# Computing the mod-3 Galois image of a principally polarized abelian surface over the rationals

Shiva Chidambaram

Abstract. There has been considerable work around computing the images of Galois representations coming from elliptic curves. This paper reports on an algorithm to determine the image of the mod-3 Galois representation associated to a principally polarized abelian surface over $\mathbb{Q}$. Conjugacy class distribution of subgroups of $\mathrm{GSp}(4, \mathbb{F}_3)$ is a key ingredient. While this ingredient is feasible to compute for $\mathrm{GSp}(4, \mathbb{F}_\ell)$ for any small prime $\ell$, the problem of distinguishing Gassmann-equivalent subgroups is delicate. We accomplish it for $\ell = 3$, using a combination of techniques. The algorithm does not require the knowledge of the endomorphism ring.

## 1. Introduction

Given an elliptic curve $E/\mathbb{Q}$, the problem of understanding the Galois action on its $\ell$-torsion points for a prime $\ell$ is fundamental. This leads to the concrete question of determining the image of the associated mod-$\ell$ Galois representation $\overline{\rho}_{E,\ell} : G_\mathbb{Q} \to \mathrm{GL}(2, \mathbb{F}_\ell)$ up to conjugacy in $\mathrm{GL}(2, \mathbb{F}_\ell)$. There are efficient algorithms [**16**] accomplishing this task. Moreover, when $E$ does not have complex multiplication, the works [**14, 15**] present algorithms to compute the $\ell$-adic Galois image, and Zywina goes further and computes the full adelic Galois image [**19**].

A natural next step is to tackle this problem for a principally polarized abelian surface $A/\mathbb{Q}$. For any prime $\ell$, let $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$. The $\ell$-torsion subgroup $A[\ell]$ is a 4-dimensional vector space over $\mathbb{F}_\ell$, having a non-degenerate, Galois covariant, alternating pairing – the Weil pairing. Thus the Galois action gives rise to a mod-$\ell$ Galois representation $\overline{\rho} := \overline{\rho}_{A,\ell} : G_\mathbb{Q} \to G_\ell$, such that its composition with the similitude character $\chi_{\mathrm{sim}} : G_\ell \to \mathbb{F}_\ell^\times$ is equal to the mod-$\ell$ cyclotomic character $\chi_\ell$. Given $A/\mathbb{Q}$ and a prime $\ell$, it is desirable to determine the mod-$\ell$ Galois image $\mathrm{im}(\overline{\rho}_{A,\ell})$ up to conjugacy inside $G_\ell$. When $A$ has no extra endomorphisms, Serre's open image theorem implies that the set of primes $\ell$ with $\mathrm{im}(\overline{\rho}_{A,\ell}) \neq G_\ell$ is finite. An algorithm to determine a superset of the set of non-surjective primes was given in [**11**] and implemented and studied thoroughly in [**2**]. Building on this, [**18**] gives a complete algorithm for computing the rational isogeny class of $A$.

**Definition 1.1.** A subgroup $H$ of $G_\ell$ is said to be eligible if the restriction of $\chi_{\mathrm{sim}}$ to $H$ is surjective, and there exists $x \in H$ of order 2 such that $\chi_{\mathrm{sim}}(x) = -1$.

---

2020 *Mathematics Subject Classification.* Primary 11F80; 11G10.

The author was supported by Simons Foundation grant 550033.

Since $\chi_\ell = \chi_{\text{sim}} \circ \overline{\rho} : G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ is surjective, and complex conjugation is an order 2 element $c \in G_{\mathbb{Q}}$ with $\chi_\ell(c) = -1$, the mod-$\ell$ Galois image $\operatorname{im}(\overline{\rho}_{A,\ell})$ of a principally polarized abelian surface over $\mathbb{Q}$ can only be an eligible subgroup.

We provide a method to completely accomplish this task when $\ell = 3$. It works for all principally polarized abelian surfaces without any restriction on endomorphism type. It consists of a probabilistic Monte Carlo Algorithm 2.3 that determines the conjugacy class distribution of the image of $\overline{\rho}_{A,3}$, followed by a deterministic Algorithm 2.9 that determines $\operatorname{im}(\overline{\rho}_{A,3})$ up to $G_3$-conjugacy. We present the algorithm for Jacobians of genus 2 curves, but it can be extended to include abelian surfaces presented as the Weil restriction of an elliptic curve over a quadratic field.

Magma [**3**] code implementing the algorithm is available at the GitHub repository [**9**]. The main intrinsic is called `mod3Galoisimage`, which takes a genus 2 curve as input, and optionally a lower bound for probability $\epsilon$, and two prime bounds $B_1, B_2$ (see Algorithm 2.3). Worked out examples can be found in the file `examples.m`. We have used it to compute the mod-3 Galois images for all 66 158 genus 2 curves in the L-functions and Modular Forms Database LMFDB [**13**]. We have also computed these images for a bigger dataset consisting of 487 493 genus 2 curves with 5-smooth conductors. Section 2 presents our main algorithms and Section 3 discusses the challenges in computing mod-$\ell$ images for $\ell > 3$.

