroup of $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[n]$ for some n. Such an isomorphism does not exist for all subgroups G; in what follows, we consider some necessary conditions for $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ to be isomorphic to a Jacobian and consider how they translate to conditions on G.

First, the Jacobian of any curve C comes with a ***principal polarization***. This is an isomorphism $\lambda : \mathrm{Jac}(C) \to \mathrm{Jac}(C)^\vee$, satisfying technical conditions laid out in [Mil08, § 1.11]. We will consider more generally necessary conditions for $(A_1 \times A_2)/G$ to be a Jacobian, where A_1 and A_2 are arbitrary principally polarized abelian varieties. Let $\lambda_1 : A_1 \to A_1^\vee$ and $\lambda_2 : A_2 \to A_2^\vee$ be these polarizations.

For any abelian variety A, a polarization $\lambda : A \to A^\vee$ induces for each n the ***Weil Pairing***

$$e_n^\lambda \colon A[n] \times A[n] \to \mu_n, \tag{2.1}$$

an alternating bilinear form taking values in the n-th roots of unity. (See [Mil08, § 1.13] for the exact definition.)

The pairings $e_n^{\lambda_1}$ and $e_n^{\lambda_2}$ on A_1 and A_2 induce a pairing

$$\begin{aligned} e_n \colon (A_1 \times A_2)[n] \times (A_1 \times A_2)[n] &\to \mu_n \\ ((P_1, P_2), (Q_1, Q_2)) &\mapsto e_n^{\lambda_1}(P_1, Q_1)\, e_n^{\lambda_2}(P_2, Q_2) \end{aligned} \tag{2.2}$$

coming from the product polarization

$$\lambda_1 \times \lambda_2 : A_1 \times A_2 \to A_1^\vee \times A_2^\vee \simeq (A_1 \times A_2)^\vee. \tag{2.3}$$

We only consider cases in which the polarization on the quotient comes from the n-th power of this product polarization. (See [Han20, Remark 1.1.4, Theorem 1.1.10] for why generically one does not gain anything by considering polarizations other than the n-th power of the product.) In order for this to yield a polarization on the quotient, G must be ***isotropic***, i.e., the pairing must vanish on $G \times G$. Furthermore, by [BCCK24, Lemma 2.1] G must be maximal with respect to this property in order for the polarization to be principal.

The polarization of any Jacobian is indecomposable, so it is also necessary the the polarization on the quotient be indecomposable. For this reason, it is also necessary that G be ***indecomposable***, i.e., not of the form $G_1 \times G_2$ for $G_1 \subset A_1$, $G_2 \subset A_2$, as otherwise the polarization will be a product of polarizations on A_1/G_1 and A_2/G_2.

To summarize, G must be an ***indecomposable maximal isotropic subgroup***. Let us now specialize to the case where $A_1 = \mathrm{Jac}(X)$ and $A_2 = \mathrm{Jac}(Y)$ for curves X and Y of genera 1 and 2, respectively. Suppose that G is an indecomposable maximal isotropic subgroup. Then $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ is an abelian variety of dimension 3 defined over some extension k' of k. If the polarization of $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ is indecomposable, then by [OU73], $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ is isomorphic to the Jacobian of some curve Z, where Z and the isomorphism are defined over some further extension k'' of k'. Serre proved in the appendix to [Lau01] that one may in fact take k'' to be a quadratic extension of k'.

With this information, we can now formally define a gluing.

Definition 2.4. An ***(n, n)-gluing*** of the curves X and Y over k is a triple (Z, ψ, G), where Z is a smooth curve over k and a subgroup $G \subseteq \mathrm{Jac}(X)[n] \times \mathrm{Jac}(Y)[n]$ such that ψ gives an isomorphism of principally polarized abelian varieties

$$\frac{\mathrm{Jac}(X) \times \mathrm{Jac}(Y)}{G} \xrightarrow{\sim} \mathrm{Jac}(Z). \tag{2.5}$$

In the situation when $n = \ell$, a prime number, [HSS21, § 1] gives the following description of such subgroups.

Proposition 2.6. [HSS21, Proposition 1.18] *A subgroup $G \subseteq \mathrm{Jac}(X)[\ell] \times \mathrm{Jac}(Y)[\ell]$ is an indecomposable maximal isotropic subgroup if and only if*

$$G = \{(x, y) \mid \phi(x) = y + H\} \tag{2.7}$$

for some one-dimensional subgroup $H \subset G$ and some antisymplectic isomorphism $\phi : \mathrm{Jac}(X)[\ell] \to H^{\perp}/H$.

For most choices of G, the resulting abelian variety $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ will not be defined over k. In order for $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ to be defined over k, it is necessary that G must be Galois-stable. [HSS21, Proposition 1.39] worked out what this means in terms of (G, ϕ) in Proposition 2.6.

Theorem 2.8. [HSS21, Proposition 1.39] *Following the notations of Proposition 2.6, G is Galois stable if and only if both of the following holds*

(i) H is Galois-stable.
(ii) ϕ is Galois-equivariant.

Conversely, from the paragraph preceding Definition 2.4, we have the following converse.

Theorem 2.9. *Suppose that*

(i) G is Galois-stable (i.e., satisfies both conditions of Theorem 2.8); and
(ii) the quotient $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ is not a product of two or more Jacobians.

Then, there exists a curve Z such that $\mathrm{Jac}(Z) \simeq (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$, and the isomorphism is defined over a quadratic extension of k.

Condition (ii) of Theorem 2.9 can be verified numerically in terms of period matrix of $(\mathrm{Jac}(X)\times\mathrm{Jac}(Y))/G$: at most one of its even theta values can vanish. For most of the paper, we focus on searching for pairs of curves (X, Y) over $\mathbb{Q}$ for which there exists Galois-stable maximal isotropic subgroup $G \subset \mathrm{Jac}(X)[\ell] \times \mathrm{Jac}(Y)[\ell]$ (equivalently, (H, ϕ) satisfying the conditions of Theorem 2.8). For this to hold, we need both of the following to be true:

(i) there exists a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup of $\mathrm{Jac}(Y)[\ell]$.
(ii) $H^{\perp}/H$ and $\mathrm{Jac}(X)[\ell]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, and the isomorphism is antisymplectic.

Fix a genus 2 curve Y. In Section 3, we describe how to rule out elliptic curves that do not satisfy (i) or the isomorphic part of (ii). Then, in Section 5, we discuss how to test the remaining condition of (ii): that the isomorphism is antisymplectic.

Remark 2.10. Even if there exists a Galois-stable maximal isotropic subgroup of $\mathrm{Jac}(X)[\ell]\times\mathrm{Jac}(Y)[\ell]$, there might still not be a gluing. Consider the genus 2 curve Y given by `2646.b.71442.1` on the LMFDB, the elliptic curve X given by `21.a6` on the LMFDB, and $\ell = 3$. In this case, we can show that there exists such subgroup G. However, we have a strong numerical evidence that there does not exist a gluing between X and Y. More specifically, we believe that the Jacobian of the genus 2 curve is 2-isogenous to product of two elliptic curves, and quotienting out by G splits the $\mathrm{Jac}(Y)$ factor into product of two elliptic curves. We have yet to investigate a condition to tell a priori whether $(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$ will be a Jacobian or not.

3. Rational ℓ-torsion Subgroups

Throughout this section, we fix a genus 2 curve Y and study for what primes ℓ there might exist an (ℓ, ℓ)-gluing, and if so, whether there exists such a genus 1 curve X for which X and Y admit (ℓ, ℓ)-gluing.

It turns out that for a fixed Y, the condition (i) of Theorem 2.8 already rules out the possible primes ℓ to a finite set, which we detail in Section 3.1. Then, once we know ℓ, we present an algorithm that computes the trace of Frobenius element acting on $H^{\perp}/H$ in Section 3.2. We explain how this constrains X in Section 3.3.

We now introduce the concept of Frobenius polynomial. For any prime $p \neq \ell$ and elliptic curve X for which X has a good reduction modulo p, let K be a number field that contains all coordinates of all points in $\mathrm{Jac}(Y)[\ell]$. Pick any prime ideal $\mathfrak{p}$ above p, and let Frob_p be the Frobenius element corresponding to $\mathfrak{p}$. Then, $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ is a finite field, and Frob_p acts on $\mathrm{Jac}(Y)$ by

$$(x : y : z) \mapsto (x^p : y^p : z^p) \pmod{\mathfrak{p}} \tag{3.1}$$

This map induces an action of Frob_p on $\mathrm{Jac}(Y)[\ell] \simeq \mathbb{F}_\ell^4$ by a linear map in $\mathrm{GL}_4(\mathbb{F}_\ell)$ with characteristic polynomial congruent modulo ℓ to the ***Frobenius polynomial***, which is of the form

$$F_{Y,p}(T) := T^4 - a_{p,Y}T^3 + a'_{p,Y}T^2 - pa_{p,Y}T + p^2 \in \mathbb{Z}[x], \tag{3.2}$$

independent of ℓ, which can be computed by counting the number points of Y over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. See [Mil08, Chapter II] for more details.

3.1. **Finding Possible Primes.** The condition that $\mathrm{Jac}(Y)[\ell]$ must have a 1-dimensional Galois-stable subspace H already restricts the possible values of ℓ to a finite set, even without knowing the curve X. Let $\mathcal{L}$ be a set of primes for which H exists. An algorithm to determine a finite superset of $\mathcal{L}$ is studied in [BCCK24, §3.1], using Dieulefait's criterion in [Die02, §3.1]. Their algorithm only filters out ℓ not dividing the conductor N_Y and does not do anything on those ℓ's that divide N_Y. Thus, we modify their algorithm to filter out some candidate for when ℓ divides the conductor N_Y of as well.

The action of an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Jac}(Y)[\ell] \in \mathbb{F}_\ell^4$ can be expressed as a matrix in $\mathrm{GL}_4(\mathbb{F}_\ell)$. This induces a representation $\overline{\rho}_Y : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(\mathrm{Jac}(Y)[\ell])$ of dimension 4. The 1-dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subspace H induces two 1-dimensional representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times$:

- on H itself; we let this representation correspond to the character $\varepsilon_1 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(H) \simeq \mathbb{F}_\ell^\times$.
- on $\mathrm{Jac}(Y)[\ell]/H^\perp$ (by Galois-equivariance of Weil pairing); we let this representation correspond to the character $\varepsilon_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(\mathrm{Jac}(Y)[\ell]/H^\perp) \simeq \mathbb{F}_\ell^\times$.

We have that $\varepsilon_1\varepsilon_2 = \chi_\ell$, where χ_ℓ is the mod-ℓ cyclotomic character. Because $\mathbb{F}_\ell^\times$ is abelian, by the Kronecker-Weber theorem, ε_i $(i = 1, 2)$ must factor through $\mathrm{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q}) \simeq (\mathbb{Z}/e\mathbb{Z})^\times$ for some positive integer e (where ζ_e is a primitive e-th root of unity). The smallest such e is called the ***conductor*** of ε_i.

Proposition 3.3. *If N_Y is the conductor of Y and d is the largest integer such that d^2 divides $N_Y/\ell^{\nu_\ell(N_Y)}$. Define*

$$D = \begin{cases} \ell d & \ell \text{ divides } N_Y \\ d & \ell \text{ does not divide } N_Y. \end{cases}, \tag{3.4}$$

Then, the conductor of at least one of ε_1 and ε_2 divides D.

