Computing the mod-3 Galois image of a principally polarized abelian surface over $\mathbb{Q}$

Shiva Chidambaram

University of Wisconsin-Madison

chidambaram3@wisc.edu

LuCaNT 2025, ICERM

July 11, 2025

From elliptic curves to pp abelian surfaces: Galois images

	elliptic curves $/\mathbb{Q}$	pp abelian surfaces $/\mathbb{Q}$
n-torsion	$(\mathbb{Z}/n)^2$	$(\mathbb{Z}/n)^4$
Galois action	$\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}/n)$	$\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}(4, \mathbb{Z}/n)$
respects Weil pairing	$\det \circ \rho_n = \chi_n$ where $\zeta_n^{\chi_n(\sigma)} = \sigma(\zeta_n)$	$\rho_n : G_{\mathbb{Q}} \to \mathrm{GSp}(4, \mathbb{Z}/n)$ and $\chi_{\mathrm{sim}} \circ \rho_n = \chi_n$ where $\chi_{\mathrm{sim}} : \mathrm{GSp}(4, \mathbb{Z}/n) \to \mathbb{Z}/n^\times$.

For a prime ℓ, can we compute the image of ρ_ℓ?

mod-ℓ image	Sutherland	?
ℓ-adic image	Rouse-Zureick–Brown and Rouse-Sutherland-Zureick–Brown	?
adelic image	Zywina	?

Main result: $\ell = 3$

Algorithm

Given any genus 2 curve $C/\mathbb{Q}$ with Jacobian J, we can compute the mod-3 image $\rho_3(G_{\mathbb{Q}})$ as a subgroup of $G = \mathrm{GSp}(4, \mathbb{Z}/3)$.

Steps

1. Find a finite list L of subgroups of G, containing $\rho_3(G_{\mathbb{Q}})$, such that L forms a single Gassmann-equivalence class, i.e., all subgroups in L have same distribution of G-conjugacy classes.
2. If L has more than one subgroup H, determine if any global data distinguishes these subgroups. Typically this is of the form $\max_{[H:H_1]=d} \dim(\mathbb{F}_3^4)^{H_1}$ for small d.
   - If yes, compute this from the curve as $\max_{\substack{[K:\mathbb{Q}]=d \\ K \subseteq \mathbb{Q}(J[3])}} \dim J[3](K)$.
   - Otherwise, bruteforce: construct the 3-torsion field K and let $\mathrm{Gal}(K|\mathbb{Q})$ act on $J[3](K)$.

Remarks

- Precomputation step: Compute the lattice of all subgroups of $\mathrm{GSp}(4, \mathbb{Z}/\ell)$ with surjective similitude character.
  Subgroup labels: $\ell.N.i$, where ℓ is the level, N is the index, and i is a counter computed deterministically using the subgroup lattice structure, orbits, conjugacy classes.
- Step 1 works for any ℓ as long as enough subgroups are computed in the precomputation step. Ongoing work to compute mod-ℓ images for typical genus 2 curves.
- Code: https://github.com/shiva-chid/mod3Galoisimage/.
- Computed the mod-3 image for all
  - 66 158 genus 2 curves in LMFDB
  - 487 493 curves in a dataset with 5-smooth conductors.
- Works for all pp abelian surfaces with no restriction on endomorphism type.

Example: Failure of local-global principle for 3-isogenies

Example

$H = 3.1080.4$ is the largest subgroup such that every element in H stabilizes an isotropic plane, but the group does not stabilize any.

The curve

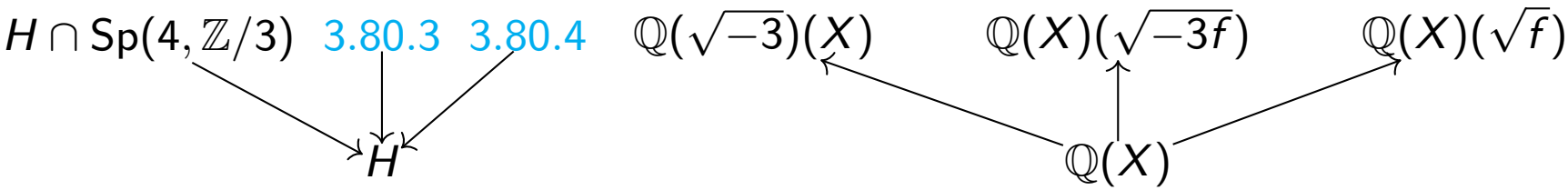
$$C : y^2 = 2x^5 - 5x^4 - x^3 + 5x^2 + 2x$$

with LMFDB label 25600.f.512000.1 has mod-3 image equal to H.

So the Jacobian J does not admit a $(3,3)$-isogeny over $\mathbb{Q}$, even though $\tilde{J}_{\mathbb{F}_p}$ admits a $(3,3)$-isogeny for every prime p of good reduction.