Any representation $\overline{\rho} : G_{\mathbb{Q}} \to G_3$ with $\chi_{\text{sim}} \circ \overline{\rho} = \chi_3$ is known to arise as the mod-3 Galois representation of infinitely many prinicipally polarized abelian surfaces over $\mathbb{Q}$ [**4**]. This is proven by showing that the corresponding twist of the Siegel modular variety $\mathcal{A}_2(3)$, which may not be rational over $\mathbb{Q}$ [**6**], is nevertheless unirational over $\mathbb{Q}$ via a map of degree at most 6. A consequence of this result is that any eligible subgroup of $G_3$ arises as the mod-3 Galois image of some principally polarized abelian surface over $\mathbb{Q}$. Up to conjugacy $G_3$ has 492 subgroups; 330 of them are not contained in $\operatorname{Sp}(4, \mathbb{F}_3)$ and 280 of them are eligible subgroups. This leads to the following question.

**Question 1.2.** Can we *explicitly* realize each of the 280 eligible subgroups of $G_3$ as the mod-3 Galois image of some principally polarized abelian surface over $\mathbb{Q}$?

Our computations on the LMFDB curves and the 5-smooth curves have already yielded 227 subgroups of $G_3$ as mod-3 Galois images. The work [**5**] outlines a method of explicitly constructing a genus 2 curve starting from the mod-3 Galois representation $\overline{\rho}$. Out of the remaining 53 subgroups, it seems feasible to use this approach for the 26 subgroups of order less than 48. Section 4 discusses progress towards this question.

**Notation:** Throughout this article, we use the LMFDB labeling scheme [**1**] for referring to subgroups of $G_\ell$. The label is a string `ℓ.i.n`, where `i` is the index in $G_\ell$, and `n` is a counter giving a canonical ordering of all index-$i$ subgroups of $G_\ell$.

## 2. Computing the mod-3 Galois image

Suppose $A$ is given as the Jacobian of a genus 2 curve $C/\mathbb{Q} : y^2 = f(x)$ with $\deg(f) = 5$ or 6. Let $S$ denote the set of primes of bad reduction for $A$. We want to determine the image of $\overline{\rho}_{A,3}$ up to conjugacy in $G_3$. This group is abstractly isomorphic to the Galois group of the 3-torsion field. Although the latter can be computed from a 3-division polynomial, it is not enough to determine $\operatorname{im}(\overline{\rho}_{A,3})$ up to $G_3$-conjugacy. The difficulty comes from the presence of outer automorphisms. Remark 2.1 discusses this issue in the simpler case $\ell = 2$.

**18 Jun 2025 19:18:56 PDT**
**250131-Chidambaram Version 4 - Submitted to LuCaNT**

**Remark 2.1.** For $\ell = 2$, since the 2-torsion field of $A$ is the splitting field of $f(x)$, the mod-2 Galois image is abstractly isomorphic to the Galois group $\mathrm{Gal}(f) \subseteq S_6 \simeq G_2$. But the identification $S_6 \simeq G_2$ must be chosen carefully since $S_6$ has an outer automorphism. This is done, for instance, by noting that pairs of Weierstrass points on $C$ correspond to points in $A[2]$, and matching the two conjugacy classes of order-48 subgroups correctly: the subgroup of $S_6$ that has orbits of size 2 and 4 must match with the subgroup of $G_2$ having a fixed point, while the other transitive subgroup of $S_6$ must match with the one having no fixed points.

**2.1. Computing the Gassmann-equivalence class.** When computing any Galois group, the Chebotarev density theorem is a very useful tool. Suppose the Galois group is a subgroup of a group $G$. Then one computes the conjugacy class of $\mathrm{Frob}_p$ for all unramified primes $p \leq X$. This sampled frequency is compared against the conjugacy class distributions of subgroups of $G$, and ideally this pins down the Galois group with high certainty, since Chebotarev guarantees that the distribution of $\mathrm{Frob}_p$ for $p \leq X$ matches that of the Galois group as $X \to \infty$.

This general approach yields the probabilistic method of Algorithm 2.3, wherein we prune out subgroups whose conjugacy class distributions are very unlikely to yield the sampled Frobenius distribution. Since the computation of the Frobenius conjugacy class in $G_3$ is intensive, we do it only when needed. First we focus on two essential features of a conjugacy class in $G_3$: the characteristic polynomial, and the dimension of the 1-eigenspace, which are more efficiently computable. This data is called the signature of the conjugacy class.

**Definition 2.2.** For a prime $p$ of good reduction for $A$, the Frobenius signature of $A$ at $p$ is defined to be the tuple $\langle L_p(A,t) \pmod 3, \dim_{\mathbb{F}_p} A[3](\mathbb{F}_p)\rangle$, where $L_p(A,t)$ is the Euler factor of $A$ at $p$. Note that $\det(I - \overline{\rho}_{A,3}(\mathrm{Frob}_p)t) \equiv L_p(A,t) \pmod 3$.

Although Algorithm 2.3 goes far, it cannot completely determine the mod-3 Galois image because of the existence of non-conjugate but Gassmann-equivalent [**17**, Def 2.8] subgroups, i.e., subgroups giving rise to the same conjugacy class distribution. The 280 eligible subgroups of $G_3$ give rise to 230 distinct conjugacy class distributions. These are 38 pairs, 3 triples and 2 quadruples of Gassmann-equivalent subgroups.

**Algorithm 2.3.** *Input:*

- a genus 2 curve $C$ over $\mathbb{Q}$ such that $A = \mathrm{Jac}(C)$
- a positive real number $\epsilon$ close to 0; two integers $B_1 \geq B_2 \geq 1$.
- a pre-computed list $L$ of the 280 eligible subgroups of $G_3$ along with their signature distributions and conjugacy class distributions.