Proof. First, we show in general that the conductor of ε_1 and ε_2 both divides ℓd. Let $I_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell^{\mathrm{unr}})$ be the inertia group. Then, there exist integers α and β such that $\varepsilon_1|_{I_\ell} = \chi_\ell^\alpha$ and $\varepsilon_2|_{I_\ell} = \chi_\ell^\beta$, where $\alpha + \beta \equiv 1 \pmod{\ell - 1}$. Thus, if $\varepsilon_1' = \varepsilon_1\chi_\ell^{-\alpha}$ and $\varepsilon_2' = \varepsilon_2\chi_\ell^{-\beta}$, then both ε_1' and ε_2' are characters from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ unramified at ℓ. Moreover, they multiply to the trivial character. Thus, they have the same conductor; let it be k.

Therefore, the conductor of $\overline{\rho}_Y$ must be divisible by k^2, so k^2 divides $N_Y/\ell^{\nu_\ell(N_Y)}$, so k divides d. Thus, the conductors of ε_1' and ε_2' both divides d, which implies that the conductors of both ε_1 and ε_2 divides ℓd.

Now, assume ℓ does not divide N_Y. By a result due to Raynaud [Ray74, Corollary 3.4.4], we have that $\{\alpha, \beta\} = \{0, 1\}$. Therefore, at least one of ε_1 and ε_2 is unramified away from ℓ, implying that the conductor of ε_1 or ε_2 is the same as that of ε_1' or ε_2'. □

Proposition 3.3 shows that at least one of ε_1 and ε_2, say ε, factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q}) \simeq (\mathbb{Z}/D\mathbb{Z})^\times$, inducing a Dirichlet character $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{F}_\ell^\times$. This narrows down the possible candidates for χ to a finite set.

Furthermore, for any prime p, the image of Frob_p in $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/D\mathbb{Z})^\times$ is p. Thus, if f is the order of p in $(\mathbb{Z}/D\mathbb{Z})^\times$, then

$$\varepsilon\left(\mathrm{Frob}_p\right)^f = \varepsilon\big(\mathrm{Frob}_p^f\big) = \varepsilon\left(p^f\right) = \varepsilon(1) = 1. \tag{3.5}$$

Moreover, $\varepsilon(\mathrm{Frob}_p)$ is an eigenvalue of Frob_p (with eigenvector in H). This means that the polynomial $T - \varepsilon(\mathrm{Frob}_p)$ divides $F_{Y,p}(T)$. In other words, $F_{Y,p}(T)$ and $T^f - 1$ have a common root in $\mathbb{F}_\ell$, and so the resultant $\mathrm{Res}(F_{Y,p}(T), T^f - 1)$ is divisible by ℓ. This gives rise to the following algorithm.

Algorithm 3.6. *Input:* a curve Y of genus 2, its conductor N_Y, and a finite set of primes $\mathcal{P}$, each of which gives a good reduction of Y.

Output: a finite superset of $\mathcal{L}$, the set of primes ℓ for which there exist a one-dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup $H \subset \mathrm{Jac}(X)[\ell]$.

(1) Let d be the largest positive integer such that $d^2 \mid N_Y$.
(2) For each prime $p \in \mathcal{P}$, do the following:
   - compute the Frobenius polynomial $F_{Y,p}(T)$; and
   - compute the order f_p of p in $(\mathbb{Z}/d\mathbb{Z})^\times$.

(3) Let $\mathcal{L}_{\text{good}}$ be the set of prime dividing $\gcd_{p\in\mathcal{P}} \operatorname{Res}(F_{Y,p}(T), T^{f_p} - 1)$.
(4) For each prime ℓ dividing N_Y, we run the following test for each prime $p \in \mathcal{P}$.
  - Compute D as in (3.4).
  - Compute the Frobenius polynomial $F_{Y,p}(T)$ and the order g_p of p in $(\mathbb{Z}/D\mathbb{Z})^\times$; and
  - Check whether $F_{Y,p}(T)$ and $T^{g_p} - 1$ have a common root in $\mathbb{F}_\ell$.

  Let $\mathcal{L}_{\text{bad}}$ be the set of primes ℓ dividing N_Y that pass through the above test for all primes p.
(5) Return $\mathcal{L} = \mathcal{L}_{\text{good}} \cup \mathcal{L}_{\text{bad}}$.

The discussion preceding this algorithm shows that Algorithm 3.6 indeed returns a valid superset of $\mathcal{L}$. Such a superset is always finite: by the Riemann hypothesis for curves, all roots of $F_{Y,p}$ have absolute value $\sqrt{p}$, so $\operatorname{Res}(F_{Y,p}(T), T^{f_p} - 1) \neq 0$ for all primes p, and hence $\mathcal{L}_{\text{good}}$ is always finite.

3.2. **The Frobenius Action on $H^\perp/H$.** Assuming that H exists, we now proceed to study the condition (ii) of Theorem 2.8. We defer the study of the symplectic condition to Section 5 and focus on the condition that $H^\perp/H$ and $\operatorname{Jac}(X)[\ell]$ are isomorphic as $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

For any prime p at which Y has a good reduction, the Frobenius element Frob_p acts on $H^\perp/H$ by a matrix in $\operatorname{GL}_2(\mathbb{F}_\ell)$. We define

$$b_p = \text{trace of } \operatorname{Frob}_p \text{ on } H^\perp/H. \tag{3.7}$$

The traces b_p are important data describing the Galois action on $H^\perp/H$, which will allow us to search for a suitable elliptic curve X. See Proposition 3.10 for more details. In this subsection, we will explain how to compute b_p.

Recall from Section 3.1 that the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on H is determined by a character $\varepsilon : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times$, and ε factors through $\operatorname{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q}) \simeq (\mathbb{Z}/D\mathbb{Z})^\times$, where D is defined in (3.4). Thus, ε corresponds to a Dirichlet character $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{F}_\ell^\times$, and we have $\varepsilon(\operatorname{Frob}_p) = \chi(p)$.

For any prime p, the action of Frob_p onto one-dimensional subspaces H and $\operatorname{Jac}(Y)[\ell]/H^\perp$ must be multiplication by $\chi(p)$ and $p/\chi(p)$ in some order, which are two eigenvalues of Frob_p acting on $\operatorname{Jac}(Y)$. The trace on $H^\perp/H$ must be the sum of the remaining two eigenvalues. Thus,

$$b_p = a_{p,Y} - \chi(p) - \frac{p}{\chi(p)} \pmod{\ell}. \tag{3.8}$$

Hence, if one knows χ, one can determine b_p for all p. For a fixed Y, there are finitely many possibilities for $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{F}_\ell^\times$. We rule out χ by checking that, for any prime q not dividing N_Y, the number $\chi(q)$ must be a root of $F_{Y,q}(T)$. This leads to the following algorithm.

Algorithm 3.9. *Input.* A genus 2 curve Y, its conductor N_Y, a prime ℓ, and a finite set of primes $\mathcal{Q}$.

Output. A finite list of candidate functions that take a prime number $p \neq \ell$ and output b_p (defined in (3.7)) modulo ℓ.

(1) Compute D as defined in (3.4).
(2) Enumerate the set $\mathcal{X}$ of all Dirichlet characters $(\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{F}_\ell^\times$.
(3) For each prime $q \in \mathcal{Q}$, compute $F_{Y,q}(T)$. Remove from $\mathcal{X}$ any character χ such that $\chi(q)$ is not a root of $F_{Y,q}(T)$.
(4) For each function $\chi \in \mathcal{X}$, we return the function

$$p \;\mapsto\; a_{p,Y} - \chi(p) - \frac{p}{\chi(p)} \pmod{\ell}.$$

From (3.8), we can see that the output of this algorithm includes at least one function for each possible H. If there are multiple possible H's, the algorithm returns multiple functions, each corresponding to a candidate H.

3.3. **Frobenius Traces of Gluable Elliptic Curve.** For this entire section, fix a genus 2 curve Y and a prime $\ell \geq 3$ such that there exists a one-dimensional $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup $H \subset \operatorname{Jac}(Y)[\ell]$. For any prime p at which Y has a good reduction, let b_p denote the trace of Frob_p in $H^\perp/H$ (as computed in Algorithm 3.9).

Suppose that X is an elliptic curve such that $X[\ell]$ and $H^\perp/H$ are isomorphic as $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. By comparing b_p with the trace of Frobenius at p of X (which we denoted $a_{p,X}$), we can rule out some of such X, as detailed in the following proposition.

Proposition 3.10. *Let X be an elliptic curve such that $\mathrm{Jac}(X)[\ell]$ and $H^\perp/H$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Let $p \neq \ell$ be a prime such that Y has a good reduction modulo p.*

(i) *If X has a good reduction modulo p, then $b_p \equiv a_{p,X} \pmod{\ell}$.*
(ii) *If X has a split multiplicative reduction modulo p, then $b_p \equiv 1+p \pmod{\ell}$.*
(iii) *If X has a non-split multiplicative reduction modulo p, then $b_p \equiv -(1+p) \pmod{\ell}$.*
(iv) *If $\ell \geq 5$, then X cannot have additive reduction modulo p.*

Proof.

(i) The Frobenius element Frob_p acts on $H^\perp/H$ and on $\mathrm{Jac}(X)[\ell]$ by the same matrix in $\mathrm{GL}_2(\mathbb{F}_\ell)$ up to a change of basis. Thus, they have the same trace modulo ℓ.
(ii) By the theory on Tate's curve [Sil94, Theorem V.5.3.], there exists $q \in \mathbb{Q}_p$ such that $X/\overline{\mathbb{Q}}_p \simeq \overline{\mathbb{Q}_p}^\times/q^{\mathbb{Z}}$ as groups. This isomorphism is Galois equivariant. By considering the ℓ-torsion of both sides, we find that $\mathrm{Jac}(X)[\ell] \simeq \langle q^{1/\ell}, \zeta_\ell\rangle$ (where ζ_ℓ is the ℓ-root of unity). Therefore, the Frobenius element Frob_p acts on $\mathrm{Jac}(X)[\ell]$ by matrix $\left(\begin{smallmatrix}1 & * \\ 0 & p\end{smallmatrix}\right)$, so it must act on $H^\perp/H$ by the same matrix in modulo ℓ. Hence, we conclude that $b_p \equiv 1+p \pmod{\ell}$.
(iii) There exists a quadratic twist X' of X such that X' has a split multiplicative reduction modulo ℓ. By (ii), the trace of Frob_p acting on $X'[\ell]$ is $1+p$. Thus, the trace of Frob_p acting on $X[\ell]$ is $-(1+p)$, which must be equal to b_p in modulo ℓ.
(iv) If $p \neq \ell \geq 5$ and X has additive reduction modulo p, then we claim that the torsion field $\mathbb{Q}(\mathrm{Jac}(X)[\ell])$ is ramified at p. To see this, following the notations of [Sil09, Chapter VII], let X_0 and X_1 denote the points in $X(\mathbb{Q}_p)$ that reduce to nonsingular point and the additive identity $\widetilde{O}$ in $X(\mathbb{F}_p)$, respectively. By [Sil09, Theorem VII.6.1], the size of the group $X(\mathbb{Q}_p)/X_0$ is at most 4. Thus, for $\ell \geq 5$, we have $X(\mathbb{Q}_p)[\ell] \subseteq X_0$. However, if $\mathbb{Q}(X[\ell])$ were unramified at p, X_1 would not have any ℓ-torsion, so by [Sil09, Proposition 2.1], one would have $(\mathbb{Z}/\ell\mathbb{Z})^2$ as a subgroup of $X(\overline{\mathbb{F}}_p)_{\mathrm{ns}} \simeq (\overline{\mathbb{F}}_p, +)$, a contradiction.
Thus, the Galois representation $\overline{\rho}_X : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is ramified at p. However, the Galois representation $\overline{\rho}_{H^\perp/H} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is isomorphic to $\overline{\rho}_X$ but is unramified at p, a contradiction. □

Corollary 3.11. *Suppose $p \neq \ell$ and $\ell \geq 5$. If*

$$b_p \notin \{-(p+1), p+1\} \cup [-2\sqrt{p}, 2\sqrt{p}], \tag{3.12}$$

then there is no elliptic curve X such that $H^\perp/H$ and $\mathrm{Jac}(X)[\ell]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

Proof. Follows from Proposition 3.10 and Hasse-Weil bound. □

Corollary 3.11 can be used to prove that some genus 2 curves have no gluable elliptic curves. We provide an example for $\ell \in \{11, 13, 19\}$.

