PROBABLISTIC DETERMINATION OF MOD-3 GALOIS IMAGES OF ABELIAN SURFACES OVER THE RATIONALS

SHIVA CHIDAMBARAM

ABSTRACT. There has been considerable work around computing 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 an 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 ℓ, 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 knowledge of the endomorphism ring.

1. INTRODUCTION

Given an elliptic curve $E/\mathbb{Q}$, the problem of understanding the Galois action on its ℓ-torsion points for a prime ℓ is fundamental. This leads to the concrete question of determining the image of the associated mod-ℓ Galois representation $\overline{\rho}_{E,\ell} : G_\mathbb{Q} \to \mathrm{GL}(2,\mathbb{F}_\ell)$ upto conjugacy in $\mathrm{GL}(2,\mathbb{F}_\ell)$. There are efficient algorithms [Sut16] accomplishing this task. Moreover, when E does not have complex multiplication, the works [RSZ22; RZ15] present algorithms to compute the ℓ-adic Galois image, and Zywina goes further and computes the full adelic Galois image [Zyw22].

A natural next step is to tackle this problem for an abelian surface $A/\mathbb{Q}$. For any prime ℓ, let $G_\ell = \mathrm{GSp}(4,\mathbb{F}_\ell)$. The ℓ-torsion subgroup $A[\ell]$ is a 4-dimensional vector space over $\mathbb{F}_\ell$, having a non-degenerate alternating pairing – the Weil pairing. Thus the Galois action gives rise to a mod-ℓ Galois representation $\overline{\rho} := \overline{\rho}_{A,\ell} : G_\mathbb{Q} \to G_\ell$. Furthermore, the Galois action is equivariant with respect to the Weil pairing. So the composition of the similitude character $\chi_{\mathrm{sim}} : G_\ell \to \mathbb{F}_\ell^\times$ with $\overline{\rho}$ is equal to the mod-ℓ cyclotomic character χ_ℓ. Given $A/\mathbb{Q}$ and a prime ℓ, it is desirable to determine the mod-ℓ Galois image $\overline{\rho}_{A,\ell}(G_\mathbb{Q})$ upto conjugacy inside G_ℓ. We provide a probablistic algorithm to completely accomplish this task when $\ell = 3$. It works for all abelian surfaces without any restriction on endomorphism type. Magma code implementing the algorithm is available at the Github repository [Chi]. The mod-3 Galois images data for genus 2 curves in LMFDB was computed using this algorithm. We have also computed these images for a bigger dataset consisting of 487 493 genus 2 curves with 5-smooth conductors.

Any representation $\overline{\rho} : G_\mathbb{Q} \to G_3$ with $\chi_{\mathrm{sim}} \circ \overline{\rho} = \chi_3$ is known to arise as the mod-3 Galois representation of infinitely many abelian surfaces over $\mathbb{Q}$ [BCGP21]. This is proven by showing that the corresponding twist of the Siegel modular variety $\mathcal{A}_2(3)$, which may not be rational over $\mathbb{Q}$ [CC22], is nevertheless unirational over $\mathbb{Q}$

2020 *Mathematics Subject Classification.* 11F80; 11G10.
Key words: Galois image, abelian surface, Gassmann equivalence

via a map of degree at most 6. A consequence of this result is that any subgroup of G_3 that has an order-2 element $g \notin \mathrm{Sp}(4, \mathbb{F}_3)$ arises as the mod-3 Galois image of some abelian surface over $\mathbb{Q}$. We note that the total number of subgroups of G_3 upto conjugacy is 492, and 330 of them are not contained in $\mathrm{Sp}(4, \mathbb{F}_3)$, while 280 of these subgroups satisfy the condition from above. This leads to the following question.

Question 1.1. *Can we explicitly realize all the* 280 *possible subgroups of* G_3 *as mod-*3 *Galois images of some abelian surfaces 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 [BF22] 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.

2. Algorithms

Suppose A is given as the Jacobian of a genus 2 curve $C/Q : y^2 = f(x)$ with $\deg(f) = 5$ or 6. This section outlines the ingredients for an algorithm to compute the mod-ℓ Galois image of A.

2.1. $\ell = 2$**.** The 2-torsion field of A is exactly the splitting field of $f(x)$. So the mod-2 Galois image can be computed as the Galois group of $f(x)$. The latter is a subgroup of S_6, and S_6 is isomorphic to G_2. But some care is needed since S_6 has an outer automorphism. We choose the right identification $S_6 \simeq G_2$ by considering the conjugacy classes of order-48 subgroups of S_6. There are two: one of them has orbits of size 2 and 4, while the other is transitive. The first one must be identified with the order-48 subgroup of G_2 having a fixed point, while the second one must correspond to the other subgroup that does not have a fixed point. This is because pairs of Weierstrass points on C correspond to 2-torsion points on A.

2.2. $\ell = 3$**.** When computing any Galois group, Chebotarev density theorem is a very useful tool. Suppose it is known apriori that the Galois group is contained in a given group G. Then one computes the Frobenius conjugacy class for unramified primes p upto a chosen bound. This sampled frequency is compared against the conjugacy class distributions of subgroups of G, and in an ideal scenario, this probablistic algorithm determines the group.