*Output:* the Gassmann-equivalence class of subgroups of $G_3$ containing $\mathrm{im}(\overline{\rho}_{A,3})$.

**Step 1** For each prime $p \notin S \cup \{3\}, p \leq B_1$, compute the Frobenius signature.

**Step 2** Using the pre-computed list of signature distributions, apply Bayes' rule to calculate for each $H \in L$ the probablity that $\mathrm{im}(\overline{\rho}_{A,3}) = H$ given the sampled Frobenius sign distribution from **Step 1**.

**Step 3** Remove those $H \in L$ whose probability is smaller than $\epsilon$. If the remaining subgroups form a unique Gassmann-equivalence class, return it.

**Step 4** Otherwise, for each prime $p \notin S \cup \{3\}, p \leq B_2$, compute the conjugacy class of $\overline{\rho}_{A,3}(\mathrm{Frob}_p) \in G_3$ by computing $A[3](\overline{\mathbb{F}}_p)$ as a subgroup of $A(\mathbb{F}_{p^k})$ for some $k \geq 1$, and constructing a symplectic basis of $A[3]$.

18 Jun 2025 19:18:56 PDT
250131-Chidambaram Version 4 - Submitted to LuCaNT

**Step 5** Using the pre-computed list of conjugacy class distributions, apply Bayes' rule to calculate for each remaining $H \in L$ the probablity that $\mathrm{im}(\overline{\rho}_{A,3}) = H$ given the sampled Frobenius conjugacy class distribution from **Step 4**.

**Proposition 2.4.** For any $0 < \epsilon < \frac{1}{4}$, there exists $B$ such that Algorithm 2.3 with $B_i \geq B$ returns the Gassmann-equivalence class containing $\mathrm{im}(\overline{\rho}_{A,3})$.

Proof. By the Chebotarev density theorem, the sampled Frobenius distribution converges to the conjugacy class distribution of the Gassmann-equivalence class containing $\mathrm{im}(\overline{\rho}_{A,3})$, as $B_2 \to \infty$. The proposition follows immediately. □

**Example 2.5.** The largest subgroup of $G_3$ that fails the local-global principle for stabilizing a maximal isotropic subspace of $\mathbb{F}_3^4$ is $H = 3.1080.4$, i.e., every element of $H$ stabilizes some 2-dimensional isotropic plane, but $H$ does not. Consider the genus 2 curve with LMFDB label 25600.f.512000.1. Algorithm 2.3 returns that the mod-3 Galois images for this curve is $H$. So the Jacobian of $C$ presents an example where the local-global principle for the existence of isogenies fails.

**Example 2.6.** Let $H$ denote the stabilizer in $G_3$ of an isotropic plane in $\mathbb{F}_3^4$. It is the group 3.40.2, and it has three index-2 subgroups: $H \cap \mathrm{Sp}(4, \mathbb{F}_3)$ and the two eligible subgroups 3.80.3 and 3.80.4. We note that 3.80.3 is the largest subgroup of $G_3$ that does not occur as the mod-3 Galois image for any genus 2 curve in the LMFDB dataset. Consider the moduli space $X/\mathbb{Q}$ parametrizing $(3,3)$-isogenies of principally polarized abelian surfaces (it is the analog of the modular curve $X_0(3)$). In other words, $X$ is the moduli space of abelian surfaces with $\mathrm{im}(\overline{\rho}_{A,3}) \subseteq 3.40.2$. The three index-2 subgroups correspond to three degree-2 covers. If $\mathbb{Q}(X)$ denotes the function field of $X$, the function fields of the three covers are respectively $\mathbb{Q}(\sqrt{-3})(X), \mathbb{Q}(X)(\sqrt{-3f})$ and $\mathbb{Q}(X)(\sqrt{f})$ for some $f \in \mathbb{Q}(X)$. Using a birational model of $X$ and the curves in LMFDB whose mod-3 Galois image is 3.80.4, Noam Elkies guessed the function $f$. Then a search for rational points on $X$ where $-3f$ is a square, yields the genus 2 curve $C : y^2 = -27x^6 + 54x^5 - 693x^4 + 1278x^3 - 543x^2 - 60x - 16$ with conductor $3^2\ 7^4\ 13\ 43^2$. As expected, Algorithm 2.3 verifies that its mod-3 Galois image is indeed 3.80.3.

**Remark 2.7.** The output of Algorithm 2.3 is rigorous only when it is the whole group $G_3$. An effective Chebotarev density theorem [**12**] can be used to make Algorithm 2.3 completely rigorous, if we allow ourselves to use a very large number of primes. Let $\delta$ be the minimum of the $L^\infty$ distance between any two conjugacy class distributions of eligible subgroups of $G_3$. Bounding the error term in Chebotarev density by $\delta/2$ pins down a unique Gassmann-equivalence class. By [**12**, Thm 1.1], which assumes GRH, this can be accomplished if we sample $O_{\mathrm{cond}(C)}(\delta^{-2})$ primes.

**2.2. Distinguishing Gassmann-equivalent subgroups.** We begin by noting a canonical example of non-conjugate Gassmann-equivalent subgroups of $G_\ell$.