Example 3.13. The following are genus 2 curves for which there exists H, but does not have any elliptic curve that admits a gluing over $\mathbb{Q}$.

- **$\boldsymbol{\ell = 11}$.** The curve Y with LMFDB label `353.a.353.1` and equation $y^2 + (x^3+x+1)y = x^2$ has rational 11-torsion point (so H exists), and its Frobenius polynomial at 2 is
$$F_{Y,2}(T) = T^4 + T^3 + 3T^2 + 2T^3 + 4 = (T-1)(T-2)(T^2+4T+2).$$
Following Algorithm 3.9, we have $\chi \equiv 1$, so we can compute $b_2 = -4 \pmod{11}$.
- **$\boldsymbol{\ell = 13}$.** The curve with LMFDB label `349.a.349.1` and equation $y^2+(x^3+x^2+x+1)y = -x^3-x^2$ has a rational 13-torsion point and $b_2 \equiv 8 \pmod{13}$.
- **$\boldsymbol{\ell = 19}$.** The curve with LMFDB label `169.a.169.1` and equation $y^2 + (x^3+x+1)y = x^5+x^4$ has a rational 19-torsion point and $b_2 \equiv -6 \pmod{19}$.

By Corollary 3.11, there is no elliptic curve gluable to any of the three examples above.

Remark 3.14. When $\ell \in \{3, 5\}$, by [Rub97, Theorem 3], there always exists an elliptic curve X such that $H^\perp/H$ and $\mathrm{Jac}(X)[\ell]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Furthermore, one can make it isomorphic with a correct symplectic type [Fis06, Section 13]. Thus, there always exists a gluable elliptic curve provided that $\ell \in \{3, 5\}$ and H exists.

We do not yet know whether there is an example of a genus 2 curve for which H exists when $\ell = 7$, but there is no gluable elliptic curve.

4. Proving Isomorphism of Galois Representations

In this section, we utilize Serre's modularity conjecture to study the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $H^\perp/H$ more closely. The result of this is that, if the Galois representation associated to $H^\perp/H$ is irreducible, then there is an algorithm to rigorously prove that $H^\perp/H$ and $\mathrm{Jac}(X)[\ell]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

We begin by reviewing the statement of Serre's modularity conjecture in Section 4.1 and use it to show that the representation corresponding to $H^\perp/H$ is modular in Section 4.2. After this, the algorithm is divided into two steps.

(1) Proving that there indeed exists a one-dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup $H \subset \mathrm{Jac}(Y)[\ell]$. We do this by utilizing a numerical algorithm with analytic description of Y. This is detailed in Section 4.3.
(2) Proving the isomorphism between $H^\perp/H$ and $\mathrm{Jac}(X)[\ell]$. We do this by combining modularity of the representation corresponding to $H^\perp/H$ and Sturm's bound. This gives an explicit bound on how many Frobenius traces to check, which is explained in Section 4.4.

Finally, in Section 4.5, we provide some comments about when the reducible case.

4.1. **Serre's Modularity Conjecture.** In this section, we briefly review the statement of Serre's modularity conjecture, which was proven by Khare and Wintenberger in [KW09].

Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) \geq 0\}$ denote the complex upper half plane. For any positive integer N, we have a congruence subgroup

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod N \right\} \subset \mathrm{SL}_2(\mathbb{Z}). \tag{4.1}$$

For any Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ and any positive integer k, we have the (finite-dimensional) $\mathbb{C}$-vector space $S_k(N, \varepsilon)$ of cusp forms in $\Gamma_0(N)$ with weight k and nebentypus ε, i.e., the space of functions $f : \mathbb{H} \to \mathbb{C}$ vanishing at all cusps of $\Gamma_0(N)\backslash\mathbb{H}$ such that

$$f\left(\tfrac{az+b}{cz+d}\right) = f(z)(cz+d)^k \varepsilon(d) \quad \text{for all} \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N). \tag{4.2}$$

We also denote $S_2(N) := S_2(N, \chi_{\mathrm{triv}})$, where $\chi_{\mathrm{triv}}(a) = 1$ for all a.

Each function $f \in S_2(N, \chi)$ has a ***q*-expansion** $f(z) = \sum_{n\geq 1} a_n q^n$, where $q = e^{2\pi i z}$. For any prime ℓ, one can reduce modular forms modulo ℓ by taking any mapping from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{F}}_\ell$ and reducing the q-expansion coefficients along the mapping. This gives an ***modulo ℓ-modular form*** $\overline{f} = \sum_{n\geq 1} \overline{a}_n q^n$ where $\overline{a}_n \in \overline{\mathbb{F}}_\ell$.

We now state Serre's modularity conjecture.

Theorem 4.3 (Serre's modularity conjecture, [KW09])**.** *Suppose* $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ *satisfies*

- $\overline{\rho}$ *is irreducible.*
- $\overline{\rho}$ *is odd, i.e.,* $\det \overline{\rho}(c) = -1$*, where* c *is the complex conjugation map.*

Then there exist positive integers $N = N(\overline{\rho})$*,* $k = k(\overline{\rho})$*, a character* $\varepsilon = \varepsilon(\overline{\rho}) : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$*, and a modulo* ℓ *modular form* $f \in \mathbb{F}_\ell[[q]]$ *arising from* $S_k(N, \varepsilon)$ *with coefficients in* $\mathbb{F}_\ell$ *such that* $a_p \equiv \mathrm{tr}\,\rho(\mathrm{Frob}_p) \pmod p$ *for all* p *not dividing* N*.*

[Ser87] gives an explicit recipe for determining $N(\overline{\rho})$, $\varepsilon(\overline{\rho})$, and $k(\overline{\rho})$. We will not reproduce the full definitions here, but it is important to note that they satisfy $\det \overline{\rho} = \varepsilon(\chi_\ell)^{k-1}$ and $k \in [2, \ell^2 - 1]$.

4.2. **Modularity of the Representation.** Let Y be a genus 2 curve and ℓ be a prime such that there exists a Galois-stable subgroup $H \subsetneq \mathrm{Jac}(Y)[\ell]$. Let $V_Y = \mathrm{Jac}(Y)[\ell]$. We now use Serre's modularity conjecture to study the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module structure of $H^\perp/H$.

Since H is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable, by Galois-equivariance of Weil pairing, we deduce that $H^\perp$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable. Thus, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ onto $H^\perp/H$ is well-defined and thus induces 2-dimensional mod ℓ-representations $\overline{\rho}_{H^\perp/H} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(H^\perp/H)$. First, we have the following determinant result.

Proposition 4.4. *For any* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, we have*

$$\det(\overline{\rho}_{H^\perp/H}(\sigma)) = \chi_\ell(\sigma), \tag{4.5}$$

where $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell$ *is the cyclotomic character, determined by the action of* ℓ*-th root of unity.*

Proof. Consider the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant filtration $0 \subset H \subset H^\perp \subset V_Y$, which has successive quotients are H, $H^\perp/H$, and $V_Y/H^\perp$. Therefore, we deduce that

$$\det(\sigma|_H)\det(\sigma|_{H^\perp/H})\det(\sigma|V_Y/H^\perp) = \det(\sigma|_{V_Y}) = \chi_\ell(\sigma)^2. \tag{4.6}$$

However, by Galois equivariance of Weil pairing, $\det(\sigma|_H)\det(\sigma|_{V_Y/H^\perp}) = \chi_\ell(\sigma)$, so it follows that $\det(\overline{\rho}_{H^\perp/H}(\sigma)) = \det(\sigma|_{H^\perp/H}) = \chi_\ell(\sigma)$. ☐

Plugging the complex conjugation map c into Proposition 4.4, we see that $\det\overline{\rho}_{H^\perp/H}(c) = \chi_\ell(c) = -1$, so $\overline{\rho}_{H^\perp/H}$ is odd. Thus, if we assume that $\overline{\rho}_{H^\perp/H}$ is irreducible, then the representation is modular with trivial nebentypus. The next proposition then restricts the level.

Proposition 4.7. *Assume that $\overline{\rho}_{H^\perp/H}$ is irreducible. Then, the level $N(\overline{\rho}_{H^\perp/H})$ divides N_Y.*

Proof. We claim that the conductor divides the conductor of the representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_Y)$, which in turn divides the conductor of Y.

To prove this, we consider the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant filtration $0 \subset H \subset H^\perp \subset V_Y$, which has The successive quotients are H, $H^\perp/H$, and $V_Y/H^\perp$, respectively. For any subgroup $G \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$\dim H^G + \dim(H^\perp/H)^G + \dim(V_Y/H^\perp)^G = \dim(V_Y)^G, \tag{4.8}$$

so $\dim(H^\perp/H)^G \le \dim(V_Y)^G$ (here, W^G denote the subspace of W fixed by G). Using this when G is a ramification group and summing, we deduce that for any prime $p \neq \ell$, we have $\nu_p(N(\overline{\rho}_{H^\perp/H})) \le \nu_p(N(\overline{\rho}_Y))$. Hence, we deduce that $N(\overline{\rho}_{H^\perp/H})$ divides $N(\overline{\rho}_Y)$. ☐

We now determine the weight of the representation.

Theorem 4.9. *Assume that $\overline{\rho}_{H^\perp/H}$ is irreducible (hence modular) and ℓ does not divide N_Y. Then, $\overline{\rho}_{H^\perp/H}$ is modular with weight 2.*

Proof. By [Ser87, Proposition 4], it suffices to show that $H^\perp/H$ is a finite $\mathbb{Z}_\ell$-group scheme. Since $\mathrm{Jac}(Y)$ has a good reduction modulo ℓ, it follows that $\mathrm{Jac}(Y)[\ell]$ (and hence both H and $H^\perp$) are finite $\mathbb{Z}_\ell$-group scheme. Finally, by [Ray74, Corollary 3.3.6 (1)] (with $e = 1$), it follows that $H^\perp/H$ is a finite $\mathbb{Z}_\ell$-group scheme. ☐

Corollary 4.10. *Assume $\overline{\rho}_{H^\perp/H}$ is irreducible. Let*

$$k = \begin{cases} 2 & \ell \text{ does not divide } N_Y \\ \ell^2 - 1 & \ell \text{ divides } N_Y. \end{cases} \tag{4.11}$$

Then, there exists a modular form $f \in S_k(N_Y)$ modulo ℓ such that $\overline{\rho}_{f,\ell} \simeq \overline{\rho}_{H^\perp/H}$.

In particular, if $f = \sum_{n=1}^\infty c_n q^n$ is the q-expansion of f, then $c_p \equiv b_p \pmod{\ell}$ for all primes p not dividing N_Y.

Proof. In the case that ℓ does not divide N_Y, this is immediate by Theorem 4.9.