Example: A large image not occuring in LMFDB dataset*

Let H=3.40.2 denote the stabilizer in $\mathrm{GSp}(4,\mathbb{Z}/3)$ of an isotropic plane in $\mathbb{F}_3^4$, and $X/\mathbb{Q}$ be the moduli space of pp abelian surfaces with $\rho_3(G_{\mathbb{Q}}) \subseteq H$, i.e., parametrizing $(3,3)$-isogenies. Then, for some $f \in \mathbb{Q}(X)$, we have the diagram of function fields:



- Using a birational model of X and the curves in LMFDB with mod-3 image 3.80.4, Noam Elkies guessed the function f.
- 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 $3^2\ 7^4\ 13\ 43^2$.
- Our algorithm verifies that the mod-3 image is indeed 3.80.3.

Example: Need bruteforce!

- Since $\mathrm{GSp}(4) \neq \mathrm{GL}(4)$, we have a new problem not encountered for elliptic curves. There are Gassmann equivalent subgroups of $\mathrm{GSp}(4, \mathbb{Z}/\ell)$ that are $\mathrm{GL}(4, \mathbb{Z}/\ell)$-conjugate.
- These are indistinguishable using the two criteria above.
- So we need to bruteforce, i.e., construct the 3-torsion field K, find and lift K-points on the 3-torsion locus in the Kummer surface, and let $\mathrm{Gal}(K|\mathbb{Q})$ act.

$\lvert H\rvert$	32	16	16	16	8
Label	3.3240.6 3.3240.7	3.6480.16 3.6480.3	3.6480.13 3.6480.17	3.6480.14 3.6480.15	3.12960.5 3.12960.11

Example

Consider the curve $C : y^2 = 3x^6 + 198x^4 - 396x^2 - 24$. C is one of Robin's 512 curves, i.e, $\mathrm{Jac}(C)$ has good reduction outside $\{2\}$. Its mod-3 image is 3.3240.6.

Statistics : All curves in LMFDB dataset*

mod-3 image	Count
1.1.1	59549
3.80.1	2413
3.90.1	1624
3.40.1	553
3.720.4	443
3.80.2	336
3.270.2	177
3.45.1	145
3.360.2	96
3.270.3	74
3.720.5	57
3.480.12	57

mod-3 image	Count
3.90.2	54
3.72.2	51
3.2160.20	48
3.2160.21	43
3.432.4	30
3.80.4	27
3.2160.5	25
3.36.1	22
⋮	⋮
3.40.2	7
⋮	⋮
3.27.1	3

Statistics : Typical curves in LMFDB dataset*

mod-3 image	Count	mod-3 image	Count
1.1.1	59549	3.90.2	52
3.80.1	2413	3.72.2	1
3.90.1	10	3.2160.20	5
3.40.1	553	3.2160.21	2
3.720.4	23	3.432.4	0
3.80.2	336	3.80.4	0
3.270.2	2	3.2160.5	2
$3.45.1 \simeq \mathrm{SL}(2,\mathbb{F}_3)^2 \rtimes C_2^2$	34	$3.36.1 \simeq \mathrm{SL}(2,\mathbb{F}_9) \rtimes C_2^2$	7
3.360.2	2	⋮	⋮
3.270.3	0	3.40.2	7
3.720.5	9	⋮	⋮
3.480.12	8	3.27.1	3

Step 1: Gassmann-equivalence classes of eligible subgroups

Definition

A subgroup $H \subseteq \mathrm{GSp}(4, \mathbb{Z}/\ell)$ is eligible (to be the mod-ℓ image of a pp abelian surface $/\mathbb{Q}$) if:

- The restriction of the similitude character $\chi_{\mathsf{sim}} : \mathrm{GSp}(4, \mathbb{Z}/\ell) \to (\mathbb{Z}/\ell)^\times$ to H is surjective.
- There exists $c \in H$ of order 2 such that $\chi_{\mathsf{sim}}(c) = -1$.

$\ell = 3$

- There are 280 eligible subgroups of $\mathrm{GSp}(4, \mathbb{Z}/3)$, appearing in 230 Gassmann-equivalence classes.
- These are 38 pairs, 3 triples and 2 quadruples of Gassmann-equivalent subgroups.

Step 1: ~~Conjugacy class~~ signature

- Computing the conjugacy class of the Frobenius matrix $\rho_\ell(\mathrm{Frob}_p)$ is expensive as p grows.
- For most conjugacy classes in $\mathrm{GSp}(4, \mathbb{Z}/\ell)$, the signature

$$\langle \text{char poly of } M, \quad \chi_{\mathsf{sim}}(M), \quad \dim \ker(M - I) \rangle$$

determines the class of M uniquely.

$\ell = 3$

- The 280 eligible subgroups in 230 Gassmann-equivalence classes give rise to 214 distinct distributions of conjugacy class signatures.
- These are 42 pairs, 2 triples, 5 quadruples and 1 sextuple of subgroups with same distribution of conjugacy class signatures.