We follow the probablistic approach outlined above by computing the conjugacy class of the Frobenius matrix for the first 500 primes, and subsequently computing it for more primes as needed. While this approach goes far, it cannot completely determine the mod-3 Galois image because of the existence of non-conjugate subgroups of G giving rise to the same conjugacy class distribution. We call such subgroups Gassmann-equivalent. The 280 possible subgroups of G give rise to 230 distinct conjugacy class distributions. These are 38 pairs, 3 triples and 2 quadruples of Gassmann-equivalent subgroups.

We note that this phenomenon is already encountered in [Sut16] when computing the mod-ℓ Galois images of elliptic curves. Concretely, the two non-conjugate subgroups

$$H_1 = \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}, \qquad H_2 \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$$

of $\mathrm{GL}(2, \mathbb{F}_\ell)$ are Gassmann-equivalent. Such subgroups are distinguished in [Sut16] using the degrees of the minimal number fields over which the elliptic curves acquire rational ℓ-torsion points.

Most of the Gassmann-equivalent subgroups we find are already non-conjugate inside $\mathrm{GL}(4, \mathbb{F}_3)$. So the idea from [Sut16] is also expected to be very useful here. In fact, most of these subgroups can be distinguished simply by computing the rational 3-torsion subgroup $A[3](\mathbb{Q})$. We also compute $A[3](\mathbb{Q}(\zeta_3))$ and the maximum size of 3-torsion defined over number fields of small degrees. This distinguishes all remaining Gassmann-equivalent subgroups that are non-conjugate inside $\mathrm{GL}(4, \mathbb{F}_3)$. Table 1 gives the number field degrees used to distinguish these subgroups. A key ingredient for these calculations is the set of bilinear forms defining addition on the Kummer surface $\mathcal{K} = A/\{\pm\}$, which were computed in [CF96]. We use them to cut out the 3-torsion locus on $\mathcal{K}$ as explained in [CCG20]. Concretely, this is done by writing $2P = -P$ in terms of the Kummer coordinates of an arbitrary point $P \in A$. Now we can compute small degree points on this locus. Alternatively, we can use a 3-division polynomial to identify the number fields K of a specific degree d contained in the 3-division field, and compute K-points on this locus. We use a general 3-division polynomial given to us by David Roberts.

There are 5 pairs of subgroups that are both Gassmann-equivalent and $\mathrm{GL}(4, \mathbb{F}_3)$-conjugate: {`3.3240.6`, `3.3240.7`}, {`3.6480.13`, `3.6480.17`}, {`3.6480.3`, `3.6480.16`}, {`3.6480.14`, `3.6480.15`}, {`3.12960.5`, `3.12960.11`}. Since these groups are small (order ≤ 32), we distinguish them by literally constructing a symplectic basis of $A[3]$ over the 3-division field K.

2.3. $\ell > 3$**.** For any prime $\ell > 3$, the probablistic approach of sampling Frobenius matrices and comparing against the conjugacy class distributions of subgroups of G_ℓ is still available. But the problem of distinguishing Gassmann-equivalent subgroups gets considerably harder. Firstly, there are many more Gassmann-equivalent subgroups. Secondly, distinguishing all of them requires computing much more information about $A[\ell]$, which becomes computationally challenging.

For example, suppose $\ell = 5$. There are 1278 subgroups of G_5 upto conjugacy, such that the similitude character restricted to them is surjective. Out of these, 1125 possess an order 2 element with similitude -1. Since complex conjugation is such an element, these are exactly the candidates for the mod-5 Galois image of an abelian surface $A/\mathbb{Q}$. They give rise to only 773 distinct conjugacy class distributions. Hence many more Gassmann-equivalent subgroups show up than for $\ell = 3$. While most of them are not conjugate inside $\mathrm{GL}(4, \mathbb{F}_5)$, there are also fairly big subgroups that are. Specifically, there is a pair of Gassmann-equivalent $\mathrm{GL}(4, \mathbb{F}_5)$-conjugate subgroups `5.48750.5`, `5.48750.6` of order 768.

We believe that a lot of these difficulties can be overcome by taking endomorphism ring information into account. Endomorphisms constrain the Galois action, thus there are fewer candidates for the Galois image. Furthermore, with a fixed endomorphism ring, encountering an abelian surface with an unusually small Galois image also becomes rare.

3. Towards explicitly realizing all mod-3 Galois images

As mentioned in the introduction, [BF22] yields in principle a way to explicitly realize any of the 280 possible subgroups H of G_3 as the Galois image of an abelian

Table 1. Maximum dimension of subspace of $\mathbb{F}_3^4$ fixed by an index-d subgroup of H, and by $H \cap \mathrm{Sp}(4, \mathbb{F}_3)$.