If ℓ divides N_Y, then the (untwisted) weight of $\overline{\rho}_{H^\perp/H}$ is in the interval $[2, \ell^2 - 1]$ and is $\equiv 2 \pmod{\ell - 1}$. We note that given any modular form $f \in S_k(N_Y)$ modulo ℓ, there is an modulo ℓ modular form $E_{\ell-1}f \in S_{k+\ell-1}(N_Y)$, whose q-expansion in modulo ℓ is the exactly the same as f. (Here, $E_{\ell-1}$ denote the Eisenstein series.) Thus, regardless of what the weight of $\overline{\rho}_{H^\perp/H}$ is, one can increment the weight by $\ell - 1$ at a time without changing the coefficients modulo ℓ. Hence, there is a corresponding modular form of weight $\ell^2 - 1$. This concludes the proof. ☐

4.3. **Proving Existence of H.** In this subsection, we describe a numerical algorithm that can prove the existence of H.

Recall that the Jacobian of a curve of genus 2 over $\mathbb{C}$ is isomorphic to a complex torus $\mathbb{C}^2/\Lambda$ for some four-dimensional lattice Λ. This isomorphism can be constructed explicitly. To do so, recall that points on the $\mathrm{Jac}(Y)$ can be parametrized by $\{P_1, P_2\} \in \mathrm{Sym}^2 Y$. For two chosen base points $Q_1, Q_2 \in \mathrm{Jac}(Y)$, we define the ***Abel-Jacobi map***

$$\begin{aligned} \mathrm{AJ}_{Q_1,Q_2} : \mathrm{Sym}^2 Y &\to H^0(Y,\Omega)/H_1(Y,\mathbb{Z}) = \mathbb{C}^2/\Lambda \\ \{P_1, P_2\} &\mapsto \left(\int_{Q_1}^{P_1}\omega_1 + \int_{Q_2}^{P_2}\omega_1, \quad \int_{Q_1}^{P_1}\omega_2 + \int_{Q_2}^{P_2}\omega_2\right), \end{aligned} \tag{4.12}$$

where one picks a basis for ω_1, ω_2 for differentials $H^0(Y, \Omega)$; one working basis is $\omega_1 = dx/y$ and $\omega_2 = x\,dx/y$ if $y^2 = f(x)$ is a hyperelliptic model of Y. This map does not depend on the choice of path, as we are considering their values modulo $\Lambda = H_1(Y, \mathbb{Z})$. For more details about this map, we refer the reader to [Mil08, §1.18].

On this torus, the ℓ-torsion is simply the ℓ^4 points in $\frac{1}{\ell}\Lambda$. Fix some subgroup $H \subset \frac{1}{\ell}\Lambda$ of dimension one and let the nonzero points in H be $P_1, P_2, \ldots, P_{\ell-1}$. For each $1 \le i \le \ell - 1$, pulling back P_i gives a point on the Jacobian. Based on the representation of P_i in $\mathrm{Sym}^2 Y$, we define a polynomial

$$Q_i(T) := \begin{cases} (T - x_{i,1})(T - x_{i,2}) & \text{if } P_i \mapsto \{(x_{i,1}, y_{i,1}), (x_{i,2}, y_{i,2})\} \in \mathrm{Sym}^2 Y \\ T - x_i & \text{if } P_i \mapsto \{(x_i, y_i)\} \in \mathrm{Sym}^2 Y. \end{cases} \tag{4.13}$$

If H is Galois stable, then the coefficients of the polynomial $Q(T) = \prod_{i=1}^{\ell-1} Q_i(T)$ are rational. Therefore, if one computes everything over $\mathbb{C}$ with sufficient precision, one can run a rational recognition algorithm on the coefficients to determine whether or not this H is Galois-stable.

Finally, to eliminate the possibility for floating point error, we verify that the recognized polynomial $Q(T)$ is valid by computing the coordinate of points in H, which will be in a degree 2-extension of $\mathbb{Q}(x)/(Q(x))$, hence an extension of degree $4(\ell - 1)$ of $\mathbb{Q}$. One can verify that this point is indeed an ℓ-torsion. If this is the case, then we have proven an existence of H, with polynomial Q that can be used as a certificate.

4.4. **Proving Isomorphism.** One notable property of modular forms is that if the first few coefficients (up to the Sturm bound [Stu87]) of two modular forms are congruent modulo ℓ, then the entire modular forms are congruent. Combining this fact with modularity of $\overline{\rho}_{H^\perp/H}$ gives an algorithm to deterministically prove the isomorphism between two mod-ℓ Galois representations $\overline{\rho}_{H^\perp/H}$ and $\overline{\rho}_X$. The algorithm mirrors [KO92, Proposition 4], which is used to prove mod-ℓ congruences between elliptic curves. We now describe a version of this algorithm in our setting of genus 2 curves.

Algorithm 4.14. *Input.* An elliptic curve X (with conductor N_X), a prime $\ell \ge 3$, and a genus 2 curve Y (with conductor N_Y) such that

- there exists a one-dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup $H \subset \mathrm{Jac}(Y)[\ell]$; and
- the representation $\overline{\rho}_{H^\perp/H}$ is irreducible.

Output. `true` if $\overline{\rho}_{H^\perp/H} \simeq \overline{\rho}_X$ and `false` otherwise.

(1) Compute M and the Sturm's bound by

$$M = \mathrm{lcm}\left(N_X,\ N_Y \prod_{\substack{\text{prime } p \\ p \mid N_Y}} p\right), \qquad B = \tfrac{k}{12}\mu(M) = \tfrac{k}{12} M \prod_{\substack{\text{prime } p \\ p \mid M}} \left(1 - \tfrac{1}{p}\right), \tag{4.15}$$

where k is defined in (4.11).

(2) For each prime $p \le B$ not dividing N_Y,
  - if p does not divide N_X, check whether $b_p \equiv a_{p,X} \pmod{\ell}$.
  - if X has a multiplicative reduction modulo p, check whether $b_p a_{p,X} \equiv p + 1 \pmod{\ell}$.

  Return `true` if and only if the condition above is satisfied for all $p \le B$.

It is worth noting that this algorithm is only feasible when the conductor of Y is very small: if the conductor N_Y is squarefree, then the algorithm requires checking $\Theta(N_Y^2)$ traces.

Remark 4.16. To certify irreducibility of $\overline{\rho}_{H^\perp/H}$, we do the following: first enumerate the set $\mathcal{X}$ of characters $\varepsilon : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ that has conductor dividing D (where D is in Proposition 3.3). Then, for each prime $p \le B$ for which Y has a good reduction, eliminate any character $\chi \in \mathcal{X}$ such that $b_p \not\equiv \varepsilon(p) + \frac{p}{\varepsilon(p)} \pmod{\ell}$. If it happens that $\mathcal{X} = \emptyset$, we can conclude that H is irreducible.

Proof of Correctness of Algorithm 4.14. By Proposition 3.10, if $\overline{\rho}_{H^\perp/H} \simeq \overline{\rho}_X$, then the conditions in (4) are all satisfied, so the algorithm returns `true`. Thus, it suffices to show that if the conditions in (4) are all satisfied, theen $\overline{\rho}_{H^\perp/H} \simeq \overline{\rho}_X$.

By Modularity Theorem [BCDT01, Theorem A], let $\overline{f} \in S_2(\Gamma_0(N_X))$ be the modular form corresponding to ρ_X. By the weight-incrementing argument in the proof of Corollary 4.10, there is a modular form $f \in$

$S_k(\Gamma_0(N_X))$ that has the same reduction modulo ℓ as $\overline{f}$. By Corollary 4.10, let $g \in S_k(\Gamma_0(N_Y))$ be the modular form corresponding to $\rho_{H^\perp/H}$.

For any modular form $h \in S_k(\Gamma_0(N))$ with q-expansion $h = \sum_{n\geq 1} c_n q^n$, define

$$F_{p,h}(T) = \begin{cases} 1 - c_pT & p \mid N \\ 1 - c_pT + pT^2 & p \nmid N. \end{cases} \tag{4.17}$$

In particular, the L-function corresponding to h is

$$L_h(s) = \sum_{n\geq 1} c_n n^{-s} = \prod_{p \text{ prime}} F_{p,h}(p^{-s})^{-1}. \tag{4.18}$$

Let $R_d : S_k(\Gamma_0(N)) \to S_k(\gamma_0(Nd))$ denote the operator that takes a function h to another function $\tau \mapsto h(d\tau)$. Note that the L-function corresponding to R_dh is $d^{-s}L_h(s)$. By comparing individual L-factor, we have

$$F_{p,R_ph}(T) = T \cdot F_{p,h}(T). \tag{4.19}$$

For each prime $p < B$, we define operators V_p that will be acted on f and V'_p that will be acted on g so that the L-factors at primes dividing N_XN_Y are equal, and V_pf and V'_pg are both in $S_2(\Gamma_0(M))$. We have a couple cases.

(1) **If p divides N_Y.** Then, we define
$$V_p = F_{p,f}(R_p) \quad \text{and} \quad V'_p = F_{p,g}(R_p),$$
so we have $F_{p,V_pf}(T) = F_{p,V'_pg}(T) = 1$. Moreover, $\deg F_{p,f} = \max(2 - \nu_p(N_X), 0)$ by considering reduction types of X, so the power of p in the level of V_pf is $\max(2, \nu_p(N_X))$. Similarly, $\deg F_{p,g} = 1$, so the power of p in the level of V'_pg is $\nu_p(N_Y) + 1$. Both numbers are at most $\nu_p(M)$.

(2) **If p does not divide either N_X or N_Y.** Then, we have $F_{p,f}(T) = 1 - a_{p,X}T + pT^2$ and $F_{p,g}(T) = 1 - b_pT + pT^2$, which are automatically congruent modulo ℓ. Thus, we can define $V_p = V'_p = 1$, so the levels of V_pf and V'_pg are not divisible by p.

(3) **If p does not divide N_Y and $\nu_p(N_X) = 1$.** Then, we have $F_{p,f}(T) = 1 - a_{p,X}T$ and $F_{p,g}(T) = 1 - b_pT + T^2$. The fact that $a_{p,X} = \pm 1$, and the $a_{p,X}b_p \equiv p + 1 \pmod{\ell}$ implies that $1 - a_{p,X}T$ divides $1 - b_pT + pT^2$ in $\mathbb{F}_\ell[T]$. Let the quotient be $1 - cT$ for $c \in \mathbb{F}_\ell$. Then, we define
$$V_p = 1 \quad \text{and} \quad V'_p = 1 - cR_p,$$
and so the power of p in the levels of V_pf and V'_pg are both 1.

(4) **If p does not divide N_Y and $\nu_p(N_X) \geq 2$.** Then, the L-factors at p of f and g are 1 and $(1 - b_pT + T^2)^{-1}$. Thus, we define
$$V_p = 1 \quad \text{and} \quad V'_p = 1 - b_pR_p + R_p^2,$$
and so the power of p in the levels of V_pf and V'_pg are $\nu_p(N_X)$ and 2, respectively.

Now, let $V = \prod_{p\leq B} V_p$ and $V' = \prod_{p\leq B} V'_p$. Hence, we have that

- For all prime $p \leq B$, the L-factor at p of Vf and $V'g$ are equal.
- Both Vf and $V'g$ are in $S_k(\Gamma_0(M))$ for M defined in (4.15)

Thus, the q-expansion of modular forms Vf and $V'g$ are congruent modulo ℓ up to the coefficient q^B. Hence, by Sturm's theorem [Stu87, Theorem 1], we get that Vf and $V'g$ are congruent modulo ℓ. This means that $a_p \equiv b_p \pmod{\ell}$ for *every* prime $p \nmid M$.