Step 1: Chebotarev density theorem

Computing the Gassmann-equivalence class

- For good primes $3 \neq p \leq B_1$, compute signature of $\rho_3(\mathrm{Frob}_p)$: $\langle p^{-2}t^4 L_p(C, p/t) \pmod 3,\ p \pmod 3,\ \dim J[3](\mathbb{F}_p)\rangle$.
- For each eligible subgroup H, compute $\mathrm{Prob}(\rho_3(G_{\mathbb{Q}}) = H)$ given the sampled distribution of Frobenius signatures. Remove those subgroups whose probability is $< \epsilon$.
- If the remaining ones form a unique Gassmann-equivalence class, return it.
- If not, repeat by computing the matrix $\rho_3(\mathrm{Frob}_p)$ for $p \leq B_2$.

Application of Chebotarev density theorem

Given a genus 2 curve $C/\mathbb{Q}$, and a positive real number ϵ close to 0, there exists $B \geq 0$ such that this algorithm with $B_i \geq B$ returns the Gassmann-equivalence class containing $\rho_3(G_{\mathbb{Q}})$.

Step 2: Distinguishing Gassmann-equivalent subgroups

Example

Standard example of Gassmann-equivalent subgroups:

$$H_1 = \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \right\} \subset \mathrm{GL}(2, \mathbb{F}_\ell) \quad \text{and} \quad H_2 = \left\{ \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix} \right\} \subset \mathrm{GL}(2, \mathbb{F}_\ell)$$

Transposing is a conjugacy preserving bijection.

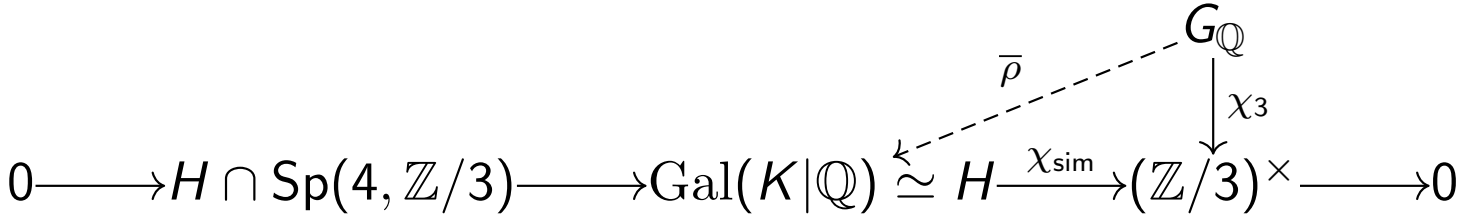
- The dimension of fixed subspace $\dim(\mathbb{F}_3^4)^H$ distinguishes most Gassmann-equivalent subgroups of $\mathrm{GSp}(4, \mathbb{Z}/3)$. So it is enough in these cases to compute $\mathrm{Jac}(C)(\mathbb{Q})[3]$ and match.
- For others, $\max_{[H:H_1]=d} \dim(\mathbb{F}_3^4)^{H_1}$ for several d are needed to distinguish. So we construct all degree d subfields K of the 3-torsion field, and for each K, compute $\dim \mathrm{Jac}(C)(K)[3]$ by finding K-points on the 3-torsion locus in the Kummer surface, and lifting them.

$\lvert H\rvert$	Label	$H \cap \mathrm{Sp}(4,\mathbb{Z}/3)$	d=1	2	3
324	3.320.1	1	1	1	1
	3.320.2	1	0	1	0
	3.320.5	0	0	1	1
	3.320.6	0	0	1	0
162	3.640.1	1	1	1	2
	3.640.2	1	1	1	1
	3.640.3	1	0	1	0
	3.640.4	1	0	1	1

$\lvert H\rvert$	Label	d=6	8	12
432	3.240.6	0	1	0
	3.240.7	0	1	1
324	3.320.3	2	-	2
	3.320.4	1	-	2
48	3.2160.9	1	1	2
	3.2160.10	1	2	2

Realization challenge

- A result of Boxer-Calegari-Gee-Pilloni implies that all 280 eligible subgroups must arise as mod-3 images of pp abelian surfaces over $\mathbb{Q}$.
- Bruin-Filatov yields in theory a way to do this, although in a round-about way.
  - For an eligible subgroup H, obtain a number field $K \supseteq \mathbb{Q}(\zeta_3)$ properly solving the embedding problem



  - Construct the corresponding twisted Burkhardt quartic threefold, and compute the genus 2 curves associated to rational points on it.

Challenge

Can we explicitly realize all eligible subgroups as mod-3 images? The unrealized ones of order > 100 are: 3.240.12, 3.270.6, 3.720.2, 3.810.3, 3.810.4, 3.810.5, 3.810.6, 3.960.9

Thanks for your attention!

I will be happy to take any questions.

Slides:

Github: