Mod-ℓ Galois image of Picard curves

Shiva Chidambaram

Massachusetts Institute of Technology

shivac@mit.edu

Joint work with Pip Goodman

Arithmetic Geometry informed by Computation

Joint Mathematics Meetings 2023

January 5, 2023

Picard curves

Let K be a number field. ($K = \mathbb{Q}$ for most of the talk.)

Definition

A Picard curve over K is a smooth projective curve C over K of genus 3 given by an affine model

$$y^3 = f(x)$$

for a degree 4 polynomial $f(x) \in K[x]$.

The map $[\zeta_3] : (x, y) \mapsto (x, \zeta_3 y)$ is an automorphism of C.

Let $J = \mathrm{Jac}(C) = \mathrm{Pic}^0(C)$ denote the Jacobian of C.
Then J is a principally polarised abelian variety of dimension 3 with $\mathrm{End}(J) \supseteq \mathbb{Z}[\zeta_3]$.

Mod-ℓ Galois representations

Let $G_K = \mathrm{Gal}(\overline{K}|K)$. Let ℓ be a prime.
Let $J[\ell]$ be the ℓ-torsion subgroup of J.
G_K acts on $J[\ell]$, giving the mod-ℓ Galois representation

$$\overline{\rho}_{J,\ell} : G_K \to \mathsf{GSp}(6, \mathbb{F}_\ell)$$

such that $\chi_{\mathsf{sim}} \circ \overline{\rho}_{J,\ell}$ is the mod-ℓ cyclotomic character χ_ℓ.

The endomorphism $[\zeta_3]$ preserves Weil pairing, so gives an element in $\mathsf{Sp}(6,\ell)$ with characteristic polynomial $(t^2+t+1)^3$.
Let $N(\ell)$ be the normalizer of $[\zeta_3]$ in $\mathsf{GSp}(6,\ell)$. The image of $\overline{\rho}_{J,\ell}$ is contained in $N(\ell)$.

Questions

1. For which ℓ, is the image of $\overline{\rho}_{J,\ell}$ not conjugate to $N(\ell)$?
2. Can we find (conj class of) the image in those cases?

Galois images in genus 1 and 2

- ℓ-adic Galois images of elliptic curves.
  Serre, Mazur, Bilu-Parent-Robledo, Sutherland, Zywina, Rouse-Zureick–Brown-Sutherland

- For an abelian surface $A/\mathbb{Q}$ with $\mathrm{End}(A) = \mathbb{Z}$, Dieulefait gives an algorithm to determine the non-surjective primes ℓ for the mod-ℓ Galois representations $\overline{\rho}_{A,\ell}$.
  For each class of maximal subgroup H of $\mathrm{GSp}(4, \cdot)$, the algorithm computes a non-zero integer M. If the image of $\overline{\rho}_{A,\ell}$ is contained in H, then ℓ must divide M.
- Banwait-Brumer-Kim-Klagsbrun-Mayle-Srinivasan-Vogt have a Sage implementation of this algorithm.

The maximal images $N(\ell)$

- $\ell = 1 \mod 3$: Then $N(\ell) \simeq (\mathrm{GL}(3,\ell) \times \mathbb{F}_\ell^\times) \rtimes \langle \gamma \rangle$, where

$$\begin{aligned} \mathrm{GL}(3,\ell) \times \mathbb{F}_\ell^\times &\to \mathrm{GSp}(6,\ell) \\ (A,\mu) &\mapsto \begin{bmatrix} \mu A & 0 \\ 0 & A^{-t} \end{bmatrix} \end{aligned}$$

  and γ permutes the two isotropic 3-dimensional subspaces.
- $\ell = 2 \mod 3$: Then $N(\ell) \simeq \Delta U(3,\ell) \rtimes \langle \mathrm{Frob} \rangle$.
  Let V be a 3-dim vector space over $\mathbb{F}_{\ell^2}$ with a hermitian form, and an orthonormal basis v_1, v_2, v_3. Let

$$\Delta U(3,\ell) := \{T : V \to V | \langle Tv, Tw \rangle = \alpha \langle v, w \rangle \text{ for some } \alpha \in \mathbb{F}_\ell^\times\}.$$
$$\mathrm{Frob} : V \to V \text{ is the semilinear map } \sum a_i v_i \mapsto \sum \overline{a_i} v_i.$$

  If $\xi \notin \mathbb{F}_\ell$ and ξ^2 is a primitive element in $\mathbb{F}_\ell$, then $\mathrm{Tr}(\xi \langle \cdot, \cdot \rangle)$ is a symplectic $\mathbb{F}_\ell$-bilinear pairing on V, and we can view $\Delta U(3,\ell) \subseteq \mathrm{GSp}(6,\ell)$ and $\mathrm{Frob} \in \mathrm{GSp}(6,\ell)$.