Thus, for any prime p, the matrices $\overline{\rho}_{H^\perp/H}(\mathrm{Frob}_p)$ and $\overline{\rho}_X(\mathrm{Frob}_p)$ are conjugates. By Chebotareav density theorem, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, one can select p such that σ and Frob_p are conjugates, and so $\overline{\rho}_{H^\perp/H}(\sigma)$ and $\overline{\rho}_X(\sigma)$ are conjugates for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus, by Brauer–Nesbitt theorem, $\overline{\rho}_{H^\perp/H}$ and $\overline{\rho}_X$ are isomorphic up to semisimplification. However, since we assumed $\overline{\rho}_{H^\perp/H}$ is irreducible, it follows that $\overline{\rho}_{H^\perp/H} \simeq \rho_X$. ☐

4.5. **The Reducible Case.** In the case that $\overline{\rho}_{H^\perp/H}$ is reducible, we cannot use the algorithm above because $\overline{\rho}_{H^\perp/H}$ is not necessarily modular. Even if $\overline{\rho}_{H^\perp/H}$ were modular, we can only use Algorithm 4.14 to show that $\overline{\rho}_{H^\perp/H}$ and ρ_X are isomorphic up to semisimplification. An algorithm using modular polynomial similar to [CF22, §3.6.] does not extend well to genus 2 curves due to the unwieldy nature of modular polynomials in genus 2. One might need to resort to explicitly computing $\overline{\rho}_{H^\perp/H}$.

5. Checking antisymplectic Condition

Throughout this section, let X and Y be curves of genus 1 and genus 2 and ℓ be a prime such that

- there is a Galois-stable 1-dimensional subspace $H \subseteq \mathrm{Jac}(Y)[\ell]$; and
- there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism $\phi : H^\perp/H \to \mathrm{Jac}(X)[\ell]$.

Then, the only condition left to verify before we can glue X and Y is that ϕ is antisymplectic, i.e., for any $P, Q \in H^\perp/H$, we have $e_\ell(\phi(P), \phi(Q)) = e_\ell(P, Q)^{-1}$. If $\ell = 2$, then this condition is tautological. Hence, we assume ℓ is odd for the remainder of this section.

If the image of the representation $\overline{\rho}_{H^\perp/H} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(H^\perp/H)$ is sufficiently nice, we may still be able to determine whether this condition holds even before trying to glue those curves. We will adapt the method in [FK22] to do so.

5.1. **Symplectic Type.** If $\phi : H^\perp/H \to \mathrm{Jac}(X)[\ell]$ is a Galois module isomorphism, then there exists a constant $\alpha \in \mathbb{F}_\ell^\times$ such that for any $P, Q \in H^\perp/H$, we have

$$e_\ell(\phi(P), \phi(Q)) = e_\ell(P, Q)^\alpha. \tag{5.1}$$

Note that if we replace ϕ by $[t] \circ \phi$ where $t \in \mathbb{Z}$ (which is still a Galois module isomorphism), then α becomes αt^2. We thus define the ***symplectic type*** of ϕ to be the image of α in $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2 \simeq \{\pm 1\}$. If the image is $+1$, then ϕ has ***positive symplectic type***, and if the image is -1, then ϕ has ***negative symplectic type***.[1] This terminology is not to be confused with symplectic and antisymplectic.

Proposition 5.2. *Suppose $\ell \equiv 1 \pmod 4$ (resp. $\ell \equiv 3 \pmod 4$). Then, there exists an antisymplectic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism $\phi : H^\perp/H \to \mathrm{Jac}(X)[\ell]$ if and only if there exists a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism $\psi : H^\perp/H \to \mathrm{Jac}(X)[\ell]$ of positive (resp. negative) symplectic type.*

Proof. Both statements follow from the fact that $-1 \in (\mathbb{F}_\ell^\times)^2$ if and only if $\ell \equiv 1 \pmod 4$. □

From Proposition 5.2, it suffices to determine whether a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism we have is of positive or negative symplectic type. It is possible that there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism of positive symplectic type and a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism of negative symplectic type at the same time. By [FK22, Theorem 15], this happens if and only if the image of mod ℓ-representation $\overline{\rho}_{X,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is abelian and not the subgroup generated by a conjugate of $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_\ell)$ for some $a \in \mathbb{F}_\ell^\times$.

5.2. **A Local Test for Symplectic Type.** In the case when the symplectic type is unique, we do not have a general algorithm for determining the symplectic type given $H^\perp/H$ and X. However, if there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which acts on $\mathrm{Jac}(X)[\ell]$ by a non-diagonalizable matrix (i.e., conjugate of $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ for some $a \in \mathbb{F}_\ell^\times$), then this element σ could be used to determine the symplectic type, as detailed in the following proposition, which is a variant of [FK22, Theorem 16].

Proposition 5.3. *Let $\langle \bullet, \bullet \rangle : \mathbb{F}_\ell^2 \times \mathbb{F}_\ell^2 \to \mathbb{F}_\ell$ be a non-degenerate alternating bilinear pairing. Let $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ be a non-diagonalizable matrix. Then, as v varies through $\mathbb{F}_\ell^2$, then $\langle v, Mv \rangle$ is either 0 or does not depend on v up to multiplication by a square.*

Proof. Without loss of generality, change the basis so that $M = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$. Also, scale the inner product by a constant so that $\left\langle \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right), \left(\begin{smallmatrix} x' \\ y' \end{smallmatrix}\right) \right\rangle = xy' - yx'$. If $v = \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, then

$$\langle v, Mv \rangle = \left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} ax + y \\ ay \end{pmatrix} \right\rangle = axy - (axy + y^2) = -y^2, \tag{5.4}$$

giving the desired conclusion. □

In the case of the ℓ-torsion of an elliptic curve X, if there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on $\mathrm{Jac}(X)[\ell]$ by a non-diagonalizable matrix, then by Proposition 5.3, the Weil pairing $e_\ell(P, \sigma(P))$ is either 1 or does not depend on $P \in \mathrm{Jac}(X)[\ell]$ (up to raising to a square power in $\mathbb{F}_\ell^\times$).

Similarly, σ acts on $H^\perp/H$ by the same matrix, so by Proposition 5.3 again, the Weil pairing $e_\ell(Q, \sigma(Q))$ is either 1 or does not depend on $Q \in H^\perp/H$ (up to raising to a square power in $\mathbb{F}_\ell^\times$). If $P = \phi(Q)$, then

$$e_\ell(P, \sigma(P)) = e_\ell(\phi(Q), \sigma(\phi(Q))) = e_\ell(\phi(Q), \phi(\sigma(Q))) = e_\ell(Q, \sigma(Q))^\alpha, \tag{5.5}$$

[1] [FK22] and [CF22] call positive and negative symplectic type symplectic and antisymplectic isomorphism, respectively. We choose a different terminology to avoid confusion.

where α is the symplectic type. Thus, comparing the nontrivial values of $e_\ell(P,\sigma(P))$ and $e_\ell(Q,\sigma(Q))$ for any $P \in \mathrm{Jac}(X)[\ell]$ and $Q \in H^\perp/H$ determines the symplectic type.

To compute this, we note by the Chebotarev density theorem that there exists a prime p for which Frob_p and σ are in the same conjugacy class. Thus, we may reduce both curves into $\overline{\mathbb{F}}_p$ and take $\sigma = \mathrm{Frob}_p$. The following Lemma 5.6 shows that all torsion points are contained in a field extension of degree only $O(\ell^2)$.

Lemma 5.6. *Suppose that p is a prime such that the action of Frob_p on $\mathrm{Jac}(X)[\ell]$ (and hence on $H^\perp/H$) is a nondiagonalizable matrix. Then, we have*

$$\mathrm{Jac}(X)_{\overline{\mathbb{F}}_p}[\ell] = \mathrm{Jac}(X)_{\mathbb{F}_{p^{\ell(\ell-1)}}}[\ell] \quad \textit{and} \tag{5.7}$$

$$\mathrm{Jac}(Y)_{\overline{\mathbb{F}}_p}[\ell] = \begin{cases} \mathrm{Jac}(Y)_{\mathbb{F}_{p^{\ell(\ell-1)}}}[\ell] & \textit{if } \ell \neq 3 \\ \mathrm{Jac}(Y)_{\mathbb{F}_{p^{18}}}[\ell] & \textit{if } \ell = 3 \end{cases} \tag{5.8}$$

Proof. Suppose that the action of Frob_p on $\mathrm{Jac}(X)_{\overline{\mathbb{F}}_p}[\ell]$ is conjugate to $\left(\begin{smallmatrix} \gamma & 1 \\ 0 & \gamma \end{smallmatrix}\right)$ for some $\gamma \in \mathbb{F}_\ell$. We compute the order of Frob_p in both torsion fields.

- For X, by the condition, Frob_p is conjugate to $\left(\begin{smallmatrix} \gamma & 1 \\ 0 & \gamma \end{smallmatrix}\right)$. The n-th power of this is $\left(\begin{smallmatrix} \gamma^n & n\gamma^{n-1} \\ 0 & \gamma^n \end{smallmatrix}\right)$, which is congruent modulo ℓ to the identity matrix when $n = \ell(\ell-1)$.
- For Y, we have that Frob_p must act on $\mathrm{Jac}(Y)_{\overline{\mathbb{F}}_p}[\ell]$ by matrix with eigenvalues α, β, γ, γ, all in $\mathbb{F}_\ell$, where α and β are the eigenvalues corresponding to H and $\mathrm{Jac}(Y)_{\overline{\mathbb{F}}_p}[\ell]/H^\perp$. In particular, we deduce that $(\mathrm{Frob}_p)^{\ell-1} - 1$ has all eigenvalues 0, and hence nilpotent matrix.

  In particular, if no Jordan block of Frob_p has size greater than ℓ, then

$$0 = \left((\mathrm{Frob}_p)^{\ell-1} - 1\right)^\ell = (\mathrm{Frob}_p)^{\ell(\ell-1)} - 1, \tag{5.9}$$

  where the second equality holds because we are in modulo ℓ. The only case that the previous sentence does not cover is when $k = 4$ and $\ell = 3$ (i.e., Frob_p is a single Jordan block), in which case, the order is 18.

Thus, every element in $\mathrm{Jac}(X)_{\overline{\mathbb{F}}_p}[\ell]$ and $\mathrm{Jac}(Y)_{\overline{\mathbb{F}}_p}[\ell]$ is fixed by $(\mathrm{Frob}_p)^{\ell(\ell-1)}$ (or $(\mathrm{Frob}_p)^{18}$ for $\mathrm{Jac}(Y)_{\overline{\mathbb{F}}_p}[\ell]$ and $\ell = 3$), completing the proof. ☐

Remark 5.10. In the version of Algorithm 5.11 given below, we will consider only the case α and β are both distinct from γ, in which case one needs to consider only $\mathbb{F}_{p^{\ell(\ell-1)}}$ even for $\ell = 3$.

5.3. **Algorithm for Determining Symplectic Type.**

With all the tools developed in Section 5.2, we now describe an algorithm to determine the symplectic type on some of the curves.

Algorithm 5.11. *Input.* Two curves X and Y of genus 1 and genus 2 for which a one-dimensional Galois-stable $H \subseteq \mathrm{Jac}(Y)[\ell]$ exists and there exists a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism $\phi : H^\perp/H \to \mathrm{Jac}(X)[\ell]$.

Output. Either `positive` or `negative` symplectic type of ϕ or `fail`, which occurs if and only if p does not exist in (1).

If H does not exist, then the algorithm returns arbitrary output.

(1) Find a prime p such that $(\mathrm{tr}\,\mathrm{Frob}_p)^2 \equiv 4p \pmod{\ell}$. Then, check that Frob_p is not a scalar multiplication by testing if the order of Frob_p does not divide $\ell - 1$.

  If p does not exist (i.e., the image of Galois representation does not have a non-diagonalizable element), then return `fail`.

  Once we found p, consider curves X and Y over $\mathbb{F}_{p^{\ell(\ell-1)}}$.