**Example 2.8.** Let $J_2 = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$, $\mathcal{J}_2 = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$. Suppose $\mathcal{J}_2' = \begin{bmatrix} & \mathcal{J}_2 \\ -\mathcal{J}_2 & \end{bmatrix}$ represents the standard alternating form on the column space $\mathbb{F}_\ell^4$, that is preserved by $G_\ell$ up to scalars. Let $H_1 \subseteq G_\ell$ be the stabilizer of a vector in $\mathbb{F}_\ell^4$, so $H_1 = \left\{ \begin{bmatrix} 1 & B & c \\ & A & D \\ & & x \end{bmatrix} : D = AJ_2B^t, \det(A) = x \right\}$. Let $H_2 \subseteq G_\ell$ be the transpose of $H_1$.

Then $H_1$ and $H_2$ are clearly non-conjugate, but they are Gassmann-equivalent [17, Prop 2.6] since transposing gives a $G_\ell$-conjugacy preserving bijection $H_1 \leftrightarrow H_2$.

In [16], while computing the mod-$\ell$ Galois image $\operatorname{im}(\overline{\rho}_{E,\ell})$ of an elliptic curve $E/\mathbb{Q}$, Sutherland tackles this problem of distinguishing Gassmann-equivalent subgroups of $\mathrm{GL}(2, \mathbb{F}_\ell)$ by computing the degree of the minimal number field over which $E$ acquires $\ell$-torsion points. For example, if $\operatorname{im}(\overline{\rho}_{E,\ell}) = \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}$, then $E(\mathbb{Q})$ must have an $\ell$-torsion point, whereas if $\operatorname{im}(\overline{\rho}_{E,\ell}) = \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$, then the minimal degree of a number field $K$ such that $E(K)$ has an $\ell$-torsion point is $\ell - 1$.

We develop this idea further in Algorithm 2.9 to distinguish any two Gassmann-equivalent subgroups of $G_3$ that are not conjugate in $\mathrm{GL}(4, \mathbb{F}_3)$. There are exactly 5 Gassmann-equivalence classes of size 2, listed in Table 1, containing $\mathrm{GL}(4, \mathbb{F}_3)$-conjugate subgroups. These are indistinguishable by the methods described above. Since these groups are small (order $\leq 32$), we distinguish them in Algorithm 2.9 by literally constructing a symplectic basis of $A[3]$ over the 3-torsion field $K$.

TABLE 1. Non-conjugate Gassmann-equivalent subgroups of $\mathrm{GSp}(4, \mathbb{F}_3)$ that are conjugate in $\mathrm{GL}(4, \mathbb{F}_3)$.

| $\lvert H\rvert$ | Label | Entries in generators read horizontally |
|---|---|---|
| 32 | 3.3240.6 | [ 0, 0, 1, 2, 2, 2, 0, 1, 1, 1, 1, 0, 2, 1, 1, 0 ] |
| | | [ 2, 1, 0, 1, 2, 2, 0, 1, 1, 1, 2, 1, 2, 1, 1, 0 ] |
| | | [ 1, 1, 2, 1, 2, 0, 0, 2, 1, 2, 0, 2, 2, 1, 1, 2 ] |
| 32 | 3.3240.7 | [ 2, 0, 0, 0, 1, 0, 2, 0, 2, 2, 0, 0, 1, 2, 2, 1 ] |
| | | [ 1, 0, 2, 1, 0, 1, 1, 2, 0, 0, 2, 0, 0, 0, 0, 2 ] |
| | | [ 2, 1, 2, 0, 2, 2, 0, 2, 1, 1, 1, 2, 2, 1, 1, 1 ] |
| 16 | 3.6480.16 | [ 2, 0, 0, 1, 0, 1, 0, 0, 0, 1, 2, 0, 0, 0, 0, 1 ] |
| | | [ 0, 2, 1, 0, 1, 2, 1, 1, 2, 0, 0, 1, 1, 2, 2, 2 ] |
| 16 | 3.6480.3 | [ 0, 2, 1, 0, 2, 1, 2, 1, 1, 1, 2, 1, 2, 1, 1, 0 ] |
| | | [ 2, 2, 1, 0, 0, 1, 1, 1, 0, 0, 2, 1, 0, 0, 0, 1 ] |
| 16 | 3.6480.13 | [ 1, 2, 1, 0, 1, 1, 0, 1, 2, 2, 2, 1, 1, 2, 2, 2 ] |
| | | [ 1, 0, 2, 1, 0, 1, 1, 2, 0, 0, 2, 0, 0, 0, 0, 2 ] |
| 16 | 3.6480.17 | [ 0, 1, 2, 2, 2, 2, 2, 2, 1, 1, 1, 2, 0, 1, 1, 0 ] |
| | | [ 2, 0, 2, 1, 2, 1, 2, 2, 1, 1, 2, 0, 2, 1, 1, 1 ] |
| 16 | 3.6480.14 | [ 2, 1, 0, 1, 0, 2, 0, 0, 2, 2, 1, 2, 0, 2, 0, 1 ] |
| | | [ 2, 0, 1, 2, 2, 1, 2, 1, 0, 0, 2, 0, 0, 0, 1, 1 ] |
| | | [ 1, 1, 1, 0, 2, 2, 0, 2, 2, 0, 2, 1, 0, 1, 2, 1 ] |
| 16 | 3.6480.15 | [ 1, 2, 0, 2, 0, 1, 0, 0, 1, 1, 2, 1, 0, 1, 0, 2 ] |
| | | [ 2, 0, 1, 2, 1, 0, 0, 1, 2, 2, 0, 0, 1, 2, 2, 1 ] |
| | | [ 2, 0, 1, 1, 1, 1, 1, 1, 2, 1, 2, 0, 1, 2, 2, 1 ] |
| 8 | 3.12960.5 | [ 2, 0, 0, 1, 0, 1, 0, 0, 0, 1, 2, 0, 0, 0, 0, 1 ] |
| | | [ 1, 0, 2, 1, 2, 0, 0, 2, 1, 1, 0, 0, 2, 1, 1, 2 ] |
| 8 | 3.12960.11 | [ 2, 2, 1, 0, 1, 1, 1, 1, 2, 0, 2, 1, 1, 2, 2, 1 ] |
| | | [ 0, 2, 1, 1, 1, 1, 1, 1, 2, 2, 2, 1, 0, 2, 2, 0 ] |