Main result

Algorithm

Input: a degree 4 polynomial $f(x) \in \mathbb{Q}[x]$ with no repeated roots.
Output: A finite list of primes containing all the primes ℓ such that $\overline{\rho}_{J,\ell}$ has non-maximal image, i.e., $\mathrm{im}\,\overline{\rho}_{J,\ell} \subsetneq N(\ell)$.

Ingredients:

- [Bray-Holt-Roney–Dougal] The Maximal Subgroups of the Low-Dimensional Finite Classical Groups.
- [Goodman] Superelliptic curves with large Galois images.
- [Asif-Fite-Pentland] Computing L-polynomials of Picard curves from Cartier Manin matrices.
- [Bouw-Koutsianas-Sijsling-Wewers] Conductor and discriminant of Picard curves.

Example

Let $C : y^3 = x^4 - x^2 - x + 1$. Conductor of C is $3^8 23^2$.

The mod-ℓ Galois representation of $\mathrm{Jac}(C)$ has maximal image for all primes ℓ outside the set

$$\{2, 3, 5, 7\} \cup \text{Bad Primes}(C) \cup \{\}.$$

$\ell = 1 \mod 3$. Maximal subgroups of $\mathrm{GL}(3, \ell)$.

Let V be a 3-dim vector space over $\mathbb{F}_\ell$. Up to conjugacy, the maximal subgroups of $\mathrm{GL}(3, \ell)$ not containing $\mathrm{SL}(3, \ell)$ are:

1. **Reducible:** Stabilizer of a subspace $U \subsetneq V$ where $\dim U = 1$ or 2. Both cases yield conjugate subgroups inside $\mathrm{GSp}(6, \ell)$.
2. **Imprimitive:** Stabilizer of a decomposition $V \simeq \oplus_{i=1}^{3} V_i$. Isomorphic to $\mathrm{GL}(1, \ell)^3 \rtimes S_3$.
3. **Field extension subgroup:** A subgroup isomorphic to $\mathrm{GL}(1, \ell^3) \rtimes \mathrm{Gal}(\mathbb{F}_{\ell^3}|\mathbb{F}_\ell)$.
4. **Symplectic type subgroup:** If $\ell = 4, 7 \mod 9$, a subgroup with projective image isomorphic to $C_3^2 \rtimes \mathrm{SL}(2, 3)$.

$\ell = 2 \mod 3$. Maximal subgroups of $\mathrm{GU}(3,\ell)$.

Let V be a 3-dim vector space over $\mathbb{F}_{\ell^2}$ with a hermitian form. Recall $GU(3,\ell)$ is the unitary group consisting of all $\mathbb{F}_{\ell^2}$-linear maps preserving the form. Up to conjugacy, the maximal subgroups of $\mathrm{GU}(3,\ell)$ not containing $\mathrm{SU}(3,\ell)$ are:

1. **Reducible:**
   - Stabilizer of an isotropic 1-dim subspace $U \subsetneq V$.
   - Stabilizer of a non-degenerate 1-dim subspace $U \subsetneq V$.

   In both cases, the semisimplification of V contains a 1-dim non-degenerate constituent.
2. **Imprimitive:** Stabilizer of an orthogonal decomposition $V \simeq \oplus_{i=1}^{3} V_i$. Isomorphic to $\mathrm{GU}(1,\ell)^3 \rtimes S_3$.
3. **Field extension subgroup:** A subgroup isomorphic to $\mathrm{GU}(1,\ell^3) \rtimes \mathrm{Gal}(\mathbb{F}_{\ell^3}|\mathbb{F}_\ell)$.
4. **Symplectic type subgroup:** If $\ell = 2, 5 \mod 9$, a subgroup with projective image isomorphic to $C_3^2 \rtimes \mathrm{SL}(2,3)$.

Reducible case: Dihedral representations

Lemma

Suppose we are in the (absolutely) reducible case. Then there exists an odd two dimensional representation τ of $G_{\mathbb{Q}}$ satisfying the following.

- *τ restricted to $G_{\mathbb{Q}(\zeta_3)}$ is contained in the semisimplification of $\overline{\rho}_{J,\ell}\,|_{\mathbb{Q}(\zeta_3)}$.*
- *the projective image of τ is dihedral, such that the quadratic field cut out by the projectivisation of τ is $\mathbb{Q}(\zeta_3)$.*
- *$\tau|_{I_\ell} = \mathbf{1} + \chi_\ell$ or $\theta_2 + \theta_2^\ell$.*

Such representations τ come from cusp forms with CM by $\mathbb{Q}(\zeta_3)$, or alternatively from algebraic Hecke characters ψ of $\mathbb{Q}(\zeta_3)$.

Test for reducible case: Algorithm

Let N be the conductor of J. Let S be a set of primes $p = 1 \mod 3$.