(2) Pick a random point $P \in \mathrm{Jac}(X)[\ell]$ and then compute $w_1 := e_\ell(P, \mathrm{Frob}_p(P))$. Repeat until this result is not 1.

(3) Determine the characteristic polynomial of $\mathrm{Frob}_p \,|\, \mathrm{Jac}(Y)[\ell]$. Write it in the form $(T-\alpha)(T-\beta)(T-\gamma)^2 \in \mathbb{F}_\ell[T]$ such that $(T-\gamma)^2$ is the characteristic polynomial of $\mathrm{Frob}_p \,|\, \mathrm{Jac}(X)[\ell]$.

  If $\alpha = \beta = \gamma$, repeat (1) again with larger primes.

(4) Pick a random point $R \in \mathrm{Jac}(Y)[\ell]$. Compute $Q = (\mathrm{Frob}_p - \alpha)(\mathrm{Frob}_p - \beta)(R)$. Then, compute $w_2 := e_\ell(Q, \mathrm{Frob}_p(Q))$. Repeat until this result is not 1.

(5) If $w_1 = w_2^{t^2}$ for some $t \in \mathbb{F}_\ell^\times$, then return `positive`. Otherwise, return `negative`.

Remark 5.12. Each attempt in both randomized steps fails with a low probability. More specifically, one can show that the probability that each attempt of both steps (2) and (4) fails is $\frac{1}{\ell}$. (For step (4), note that $\alpha\beta = \gamma^2 = p$, so both α and β are distinct from γ.)

Proposition 5.13. *Algorithm 5.11 correctly determines the symplectic type provided that p exists.*

Proof. It suffices to show that $Q \in H^\perp$. Then, the correctness follows from (5.5).

To do that, assume without loss of generality that Frob_p acts on H by multiplication by α. We define

$$V = \mathrm{Ker}(\mathrm{Frob}_p - \alpha)(\mathrm{Frob}_p - \gamma)^2. \tag{5.14}$$

Since V is a span of the three columns corresponding to α, γ, γ in the Jordan block decomposition, we deduce that $\dim V = 3$. Moreover, the action of Frob_p on $H^\perp$ has characteristic polynomial $(T-\alpha)(T-\gamma)^2$, so we have $H^\perp \subseteq V$. Comparing dimensions gives $H^\perp = V$. Finally, we note that

$$(\mathrm{Frob}_p - \alpha)(\mathrm{Frob}_p - \gamma)^2 Q = (\mathrm{Frob}_p - \alpha)^2(\mathrm{Frob}_p - \beta)(\mathrm{Frob}_p - \gamma)^2 R = 0, \tag{5.15}$$

so $Q \in H^\perp$ as desired. ☐

This algorithm is generally able to handle $\ell \in \{3, 5, 7\}$ in a few seconds.

6. Gluing Curves

Given a genus-2 curve Y, we wish to find a genus-1 curve X to which it can be glued, and then compute the resulting gluing. In this section, we will give a concrete description of our workflow for finding X and computing the gluing. For simplicity, we only look for curves Y such that the Galois representation corresponding to $H^\perp/H$ is irreducible. We then give a demo of how the steps pan out on a particular curve.

The implementation of the workflow described in this section is available at [SW25b].

6.1. **Determining ℓ.** First, as specified by Theorem 2.8 we must find ℓ for which some $H \subset \mathrm{Jac}(Y)[\ell]$ is Galois-stable. We use Algorithm 3.6 to find all possible ℓ for which this holds, possibly along with some spurious ℓ which do not work.

6.2. **Determining X.** Once ℓ is restricted to some finite set, we fix some ℓ. We assume that H as in Theorem 2.8 exists. We wish to find X such that some ψ as in Theorem 2.8 exists.

Each of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroups H corresponds to a trace function that takes a prime number p and output b_p, the trace of $H^\perp/H$. We use Algorithm 3.9 to recover all possible trace functions. (If it reports no trace function, this means that no such H exists.) For each such test function $p \mapsto b_p$, we query in LMFDB all elliptic curves X over $\mathbb{Q}$ that satisfies the conditions of Proposition 3.10 for all prime $p \le 100$. This leaves us with a list of potential elliptic curves.

Next, given a potential X and Y, one can rule out most cases where ϕ has the wrong symplectic type by applying Algorithm 5.11.

Once we have at least one elliptic curve X for which $H^\perp/H$ and $\mathrm{Jac}(X)[\ell]$ have antisymplectic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism, it is possible to characterize all of them. We have the following lemma.

Lemma 6.1. *Let X be as in the above paragraph. Then, for any elliptic curve X', the following are equivalent:*

(i) there exists an antisymplectic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism $H^\perp/H \xrightarrow{\sim} \mathrm{Jac}(X')[\ell]$

(ii) there exists a symplectic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism between $\mathrm{Jac}(X)[\ell]$ and $\mathrm{Jac}(X')[\ell]$.

Proof. Let $\phi : H^\perp/H \to \mathrm{Jac}(X)[\ell]$ be a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism. To prove that (i) implies (ii), let $\phi' : H^\perp/H \to \mathrm{Jac}(X')[\ell]$. Then, the map $\psi = \phi' \circ \phi^{-1} : \mathrm{Jac}(X)[\ell] \to \mathrm{Jac}(X')[\ell]$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism. It is symplectic because for any $P, Q \in \mathrm{Jac}(X)[\ell]$,

$$e_\ell(P,Q) = e_\ell(\phi^{-1}(P), \phi^{-1}(Q))^{-1} = e_\ell\big(\phi'(\phi^{-1}(P)), \phi'(\phi^{-1}(Q))\big) = e_\ell(\psi(P), \psi(Q)). \tag{6.2}$$

In the direction (ii) implies (i), given $\psi : \mathrm{Jac}(X)[\ell] \to \mathrm{Jac}(X')[\ell]$, then we can construct ϕ' by $\phi' = \psi \circ \phi$. One can similarly see that ϕ' is antisymplectic. ☐

Thus, given such an X, the problem of finding all such X' is reduced to finding an elliptic curve ℓ-congruent to X with positive symplectic type. When $\ell \in \{2, 3, 5\}$, the moduli space of all such X' is a curve of genus 0 and have been worked out in [RS01] and [RS95]. When $\ell \ge 7$, the moduli space of X' is a curve of genus at least 3. By Falting's theorem, any curve of genus greater than 1 has finitely rational points. Thus, for $\ell \ge 7$, there will be only finitely many such X' defined over $\mathbb{Q}$. Still, the equation for the curve of all possible X' has been worked out for $\ell \in \{7, 11\}$ in [Fis14].

Remark 6.3 (The reducible case). In the case where the Galois representation corresponding to $H^\perp/H$ is reducible, following the above steps above is not enough to filter the list of elliptic curves into managable size. For example, starting with the curve `961.a.961.1` in LMFDB and $\ell = 5$ leaves 3083 potential elliptic curves. This is because Frobenius traces can only prove that $\overline{\rho}_X$ and $\overline{\rho}_{H^\perp/H}$ are isomorphic up to semisimplification.

There are two possible strategies that we can narrow this list down further. Suppose that X is an elliptic curve such that $\overline{\rho}_X \simeq \overline{\rho}_{H^\perp/H}$.

(1) **Discriminant.** Suppose that p is a prime not dividing N_Y such that X has a multiplicative reduction modulo p. Thus, the Galois representation $\overline{\rho}_X$ should be unramified at p, and so by using the theory of Tate's curve, one can deduce that ℓ divides $\nu_p(\Delta_{\min}(X))$ (where $\Delta_{\min}$ denotes the minimal discriminant). Thus, we can rule out a large number of potential elliptic curves for which this condition does not hold.
(2) **Diagonal Matrix.** Let p be a prime such that $\overline{\rho}_Y(\mathrm{Frob}_p)$ is a diagonal matrix in $\mathrm{GSp}_4(\mathbb{F}_\ell)$, then $\overline{\rho}_X(\mathrm{Frob}_p)$ is also a diagonal matrix in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Thus, one can find such primes p and use them to rule of the elliptic curves further.

Running these two strategies on the curve `961.a.961.1` (with primes 1301, 2351, 4211, 5171, 16001, 17881, 24371, 31181, 35531, 36451, 37361, 45751 in Step (2)) reduces the number of candidates to only 9. However, this does not work very well on some other curves, especially $\ell = 3$, due to sheer number of candidates and the rarity of primes p in Step (2).

6.3. **Computing Gluing.** The computation of gluing is based on the numerical algorithm in [HSS21, Section 2.1] and the code from [HSS20]. However, we made several optimizations. First, we replace the original theta function algorithm with a faster implementation from FLINT [EK24]. Second, the original code repeatedly tests a random maximal isotropic subgroup of $\mathrm{Jac}(X)[\ell] \times \mathrm{Jac}(Y)[\ell]$. However, this proves to be inefficient since there are $\Theta(\ell^6)$ such subgroups [HSS21, Corollary 1.20].

To optimize this, we propose the following two-step approach to search for the desired subgroup.

(1) Determine which one-dimensional subgroup H is rational.
(2) Determine which antisymplectic isomorphism $\phi : X[\ell] \to H^\perp/H$ gives rise to a gluing.

This gives the following algorithm.

Algorithm 6.4. *Input.* An elliptic curve X, a genus 2 curve Y, and a prime ℓ.

Output. A (possibly empty) list of all genus 3 curves Z defined over $\mathbb{Q}$ such that $\mathrm{Jac}(Z) \sim (\mathrm{Jac}\, X \times \mathrm{Jac}\, Y)/G$ for some maximal isotropic subgroup $G \subset \mathrm{Jac}(X)[\ell] \times \mathrm{Jac}(Y)[\ell]$.

(1) Compute the period matrix of Y, giving a basis $\{P_1, P_2, P_3, P_4\}$ of lattice Λ such that $\mathrm{Jac}(Y) \simeq \mathbb{C}^2/\Lambda$.
(2) For each ratio $(a_1 : a_2 : a_3 : a_4) \in \mathbb{P}^3(\mathbb{F}_\ell)$, test whether the subgroup H generated by torsion point $\frac{a_1}{\ell}P_1 + \frac{a_2}{\ell}P_2 + \frac{a_3}{\ell}P_3 + \frac{a_4}{\ell}P_4$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable.
(3) For each H determined to be $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable in (2), enumerate all antisymplectic isomorphisms $\phi : X[\ell] \to H^\perp/H$.
(4) For each such ϕ, use (ϕ, H) to generate the isotropic subgroup G according to [HSS21, Proposition 1.18]. Compute a period matrix of the lattice $\mathrm{Jac}(X) \times \mathrm{Jac}(Y)/G$. From this lattice, compute Diximier-Ohno invariants using [KLLRSS18] or Shioda invariants using [BILV16] and test whether they are defined over $\mathbb{Q}$ or not.
(5) For any set of invariants that are in $\mathbb{Q}$, reconstruct the curve Z using the methods in [KLLRSS18] for plane quartics or [BILV16] for hyperelliptic curves.

In Step (2), there are $\#\mathbb{P}^3(\mathbb{F}_\ell) = \ell^3 + \ell^2 + \ell + 1 = \Theta(\ell^3)$ possible H's to check. In Step (3), there are $\#\,\mathrm{SL}_2(\mathbb{F}_\ell) = \ell(\ell^2 - 1) = \Theta(\ell^3)$ isomorphisms to check. Thus, this algorithm reduces checking $\Theta(\ell^6)$ subgroups to at most checking $\Theta(\ell^3)$ things to check at a time, making it much more efficient.