Label	Generators of H	$H \cap \mathrm{Sp}(4, \mathbb{F}_3)$	d=1	2	3	6	8	12
3.320.1	[2, 2, 2, 0, 2, 1, 1, 0, 2, 0, 1, 2, 2, 0, 2, 2]	1	1	1	1	2	0	2
	[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	1	0	2
	[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	0	2
	[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, 0, 2, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 2, 1]							
3.640.1	[2, 2, 0, 0, 2, 0, 1, 2, 0, 2, 0, 0, 1, 2, 0, 2]	1	1	1	2	2	0	0
	[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	2	0	0
	[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	0	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	0	0
	[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]							
3.240.6	[0, 0, 0, 2, 0, 1, 2, 2, 0, 0, 2, 0, 2, 0, 1, 0]	0	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	0	1	0	0	1	1
	[0, 0, 2, 2, 1, 2, 0, 2, 0, 0, 1, 0, 2, 0, 2, 0]							
3.320.3	[1, 1, 0, 2, 1, 0, 2, 0, 0, 2, 1, 2, 2, 0, 2, 0]	0	0	1	0	2	0	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]	0	0	1	0	1	0	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]							
3.2160.9	[1, 1, 1, 1, 0, 2, 1, 1, 0, 0, 1, 2, 0, 0, 0, 2]	0	0	1	0	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]	0	0	1	0	1	2	2
	[2, 2, 2, 0, 0, 2, 0, 2, 1, 0, 0, 0, 2, 0, 2, 0]							
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	3
	[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	2	0	3
	[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]							
3.5760.2	[1, 1, 1, 2, 0, 0, 2, 1, 0, 2, 0, 2, 0, 0, 0, 2]	2	1	2	2	3	0	0
	[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	3	0	0
	[1, 2, 1, 2, 1, 0, 2, 1, 0, 1, 0, 1, 2, 0, 2, 2]							
3.8640.2	[1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 2, 0, 2, 1, 0, 2]	0	0	2	0	2	0	4
	[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	0	4
	[2, 1, 0, 0, 0, 1, 0, 0, 0, 0, 2, 2, 0, 0, 0, 1]							
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	4
	[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	4
	[2, 0, 2, 1, 2, 1, 0, 2, 0, 0, 2, 0, 0, 0, 1, 1]							

surface over $\mathbb{Q}$. Given such a subgroup, one first obtains a number field K properly solving the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & \overset{\overline{\rho}}{\swarrow} & \downarrow \chi_3 & & \\ 0 & \longrightarrow & H \cap \mathrm{Sp}(4,\mathbb{F}_3) & \longrightarrow & H & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 0 \end{array} \tag{3.1}$$

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 [BF22] lets us construct the corresponding twisted Burkhardt quartic threefold B, and associate to rational points on B certain genus 2 curves. Finally, we make a suitable quadratic twist to get curves whose Jacobians have mod-3 Galois image exactly equal to H. The following example was constructed by following this recipe.

Example 1. Consider the subgroup $H =$ `3.12960.9` which is isomorphic to $\mathbb{Z}/2^3$. We take $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-1}, \sqrt{2})$. Then H is the mod-3 Galois image of the curve

$$\begin{aligned} y^2 = {} & 404389000077015625x^5 + 905880526008390625x^4 - 3845554421086962500x^3 \\ & -5896039997741740000x^2 - 2199140209394684500x - 176810805117548140 \end{aligned}$$

4. 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 lmfdb support.

References

[BCGP21] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni. "Abelian surfaces over totally real fields are potentially modular". In: *Publ. Math. Inst. Hautes Études Sci.* 134 (2021), pp. 153–501 (↑ 1).

[BF22] Nils Bruin and Eugene Filatov. "Twists of the Burkhardt quartic threefold". In: *Res. Number Theory* 8.4 (2022), Paper No. 73, 16 (↑ 2, 3, 5).

[CC22] Frank Calegari and Shiva Chidambaram. "Rationality of twists of the Siegel modular variety of genus 2 and level 3". In: *Proc. Amer. Math. Soc.* 150.5 (2022), pp. 1975–1984 (↑ 1).

[CCG20] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza. "Some modular abelian surfaces". In: *Math. Comp.* 89.321 (2020), pp. 387–394 (↑ 3).

[CF96] 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 (↑ 3).

[Chi] Shiva Chidambaram. *Mod3Image* (↑ 1).

[RSZ22] 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)". In: *Forum Math. Sigma* 10 (2022). With an appendix with John Voight, Paper No. e62, 63 (↑ 1).

[RZ15] Jeremy Rouse and David Zureick-Brown. "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois". In: *Res. Number Theory* 1 (2015), Paper No. 12, 34 (↑ 1).

[Sut16] Andrew V. Sutherland. "Computing images of Galois representations attached to elliptic curves". In: *Forum Math. Sigma* 4 (2016), Paper No. e4, 79 (↑ 1, 2, 3).

[Zyw22] David Zywina. "Explicit open images for elliptic curves over $\mathbb{Q}$". 2022. arXiv: 2206.14959 [math.NT] (↑ 1).

Department of Mathematics, University of Wisconsin-Madison, Madison WI 53706-1325, USA

Email address: chidambaram3@wisc.edu

URL: https://people.math.wisc.edu/~chidambaram3