We set up some notation before describing the algorithm. Let $\mathcal{K} = A/\{\pm\}$ denote the Kummer surface associated to the abelian surface $A$, and let $\mathcal{X}$ denote

18 Jun 2025 19:18:56 PDT
250131-Chidambaram Version 4 - Submitted to LuCaNT

the image of $A[3]$ under the quotient map. Explicit biquadratic forms defining addition on $\mathcal{K}$, and the doubling formula, have been computed in [**8**, Thm 3.4.1]. Using these, equations for the 3-torsion locus $\mathcal{X} \subset \mathcal{K}$ can be computed, as in [**7**], by writing $2P = -P$ in terms of the coordinates of an arbitrary point $P \in \mathcal{K}$. Although one can obtain a 3-division polynomial by taking resultants of these equations succesively, knowing a general 3-division polynomial at the outset is very useful to make **Step 1** and **Step 3** of Algorithm 2.9 faster. Such a general 3-division polynomial was given to us by David Roberts.

**Algorithm 2.9.** *Input:*

- a genus 2 curve $C$ over $\mathbb{Q}$ such that $A = \mathrm{Jac}(C)$
- a Gassmann-equivalence class $L$ of subgroups of $G_3$ containing $\mathrm{im}(\overline{\rho}_{A,3})$.

*Output:* the image of $\overline{\rho}_{A,3}$ up to conjugacy in $G_3$.

**Step 1** If $L$ is a class given in Table 1, compute the three-torsion field $K = \mathbb{Q}(A[3])$ and its automorphism group $\mathrm{Gal}(K|\mathbb{Q})$. Find all 40 geometric points on the three-torsion locus $\mathcal{X}$, i.e., compute $\mathcal{X}(\overline{\mathbb{Q}}) = \mathcal{X}(K)$, and lift to find a full basis of $A[3]$. Fix a symplectic basis by working in some residue field. Compute matrices with respect to this basis that correspond to the action of the generators of $\mathrm{Gal}(K|\mathbb{Q})$, thus determining $\mathrm{im}(\overline{\rho})$.

**Step 2** Otherwise, for each $H \in L$, compute $\dim(\mathbb{F}_3^4)^{H_0}$ where $H_0 = H \cap \mathrm{Sp}(4, \mathbb{F}_3)$. Also compute $\max\limits_{[H:H_1]=d} \dim(\mathbb{F}_3^4)^{H_1}$ for each $d \in D = \{1, 2, 3, 6, 8, 12\}$.

**Step 3** Compute $\mathcal{X}(\mathbb{Q}(\zeta_3))$, and the points in $\mathcal{X}$ whose degree belongs to the set $D$. Lift them to 3-torsion points on $A$, and thus compute $\dim_{\mathbb{F}_3}(A[3](\mathbb{Q}(\zeta_3)))$, and $\max\limits_{[K:\mathbb{Q}]=d} \dim_{\mathbb{F}_3}(A[3](K))$ for each $d \in D$.

**Step 4** If there is a unique group $H \in L$, whose data computed in **Step 2** matches the data computed in **Step 3**, return it.

THEOREM 2.10. *Given any genus 2 curve $C/\mathbb{Q}$ with $A = \mathrm{Jac}(C)$, and the Gassmann-equivalence class $L$ containing $\mathrm{im}(\overline{\rho}_{A,3})$, Algorithm 2.9 returns $\mathrm{im}(\overline{\rho}_{A,3})$.*

PROOF. Suppose $L$ is a Gassmann-equivalence class of size $> 1$ not listed in Table 1. If $L$ appears in Tables 2 or 3, the corresponding set of indices $d$ shown in the table distinguish all subgroups appearing in $L$. Otherwise, the subgroups in $L$ are distinguished by the dimension of their fixed spaces. □

**Example 2.11.** Let $H$ denote the stabilizer in $G_3$ of an line in $\mathbb{F}_3^4$. It is the group 3.40.1, and two of its index-2 subgroups $\{$3.80.1, 3.80.2$\}$ form a Gassmann-equivalence class. While 3.80.1 is the stabilizer of a point, 3.80.2 acts trivially on a 1-dimensional quotient of $\mathbb{F}_3^4$. Consider the genus 2 curve $C$ with LMFDB label 277.a.277.2. Running Algorithm 2.3 on $C$ returns the correct Gassmann-equivalence class. Further running Algorithm 2.9 returns that the mod-3 Galois image is the group 3.80.2. So the local-global principle for the existence of a 3-torsion point fails for $\mathrm{Jac}(C)$. This is consistent with Mordell-Weil group $\mathrm{Jac}(C)(\mathbb{Q}) \simeq \mathbb{Z}/5$.