Algorithm

1. Find all algebraic Hecke characters ψ of $\mathbb{Q}(\zeta_3)$ of modulus $\mathfrak{m}$ satisfying $\mathrm{Norm}(\mathfrak{m}) | (N/3^3)$, and some further absolute bounds on $\mathrm{ord}_p \mathrm{Norm}(\mathfrak{m})$ for each prime p.
2. For each $p \in S$, compute the Euler factor
$$x^2 - (\psi(\mathfrak{p}) + \psi(\overline{\mathfrak{p}}))x + \psi(p)$$
for each ψ in (1). Take the product over all ψ. Call it $F_p(x)$.
3. For each $p \in S$, compute the L-polynomial of J at p. Call it $G_p(x)$. Note that its reduction mod ℓ is the characteristic polynomial of $\overline{\rho}_{J,\ell}(\mathrm{Frob}_p)$.
4. Let $M := \mathrm{gcd}_{p \in S} \mathrm{Res}(F_p(x), G_p(x))$.

If $J[\ell]$ is reducible, then ℓ must divide M.

Action of inertia at ℓ

Let λ be a prime of $\mathbb{Z}[\zeta_3]$ lying above ℓ. Let ρ_λ denote the Galois action on $J[\lambda]$.

Proposition(Goodman)

Suppose J has good reduction at ℓ.

- If $\ell = 1 \mod 3$, then

$$\det \rho_\lambda |_{I_{\lambda'}} = \begin{cases} \chi_\ell^2 & \text{if } \lambda' = \lambda \\ \chi_\ell & \text{if } \lambda' = \overline{\lambda} \end{cases}$$

- If $\ell = 2 \mod 3$, then $\det \rho_\lambda |_{I_\lambda} = \theta_2^{2+\ell}$, where θ_2 is a fundamental character of level 2.

Action of inertia at ℓ

Accordingly, we get using Raynaud's theorem about the constituents in the semisimplification of $\rho_\lambda \mid_{I_{\lambda'}}$

Proposition

Let θ_n is a fundamental character of level n.

- If $\ell = 1 \mod 3$, then

$$\rho_\lambda^{ss} \mid_{I_{\overline{\lambda}}} = 2\mathbf{1} + \chi_\ell, \mathbf{1} + \theta_2 + \theta_2^\ell \text{ or } \theta_3 + \theta_3^\ell + \theta_3^{\ell^2}, \text{ and}$$
$$\rho_\lambda^{ss} \mid_{I_\lambda} = \chi_\ell \otimes \left(\rho_\lambda^{ss} \mid_{I_{\overline{\lambda}}}\right)^{-T}$$

- If $\ell = 2 \mod 3$, then $\rho_\lambda^{ss} \mid_{I_\lambda} = 2\theta_2 + \theta_2^\ell$ or $\mathbf{1} + \chi_\ell + \theta_2$.

Test for Imprimitive case

Suppose that $\mathrm{im}\overline{\rho}_{J,\ell}$ is contained in the imprimitive maximal subgroup $H \simeq \mathrm{GL}(1,\ell)^3 \rtimes S_3$, or $\mathrm{GU}(1,\ell)^3 \rtimes S_3$.
We consider the projectivisation of $\overline{\rho}_{J,\ell}$.

- $P\rho_\lambda^{ss}\mid_{I_{\lambda'}} = 2\mathbf{1} + \theta_2^{1\pm\ell}$.
- The Galois image in the S_3-quotient is either C_3 or S_3.
- In either case, this quotient is only ramified at primes dividing N, and not ramified at ℓ.
- **Case 1:** There exists a C_3 extension $L|\mathbb{Q}(\zeta_3)$ unramified away from N, such that whenever $\mathrm{Frob}_\mathfrak{p}$ is non-trivial in $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3))$, we have $\mathrm{Tr}\rho_\lambda(\mathrm{Frob}_\mathfrak{p}) = 0 \mod \lambda$.
- **Case 2:** There exists a C_2 extension $L/\mathbb{Q}(\zeta_3)$ unramified away from N, such that whenever $\mathrm{Frob}_\mathfrak{p}$ is non-trivial in $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3))$, we have $ab = c \mod \lambda$ where $x^3 + ax^2 + bx + c$ is the char poly of $\mathrm{Frob}_\mathfrak{p}$.

Summary

The algorithm has been implemented in Magma at
https://github.com/shiva-chid/Picard.
It takes as input a degree 4 polynomial $f(x)$, and optionally the conductor of the curve $y^2 = f(x)$, and produces a finite set S of primes containing all non-surjective primes.

Remarks

- For small primes ℓ, the distribution of the characteristic polynomials almost exactly determines the subgroup of the maximal group (except in the reducible case).
- Thus, sampling L-polynomials gives a probablistic method to recover the image exactly in these cases. Reducible case and large ℓ seem hard.

Thank you