We implemented this algorithm in Magma V.2.28-16. The timing of this algorithm against simply enumerating all maximal isotropic subgroups is shown in Table 1. The timing was taken on CPU 12th Gen Intel i9-12900K (24) @5.100GHz on five different test cases in which one can find a gluing when working with precision 500. Note that the timing only measures time to compute (Diximier-Ohno or Shioda) invariants and does not include time to reconstruct the curve.

	$\ell = 3$	$\ell = 5$	$\ell = 7$
Enumerate all subgroups	144.5 s	5760 s	(not attempted)
Using Algorithm 6.4	11.8 s	71.9 s	241 s

Table 1. Time taken to compute invariants of all possible gluings with precision 500.

6.4. **Example.** We provide a rundown of our algorithms on a particular curve.

Example 6.5. Let Y be the genus 2 curve $y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x$ (277.a.277.1 in the LMFDB). Running Algorithm 3.6 on this curve yields the result $\{3, 5\}$, meaning that the only possible choices of ℓ are 3 and 5. From now, suppose we are looking for a $(5, 5)$-gluing, i.e., $\ell = 5$.

We next run Algorithm 3.9 on the input $(Y, 5)$. Since the conductor of Y is 277, which is prime, the algorithm concludes immediately that χ must be trivial, i.e., $\chi(p) = 1$ for all p. (This is also reflected by the fact that Y has a rational 5-torsion subgroup.) Thus, we may compute the Frobenius traces b_p of $H^\perp/H$ from the Frobenius traces $a_{p,Y}$ of Y. For example,

$$F_{Y,13}(T) = T^4 - 3T^3 + 7T^2 - 39T + 169, \quad a_{Y,13} = 3, \quad \text{and} \quad b_{13} = 3 - 1 - \frac{13}{1} = 4 \pmod 5. \tag{6.6}$$

We can repeat the above process to compute b_p for all primes $p \leq 100$. Then, we search for all elliptic curves in the LMFDB satisfying the trace constraints detailed in Proposition 3.10. The result is the four curves shown in Table 2.

	LMFDB	Equation	Symplectic Test
X_1	1939.b1	$y^2 + y = x^3 - 1916x - 32281$	positive symplectic type
X_2	18559.a1	$y^2 + y = x^3 + 11734x - 21208$	negative symplectic type
X_3	21883.b1	$y^2 + y = x^3 - 86x - 44420$	positive symplectic type
X_4	32963.c1	$y^2 + y = x^3 - 77866x + 8364065$	positive symplectic type

Table 2. Potential elliptic curves gluable to curve 277.a.277.1

We can run symplectic test in Algorithm 5.11 to test the antisymplectic condition. Both curves can be tested using $p = 19$, and the results are shown in Table 2. Since we are in the case $\ell \equiv 1 \pmod 4$, by Proposition 5.2, the symplectic test rules out X_2

Thus, our algorithm found the curves X_1, X_3, and X_4. This is *not* a proof that these curves are gluable to Y. We can either use Algorithm 4.14 or computing the gluing explicitly to prove that they actually form a Galois stable maximal isotropic subgroup G.

For $i \in \{1, 3, 4\}$, running the code referenced in Section 6.3 on X_i and Y shows that there are indeed gluings Z_i. The invariants of Z_1 and Z_3 was obtained by computing at precision 500, while the invariants of Z_4 was obtained at precision 1000. It took about 30 seconds to find the coordinates of H and less than 60 seconds to find the invariants for each of Z_1, Z_3, and Z_4. However, by far dominating every computation we have done is obtained the minimized equations for Z_4, which took just over an hour. The minimized equations of Z_1, Z_3, and Z_4 are given in (6.7), (6.8), and (6.9).

$$\begin{aligned} Z_1 : 88189x^4 &- 398531x^3y + 7700x^3z - 678120x^2y^2 + 1444780x^2yz + 231034x^2z^2 \\ &+ 238603xy^3 - 1620885xy^2z - 218291xyz^2 - 420855xz^3 + 82587y^4 \\ &- 2912900y^3z + 333537y^2z^2 - 959874yz^3 - 281678z^4 = 0 \end{aligned} \tag{6.7}$$

$$Z_3 : y^2 = 448x^8 + 3584x^7 + 2016x^6 - 476x^5 - 13020x^4 - 16408x^3 - 18340x^2 - 8988x - 4025 \tag{6.8}$$

$$\begin{aligned} Z_4 : 19351616x^4 &+ 136748535x^3y + 106394158x^3z - 235515177x^2y^2 - 46043175x^2yz + 67674485x^2z^2 \\ &- 549641282xy^3 + 36999650xy^2z - 160500711xyz^2 - 36439076xz^3 + 272167382y^4 \\ &+ 488584945y^3z - 488728851y^2z^2 + 152950443yz^3 - 115190535z^4 = 0 \end{aligned} \tag{6.9}$$

7. Examples

We now report on some examples resulting from the search process in Section 6. As in Section 6.3, the amount of time to computing gluing is measured by the time taken to compute Diximier-Ohno invariants or Shioda invariants. It does not include time to reconstruct or minimize the curve. All timings were done on CPU 12th Gen Intel i9-12900K (24) @5.100GHz.

7.1. Gluing Along Large Torsion.

Our work allows us to look for gluings along ℓ-torsion for larger ℓ.

We first note that for $\ell \in \{7, 11, 13, 17, 19, 37, 43, 67, 163\}$ (i.e., all $\ell \geq 7$ for which there exists an ℓ-isogeny of elliptic curves, by Mazur's isogeny theorem [Maz78, Theorem 1]), one can construct infinitely many gluable candidates of genus 1 and genus 2 curves. Here, a ***gluable candidate*** is a pair of curves (X, Y) such that X has genus 1, Y has genus 2, and there exists a Galois stable maximal isotropic subgroup $G \subset X[\ell] \times \mathrm{Jac}(Y)[\ell]$. From Remark 2.10, gluable candidate does not necessary produce a gluing.

To construct those gluable candidates, we consider pairs of elliptic curve X and genus 2 curve Y such that

- Y is isogenous to product of two elliptic curves $Y_1 \times Y_2$;
- Y_1 has ℓ-isogeny; and
- $X[\ell]$ and $Y_2[\ell]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

Call a gluable candidate (X, Y) ***uninteresting*** if it is of the above form and ***interesting*** otherwise.

Proposition 7.1. *For $\ell \in \{7, 11, 13, 17, 19, 37, 43, 67, 163\}$, there exists infinitely uninteresting gluable candidates (X, Y) along ℓ-torsion.*

Proof. Let $p = 2$ if $\ell \equiv 1$ or $3 \pmod 8$ and $p = 3$ if $\ell \in \{7, 13, 37\}$. Let Y_1 be an elliptic curve with ℓ-isogeny, and let Y_2 be an elliptic curve such that $Y_2[p]$ and $Y_1[p]$ are antisymplectically isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. There are infinitely many such Y_2 because when $p = 2$, one can take elliptic curves whose 2-torsion field is isomorphic to Y_1, and when $p = 3$, this follows from [Fis06, Section 13].

The curves Y_1 and Y_2 are gluable along p-torsion, producing a curve Y for which there exists a p-isogeny $\phi : Y_1 \times Y_2 \to \mathrm{Jac}(Y)$. Since $\ell \neq p$, the map ϕ induces an isomorphism $\phi : Y_1[\ell] \times Y_2[\ell] \xrightarrow{\sim} \mathrm{Jac}(Y)[\ell]$. This isomorphism is antisymplectic because by our choice of ℓ, the number $-\ell$ is a quadratic residue modulo p.

Let X be any elliptic curve such that $X[\ell]$ and $Y_2[\ell]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. In particular, we may take $X = Y_2$. We now show that X and Y are gluable.

- Since Y_1 has ℓ-isogeny, there exists a one-dimensional subgroup $G \subset Y_1[\ell]$. Then, the image $H := \phi(G \times \{0\})$ is a one-dimensional subgroup of $\mathrm{Jac}(Y)$.
- By Galois equivariance of Weil pairing, we have $H^\perp/H = \phi(\{0\} \times Y_2)$. Since ϕ is antisymplectic, $H^\perp/H$ and Y_2 are antisymplectic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. □

We thus look for interesting gluable candidates. For $\ell \geq 11$, our search across all genus 2 in LMFDB concludes that there are no interesting gluable candidates between curves in LMFDB. Therefore, we use a larger dataset of genus 2 curves provided by Sutherland [Sut22] to obtain the following examples. We check that the gluing is interesting by computing the geometric endomorphism algebra of Y using [CMSV19].

Example 7.2 (Interesting gluing along 11-torsion)**.** Let X be an elliptic curve $y^2 + xy = x^3 + 9096x + 224832$ (`966.k1` in LMFDB). Let Y be a genus 2 curve $y^2 + (x^2 + x)y = x^6 - 3x^5 + 9x^4 - 5x^3 + 12x^2 - 6x$, which has conductor 19044 and minimal discriminant 1 151 517 855 744. Our code computes a gluing along 11-torsion of X and Y in 16 minutes under precision 500, and minimizing the curve equation gives

$$\begin{aligned} Z : 39753x^4 + 89236x^3y - 76006x^3z - 3537x^2y^2 - 469x^2yz + 46697x^2z^2 - 2200xy^3 + 42003xy^2z \\ + 29597xyz^2 - 58478xz^3 - 4883y^4 - 12000y^3z - 9287y^2z^2 - 398yz^3 + 6544z^4 = 0, \end{aligned} \tag{7.3}$$

Example 7.4 (Interesting gluing along 13-torsion)**.** Let X be an elliptic curve $y^2 + y = x^3 + x^2 - 208x - 1256$ (`75.a1` in LMFDB). Let Y be a genus 2 curve $y^2 + x^3y = -5x^4 + 45x^2 + 9x$, which has conductor 151 875 and minimal discriminant 2 883 251 953 125. Our code computes a gluing along 13-torsion of X and Y in 24 minutes under precision 1000, and minimizing the curve equation gives

$$Z : y^2 = 1008x^8 - 4032x^7 + 336x^6 + 8064x^5 + 9660x^4 - 4914x^3 - 7434x^2 - 2478x + 2058 \tag{7.5}$$

7.2. **Curves with Interesting Geometric Endomorphism Rings.** For any abelian variety A, the ***geometric endomorphism ring*** $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is the ring of all endomorphisms $A \to A$ defined over $\overline{\mathbb{Q}}$. For any curve C, its geometric endomorphism ring is defined as the geometric endomorphism ring of its Jacobian $\mathrm{End}(C_{\overline{\mathbb{Q}}}) := \mathrm{End}(\mathrm{Jac}\, C_{\overline{\mathbb{Q}}})$. The ***geometric endormorphism algebra*** of a curve C is defined as $\mathrm{End}(C_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$. If Z is a gluing of X and Y, then the geometric endomorphism algebra of Z can be easily determined by the geometric endomorphism algebra of X and Y. Furthermore, one can verify the endomorphism algebra by the code in [CMSV19].

Example 7.6. Let X be the elliptic curve $y^2 = x^3 + x^2 - 3x + 1$ (`256.a2` in the LMFDB). Let Y be the genus 2 curve $y^2 + y = 6x^5 + 9x^4 - x^3 - 3x^2$ (`20736.l.373248.1` in the LMFDB).