## 3. Challenges in computing mod-$\ell$ Galois image for $\ell > 3$

For any prime $\ell > 3$, Algorithm 2.3 still works in principle to determine the Gassmann-equivalence class of $\mathrm{im}(\overline{\rho}_{A,\ell})$. The precomputation of all eligible subgroups of $G_\ell$ becomes hard for large $\ell$, but for practical purposes, it is enough to compute only those subgroups whose index is less than a well-chosen bound.

TABLE 2. Gassmann-equivalent subgroups distinguished by $\dim(\mathbb{F}_3^4)^{H_0}$ and $\max\limits_{[H:H_1]=d} \dim(\mathbb{F}_3^4)^{H_1}$ for $d \leq 3$.

| $\|H\|$ | Label | Entries in generators read horizontally | $H_0$ | d=1 | 2 | 3 |
|---|---|---|---|---|---|---|
| 324 | 3.320.1 | [ 2, 2, 2, 0, 2, 1, 1, 0, 2, 0, 1, 2, 2, 0, 2, 2 ] | 1 | 1 | 1 | 1 |
| | | [ 1, 0, 2, 0, 2, 1, 1, 2, 2, 2, 0, 1, 2, 1, 0, 1 ] | | | | |
| | 3.320.2 | [ 1, 1, 1, 2, 0, 0, 2, 1, 2, 0, 0, 1, 1, 1, 2, 2 ] | 1 | 0 | 1 | 0 |
| | | [ 0, 1, 0, 1, 2, 1, 2, 1, 1, 2, 1, 0, 0, 2, 2, 1 ] | | | | |
| | 3.320.5 | [ 1, 2, 1, 1, 0, 1, 2, 0, 0, 0, 2, 2, 0, 0, 0, 2 ] | 0 | 0 | 1 | 1 |
| | | [ 2, 2, 0, 0, 2, 1, 2, 1, 0, 0, 1, 2, 1, 1, 2, 2 ] | | | | |
| | 3.320.6 | [ 1, 2, 1, 1, 1, 0, 2, 0, 0, 2, 1, 0, 2, 2, 1, 1 ] | 0 | 0 | 1 | 0 |
| | | [ 1, 0, 2, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 2, 1 ] | | | | |
| 162 | 3.640.1 | [ 2, 2, 0, 0, 2, 0, 1, 2, 0, 2, 0, 0, 1, 2, 0, 2 ] | 1 | 1 | 1 | 2 |
| | | [ 0, 0, 1, 2, 1, 1, 0, 1, 0, 0, 2, 0, 2, 0, 2, 0 ] | | | | |
| | 3.640.2 | [ 0, 1, 0, 1, 0, 1, 0, 2, 2, 2, 2, 1, 1, 1, 2, 1 ] | 1 | 1 | 1 | 1 |
| | | [ 1, 1, 1, 0, 0, 0, 2, 1, 0, 1, 2, 2, 0, 0, 0, 1 ] | | | | |
| | | [ 2, 2, 2, 1, 0, 0, 1, 2, 0, 1, 0, 1, 0, 0, 0, 1 ] | | | | |
| | 3.640.3 | [ 2, 2, 0, 2, 1, 1, 1, 0, 1, 2, 1, 0, 1, 2, 0, 2 ] | 1 | 0 | 1 | 0 |
| | | [ 2, 2, 0, 2, 0, 2, 1, 2, 1, 2, 1, 0, 2, 0, 2, 2 ] | | | | |
| | 3.640.4 | [ 0, 0, 2, 2, 0, 0, 2, 1, 2, 1, 1, 2, 1, 1, 2, 2 ] | 1 | 0 | 1 | 1 |
| | | [ 2, 1, 2, 1, 2, 2, 0, 0, 0, 1, 2, 0, 1, 1, 2, 1 ] | | | | |
| | | [ 2, 1, 2, 2, 2, 2, 0, 1, 0, 0, 1, 1, 1, 2, 0, 2 ] | | | | |
| 36 | 3.2880.13 | [ 0, 0, 1, 2, 2, 2, 2, 1, 1, 1, 1, 0, 0, 1, 1, 0 ] | 0 | 0 | 2 | 0 |
| | | [ 2, 0, 0, 0, 0, 2, 0, 0, 1, 1, 1, 0, 2, 1, 0, 1 ] | | | | |
| | | [ 2, 1, 1, 1, 2, 2, 2, 1, 2, 1, 2, 2, 2, 2, 1, 2 ] | | | | |
| | 3.2880.17 | [ 1, 2, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 2, 0, 2, 0 ] | 0 | 0 | 1 | 0 |
| | | [ 0, 1, 0, 2, 1, 2, 2, 0, 0, 2, 0, 2, 2, 0, 2, 2 ] | | | | |
| | | [ 2, 2, 0, 2, 2, 1, 2, 0, 0, 1, 2, 1, 1, 0, 1, 1 ] | | | | |
| 18 | 3.5760.2 | [ 1, 1, 1, 2, 0, 0, 2, 1, 0, 2, 0, 2, 0, 0, 0, 2 ] | 2 | 1 | 2 | 2 |
| | | [ 2, 1, 2, 0, 0, 0, 2, 2, 1, 0, 2, 2, 2, 1, 0, 0 ] | | | | |
| | 3.5760.5 | [ 2, 1, 2, 0, 0, 0, 2, 2, 1, 0, 2, 2, 2, 1, 0, 0 ] | 2 | 1 | 2 | 1 |
| | | [ 1, 2, 1, 2, 1, 0, 2, 1, 0, 1, 0, 1, 2, 0, 2, 2 ] | | | | |
| 12 | 3.8640.2 | [ 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 2, 0, 2, 1, 0, 2 ] | 0 | 0 | 2 | 0 |
| | | [ 1, 2, 2, 0, 2, 2, 1, 2, 2, 1, 2, 1, 0, 2, 1, 0 ] | | | | |
| | 3.8640.4 | [ 0, 2, 1, 1, 1, 0, 2, 1, 1, 2, 0, 1, 1, 1, 2, 0 ] | 0 | 0 | 1 | 0 |
| | | [ 2, 1, 0, 0, 0, 1, 0, 0, 0, 0, 2, 2, 0, 0, 0, 1 ] | | | | |
| 12 | 3.8640.12 | [ 1, 1, 0, 0, 0, 2, 0, 0, 2, 0, 1, 2, 1, 2, 0, 2 ] | 0 | 0 | 2 | 0 |
| | | [ 2, 0, 1, 1, 0, 2, 1, 1, 2, 1, 1, 0, 1, 2, 0, 1 ] | | | | |
| | 3.8640.13 | [ 2, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 2, 2, 1, 0, 2 ] | 0 | 0 | 1 | 0 |
| | | [ 2, 0, 2, 1, 2, 1, 0, 2, 0, 0, 2, 0, 0, 0, 1, 1 ] | | | | |

But the problem of distinguishing Gassmann-equivalent subgroups gets considerably harder. Firstly, there are many more Gassmann-equivalent subgroups. For example, $G_5$ has 1125 eligible subgroups up to conjugacy, but they give rise to only 773 distinct conjugacy class distributions. Hence many more Gassmann-equivalent subgroups show up than for $\ell = 3$. Secondly, computing information about $A[\ell]$ as in **Step 3** of Algorithm 2.9 is a lot more computationally challenging. For eg.,

Table 3. Gassmann-equivalent subgroups distinguished by $\max\limits_{[H:H_1]=d} \dim(\mathbb{F}_3^4)^{H_1}$ for $d = 6, 8, 12$.

| $\lvert H\rvert$ | Label | Entries in generators read horizontally | d=6 | 8 | 12 |
|---|---|---|---|---|---|
| 432 | 3.240.6 | [ 0, 0, 0, 2, 0, 1, 2, 2, 0, 0, 2, 0, 2, 0, 1, 0 ] | 0 | 1 | 0 |
| | | [ 1, 0, 0, 2, 0, 2, 1, 0, 0, 0, 2, 0, 2, 0, 0, 2 ] | | | |
| | 3.240.7 | [ 2, 0, 1, 1, 0, 1, 1, 2, 0, 0, 2, 0, 2, 0, 1, 2 ] | 0 | 1 | 1 |
| | | [ 0, 0, 2, 2, 1, 2, 0, 2, 0, 0, 1, 0, 2, 0, 2, 0 ] | | | |
| 324 | 3.320.3 | [ 1, 1, 0, 2, 1, 0, 2, 0, 0, 2, 1, 2, 2, 0, 2, 0 ] | 2 | - | 2 |
| | | [ 2, 0, 0, 1, 2, 1, 1, 1, 0, 1, 0, 0, 1, 2, 0, 0 ] | | | |
| | 3.320.4 | [ 1, 2, 2, 1, 2, 1, 2, 0, 2, 0, 0, 2, 2, 0, 2, 2 ] | 1 | - | 2 |
| | | [ 1, 1, 1, 2, 2, 1, 2, 0, 2, 0, 0, 1, 2, 1, 0, 1 ] | | | |
| | | [ 2, 1, 1, 1, 1, 2, 1, 1, 1, 1, 1, 2, 1, 1, 2, 1 ] | | | |
| 48 | 3.2160.9 | [ 1, 1, 1, 1, 0, 2, 1, 1, 0, 0, 1, 2, 0, 0, 0, 2 ] | 1 | 1 | 2 |
| | | [ 0, 2, 0, 1, 2, 1, 1, 0, 2, 0, 1, 0, 2, 1, 0, 2 ] | | | |
| | 3.2160.10 | [ 0, 2, 1, 0, 1, 0, 0, 1, 0, 1, 2, 2, 2, 1, 0, 2 ] | 1 | 2 | 2 |
| | | [ 2, 2, 2, 0, 0, 2, 0, 2, 1, 0, 0, 0, 2, 0, 2, 0 ] | | | |

computing equations for the $\ell$-torsion locus on the Kummer surface seems hard already for $\ell = 7$. Thirdly, while most Gassmann-equivalent subgroups of $G_\ell$ are not conjugate inside $\mathrm{GL}(4, \mathbb{F}_\ell)$, there are also fairly big subgroups that are. Concretely, there is a pair of subgroups $\{$5.48750.5, 5.48750.6$\}$ of $G_5$ of order 768, which are Gassmann-equivalent and also conjugate in $\mathrm{GL}(4, \mathbb{F}_5)$.

We believe that a lot of these difficulties can be overcome by taking endomorphism ring information into account. This data can be easily computed thanks to [**10**]. On the one hand, endomorphisms constrain Galois action, thus there are fewer candidates for the Galois image. On the other hand, for a given endomorphism ring, having an unusually small Galois image is rare. A forthcoming work of the author will fully address the typical case, i.e., when there are no extra endomorphisms.