There are two gluings between X and Y with $\ell = 3$, whose minimized equations are given in (7.7) and (7.8).

$$Z : y^2 = -210x^7 - 630x^6 + 245x^5 + 1155x^4 - 70x^3 - 700x^2 + 140 \tag{7.7}$$

$$\begin{aligned} Z' : 8x^4 - 26x^3y + 26x^2y^2 + 32xy^3 - 3y^4 + 29x^3z - 26x^2yz + 234xy^2z \\ - 26y^3z + 153x^2z^2 + 22xyz^2 + 17y^2z^2 + 65xz^3 - 250yz^3 + 25z^4 = 0 \end{aligned} \tag{7.8}$$

One can compute $\mathrm{End}(X_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq \mathbb{Q}[\sqrt{-2}]$ and $\mathrm{End}(Y_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq B_{2,3}$, so

$$\mathrm{End}(Z_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq \mathrm{End}(Z'_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq \mathbb{Q}[\sqrt{-2}] \times B_{2,3}, \tag{7.9}$$

where $B_{2,3}$ is the unique quaternion algebra over $\mathbb{Q}$ ramified at 2 and 3.

Example 7.10. Let X be the elliptic curve $y^2 + xy = x^3 - x^2 - 107x + 552$ (`49.a2` in the LMFDB) and Y be the genus 2 curve $y^2 + (x^2 + x)y = x^5 + x^4 + 2x^3 + x^2 + x$ (`686.a.686.1` in the LMFDB). A gluing of X and Y with $\ell = 3$ is given by a quartic

$$Z : 7x^4 + 28x^2z^2 + 24xy^2z + 7y^4 - 4z^4 = 0. \tag{7.11}$$

The Jacobian $\mathrm{Jac}(Y)$ is isogenous to product of two elliptic curves, one of which is X, and the other is X' in isogeny class `14.a` in LMFDB. Therefore, $\mathrm{Jac}(Z) \sim X^2 \times X'$. Since are $\mathrm{End}(X_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{-7})$ and $\mathrm{End}(X'_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq \mathbb{Q}$, we have

$$\mathrm{End}(Z_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \simeq \mathrm{Mat}_2(\mathbb{Q}(\sqrt{-7})) \times \mathbb{Q}. \tag{7.12}$$

7.3. **Gluing Curves in the LMFDB.** We have applied our algorithms to every genus 2 curve Y in the LMFDB to identify triples (X, Y, ℓ) such that X and Y are potentially gluable along ℓ-torsion where one of the following criteria are met:

- $\ell = 3$ and $H^\perp/H$ is an irreducible Galois module. (If $H^\perp/H$ is reducible, our filtering methods result in a large number of false positives.) Our methods identified 3009 genus 2 curves Y for which at least one candidate X exists.
- $\ell \geq 5$. We have identified 704 pairs of (Y, ℓ) for which at least one candidate X exists. The distribution by ℓ is shown in Table 3. Note that all gluings for $\ell \geq 11$ are uninteresting in the sense of Proposition 7.1. Of these pairs, 44 curve Y's have $H^\perp/H$ reducible, all of which comes from $\ell = 5$.

ℓ	5	7	11	13	19	37	67
Number of Y's	649	35	11	2	4	2	1

Table 3. Number of Y for which there exists at least one candidate of gluable elliptic curves along ℓ-torsion.

For every such (Y, ℓ) such that $H^\perp/H$ is irreducible and we are able to run the symplectic test, we attempt to glue Y to the candidate X which has minimal conductor. For $\ell = 3$ we attempt this even when we cannot run the symplectic test. The result is shown in Table 4. In all but two cases that we did not find a gluing, the curve Y have a split Jacobian, in which believe that the cause of failure comes from that the condition (ii) of Theorem 2.9 does not hold (cf. Remark 2.10). One further case comes from a pair with the wrong symplectic type on which the symplectic test did not produce a result. The only other case that we did not find a gluing is when $\ell = 3$, Y is the genus 2 curve labeled `471900.a.943800.1` in LMFDB, and X is the elliptic curve `298800.ff.1` in LMFDB. In this case, the Galois representations $H^\perp/H$ and $X[3]$ are not isomorphic because the former is unramified at 83 but the latter does not.

The output of our gluings can be found in [SW25a].

	$\ell = 3$	$\ell = 5$	$\ell = 7$
$H^\perp/H$ irreducible and (for $\ell > 3$) passes symplectic test	3009	595	32
Successful gluing	2575	536	19
Gives an error	5	9	1
Did not find gluing	429	50	12

Table 4. Gluing Results.

References

[BILV16] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. "Constructing genus-3 hyperelliptic Jacobians with CM". In: *LMS J. Comput. Math.* 19 (2016), pp. 283–300 (↑ 15).

[BK75] B. J. Birch and W. Kuyk, eds. *Modular functions of one variable. IV.* Vol. Vol. 476. Lecture Notes in Mathematics. Springer-Verlag, Berlin-New York, 1975, pp. iv+151 (↑ 1).

[BCCK24] Raymond van Bommel, Shiva Chidambaram, Edgar Costa, and Jean Kieffer. "Computing isogeny classes of typical principally polarized abelian surfaces over the rationals". In: *LuCaNT: LMFDB, computation, and number theory.* Vol. 796. Contemp. Math. Amer. Math. Soc., [Providence], RI, 2024, pp. 187–214 (↑ 3, 5).

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. "On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises". In: *J. Amer. Math. Soc.* 14.4 (2001), pp. 843–939 (↑ 10).

[BHLS15] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen. "Genus-2 curves and Jacobians with a given number of points". In: *LMS J. Comput. Math.* 18.1 (2015), pp. 170–197 (↑ 2).

[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 (↑ 17, 18).

[Cre06] John Cremona. "The elliptic curve database for conductors to 130000". In: *Algorithmic number theory.* Vol. 4076. Lecture Notes in Comput. Sci. Springer, Berlin, 2006, pp. 11–29 (↑ 1).

[CF22] John E. Cremona and Nuno Freitas. "Global methods for the symplectic type of congruences between elliptic curves". In: *Rev. Mat. Iberoam.* 38.1 (2022), pp. 1–32 (↑ 1, 11, 12).

[Die02] Luis V. Dieulefait. "Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$". In: *Experiment. Math.* 11.4 (2002), pp. 503–512 (↑ 5).

[EK24] Noam D. Elkies and Jean Kieffer. "A uniform quasi-linear time algorithm for evaluating theta functions in any dimension". In preparation. 2024 (↑ 15).

[Fis06] Tom Fisher. "The Hessian of a genus one curve". In: *Proceedings of the London Mathematical Society* 104 (Nov. 2006) (↑ 7, 17).

[Fis14] Tom Fisher. "On families of 7- and 11-congruent elliptic curves". In: *LMS J. Comput. Math.* 17.1 (2014), pp. 536–564 (↑ 1, 15).

[Fis20] Tom Fisher. "Explicit moduli spaces for congruences of elliptic curves". In: *Math. Z.* 295.3-4 (2020), pp. 1337–1354 (↑ 1).

[FK22] Nuno Freitas and Alain Kraus. "On the symplectic type of isomorphisms of the p-torsion of elliptic curves". In: *Mem. Amer. Math. Soc.* 277.1361 (2022), pp. v+105 (↑ 2, 12).

[FK91] Gerhard Frey and Ernst Kani. "Curves of genus 2 covering elliptic curves and an arithmetical application". In: *Arithmetic algebraic geometry (Texel, 1989).* Vol. 89. Progr. Math. Birkhäuser Boston, Boston, MA, 1991, pp. 153–176 (↑ 1).

[Han20] Jeroen Hanselman. "Gluing curves of genus 2 and genus 1 along their 2-torsion". PhD thesis. Univeristät Ulm, 2020 (↑ 3).

[HSS20] Jeroen Hanselman, Sam Schiavone, and Jeroen Sijsling. "`gluing`, a Magma package for gluing curves of low genus along their torsion". 2020 (↑ 2, 15).

[HSS21] Jeroen Hanselman, Sam Schiavone, and Jeroen Sijsling. "Gluing curves of genus 1 and 2 along their 2-torsion". In: *Math. Comp.* 90.331 (2021), pp. 2333–2379 (↑ 2, 3, 4, 15).

[HLP00] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. "Large torsion subgroups of split Jacobians of curves of genus two or three". In: *Forum Math.* 12.3 (2000), pp. 315–364 (↑ 2).

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger. "Serre's modularity conjecture. I". In: *Invent. Math.* 178.3 (2009), pp. 485–504 (↑ 8).

[KLLRSS18] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. "Plane quartics over $\mathbb{Q}$ with complex multiplication". In: *Acta Arith.* 185.2 (2018), pp. 127–156 (↑ 15).

[KO92] A. Kraus and J. Oesterlé. "Sur une question de B. Mazur". In: *Mathematische Annalen* 293.1 (Dec. 1992), pp. 259–275 (↑ 10).

[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 (↑ 3).

[LMFDB] The LMFDB Collaboration. "The L-functions and modular forms database". `https://www.lmfdb.org`. [Online; accessed 30 July 2024]. 2024 (↑ 1).

[Maz78] Barry Mazur. "Rational isogenies of prime degree (with an appendix by D. Goldfeld)". In: *Invent. Math.* 44.2 (1978), pp. 129–162 (↑ 17).

[Mil08] James S. Milne. "Abelian Varieties (v2.00)". `www.jmilne.org/math/CourseNotes/av.html`. 2008 (↑ 3, 5, 10).

[OU73] Frans Oort and Kenji Ueno. "Principally polarized abelian varieties of dimension two or three are Jacobian varieties". In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 20 (1973), pp. 377–381 (↑ 3).

[Ray74] Michel Raynaud. "Schémas en groupes de type $(p, \ldots, p)$". In: *Bull. Soc. Math. France* 102 (1974), pp. 241–280 (↑ 5, 9).

[RR18] Christophe Ritzenthaler and Matthieu Romagny. "On the Prym variety of genus 3 covers of genus 1 curves". In: *Épijournal Géom. Algébrique* 2 (2018), Art. 2, 8 (↑ 2).

[RS95] K. Rubin and A. Silverberg. "Families of elliptic curves with constant mod p representations". In: *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*. Vol. I. Ser. Number Theory. Int. Press, Cambridge, MA, 1995, pp. 148–161 (↑ 1, 14).

[Rub97] Karl Rubin. "Modularity of mod 5 representations". In: *Modular forms and Fermat's last theorem (Boston, MA, 1995)*. Springer, New York, 1997, pp. 463–474 (↑ 7).

[RS01] Karl Rubin and Alice Silverberg. "Mod 2 Representations of Elliptic Curves". In: *Proceedings of the American Mathematical Society* 129.1 (2001), pp. 53–57 (↑ 1, 14).

[SW25a] Pitchayut Saengrungkongka and Noah Walsh. "`gluing_data`". 2025 (↑ 19).

[SW25b] Pitchayut Saengrungkongka and Noah Walsh. "`gluing_utilities`". 2025 (↑ 14).

[Ser87] Jean-Pierre Serre. "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$". In: *Duke Math. J.* 54.1 (1987), pp. 179–230 (↑ 8, 9).

[Sil97] Alice Silverberg. "Explicit families of elliptic curves with prescribed mod N representations". In: *Modular forms and Fermat's last theorem (Boston, MA, 1995)*. Springer, New York, 1997, pp. 447–461 (↑ 1).

[Sil94] Joseph H. Silverman. "Advanced topics in the arithmetic of elliptic curves". Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525 (↑ 7).

[Sil09] Joseph H. Silverman. "The arithmetic of elliptic curves". Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513 (↑ 7).

[Stu87] Jacob Sturm. "On the congruence of modular forms". In: *Number theory (New York, 1984–1985)*. Vol. 1240. Lecture Notes in Math. Springer, Berlin, 1987, pp. 275–280 (↑ 10, 11).

[Sut22] Andrew Sutherland. "A database of genus 2 curves over $\mathbb{Q}$ with conductor less than 2^{20}." 2022 (↑ 17).

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
Email address: psaeng@mit.edu

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
Email address: nwalsh21@mit.edu