## 4. Towards explicitly realizing all mod-3 Galois images

As mentioned in the introduction, [**5**] yields in theory a way to explicitly realize any of the 280 eligible subgroups $H$ of $G_3$ as the Galois image of the Jacobian of a genus 2 curve over $\mathbb{Q}$. Given such a subgroup, one first obtains a number field $K$ properly solving the embedding problem

$$\begin{tikzcd} & & & G_{\mathbb{Q}} \arrow[dl, dashed, "\overline{\rho}"'] \arrow[d, "\chi_3"] & \\ 0 \arrow[r] & H \cap \mathrm{Sp}(4, \mathbb{F}_3) \arrow[r] & H \arrow[r] & \mathbb{Z}/2 \arrow[r] & 0 \end{tikzcd} \tag{4.1}$$

i.e., $\overline{\rho}$ is surjective and $K$ is the fixed field of $\ker(\overline{\rho})$. Since $G_3$ is a split extension of $\mathbb{Z}/2$ by $\mathrm{Sp}(4, \mathbb{F}_3)$, this embedding problem is always solvable and such a number field $K$ exists. Then the recipe in [**5**] lets us construct the corresponding twisted Burkhardt quartic threefold $B$, and associate to the rational points on $B$ certain genus 2 curves. Finally, we make a suitable quadratic twist to ensure that the mod-3 Galois image of the Jacobian is exactly equal to $H$. Here is an illustrative example.

**Example 4.1.** Consider the subgroup $H$ with label 3.12960.9 which is abstractly isomorphic to $(\mathbb{Z}/2)^3$. We take $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-1}, \sqrt{2})$. We call the intrinsic `BurkhardtModel` with input containing $K$ and an isomorphism of $\overline{\rho} : \mathrm{Gal}(K|\mathbb{Q}) \simeq H$ to find a model for the corresponding twisted Burkhardt quartic $B$. We then follow the recipe in [**5**] with a randomly chosen rational point on $B$. This produces the quadratic twist by 2 of the curve $C : y^2 = x(x^4 - 6840x^2 + 456976)$, and indeed Algorithm 2.3 verifies that its mod-3 Galois image is $H$. The Jacobian of $C$ is isogenous to the product of the elliptic curve 14.a3 and its twist by $-1$. It has conductor $2^5 7^2 = 1568$, mod-3 Galois image 3.25920.3 and 3-torsion field $\mathbb{Q}(\sqrt{-1}, \sqrt{3})$. The curve $C$ is not currently on the LMFDB.

## 5. Acknowledgement

The author was supported by Simons Foundation grant 550033. I thank Andrew Sutherland for suggesting the project. I am also grateful to him, David Roberts and Nils Bruin for helpful discussions, and David Roe and Edgar Costa for their support in incorporating the data into LMFDB. I thank Noam Elkies for Example 2.6. I also extend my gratitude to the referees whose inputs greatly improved the article, and simplified Example 4.1.

## References

1. *Labelling subgroups of GSp(4,ℓ)*, `https://www.lmfdb.org/knowledge/show/g2c.galois_rep_modell_image`, 2025, [Online; accessed 18 June 2025].
2. Barinder S. Banwait, Armand Brumer, Hyun Jong Kim, Zev Klagsbrun, Jacob Mayle, Padmavathi Srinivasan, and Isabel Vogt, *Computing nonsurjective primes associated to Galois representations of genus* 2 *curves*, LuCaNT: LMFDB, computation, and number theory, Contemp. Math., vol. 796, Amer. Math. Soc., [Providence], RI, [2024] ©2024, pp. 129–163. MR 4732686
3. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
4. George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni, *Abelian surfaces over totally real fields are potentially modular*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), 153–501. MR 4349242
5. Nils Bruin and Eugene Filatov, *Twists of the Burkhardt quartic threefold*, Res. Number Theory **8** (2022), no. 4, Paper No. 73, 16. MR 4487859
6. Frank Calegari and Shiva Chidambaram, *Rationality of twists of the Siegel modular variety of genus 2 and level 3*, Proc. Amer. Math. Soc. **150** (2022), no. 5, 1975–1984. MR 4392333
7. Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza, *Some modular abelian surfaces*, Math. Comp. **89** (2020), no. 321, 387–394. MR 4011548
8. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1996.
9. Shiva Chidambaram, *Mod3Image*.
10. Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), no. 317, 1303–1339. MR 3904148
11. Luis V. Dieulefait, *Explicit determination of the images of the Galois representations attached to abelian surfaces with* $\mathrm{End}(A) = \mathbb{Z}$, Experiment. Math. **11** (2002), no. 4, 503–512. MR 1969642
12. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London-New York, 1977, pp. 409–464. MR 447191
13. The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2024, [Online; accessed 18 June 2025].
14. Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$ *(and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63, With an appendix with John Voight. MR 4468989

15. Jeremy Rouse and David Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34. MR 3500996
16. Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. MR 3482279
17. ______, *Stronger arithmetic equivalence*, Discrete Anal. (2021), Paper No. 23, 23. MR 4341956
18. Raymond van Bommel, Shiva Chidambaram, Edgar Costa, and Jean Kieffer, *Computing isogeny classes of typical principally polarized abelian surfaces over the rationals*, LuCaNT: LMFDB, computation, and number theory, Contemp. Math., vol. 796, Amer. Math. Soc., [Providence], RI, [2024] ©2024, pp. 187–214. MR 4732688
19. David Zywina, *Explicit open images for elliptic curves over* $\mathbb{Q}$, 2022.

Department of Mathematics, University of Wisconsin-Madison, Madison WI 53706-1325, USA
*Email address*: chidambaram3@wisc.edu