Computing exceptional primes for torsion Galois representations of Picard curves

Shiva Chidambaram

Massachusetts Institute of Technology

shivac@mit.edu

Joint work with Pip Goodman

PAlmetto Number Theory Series XXXVI

October 22, 2023

Torsion (or Mod-ℓ) Galois representations

- C - nice curve of genus g defined over $\mathbb{Q}$.
- $J = \mathrm{Jac}(C) = \mathrm{Pic}^0(C)$ - Jacobian of C.
  It is a principally polarized abelian variety of dimension g.
  $J(\mathbb{C})$ is a complex torus $\mathbb{C}^g/\Lambda$ for some lattice Λ.
  Example:
  If $g = 1$ and $C(\mathbb{Q}) \neq \emptyset$, then $J = C$ is an elliptic curve.
- For any prime ℓ, the ℓ-torsion subgroup $J[\ell] \simeq (\mathbb{Z}/\ell)^{2g}$ carries a non-degenerate alternating pairing $J[\ell] \times J[\ell] \to \mu_\ell$.
- The absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ acts on $J[\ell]$, equivariantly wrt this pairing, giving the ℓ-torsion (or mod-ℓ) Galois representation $\overline{\rho} := \overline{\rho}_{J,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(2g, \mathbb{F}_\ell)$ such that

$$G_{\mathbb{Q}} \xrightarrow{\overline{\rho}} \mathrm{GSp}(2g, \mathbb{F}_\ell) \xrightarrow{\chi_{\mathrm{sim}}} \mathbb{F}_\ell^\times, \qquad \chi_{\mathrm{sim}} \circ \overline{\rho} = \chi_\ell.$$

Picard curves

A Picard curve over $\mathbb{Q}$ is a smooth projective curve C of genus 3 given by an affine model $y^3 = f(x)$ for a degree 4 polynomial $f(x)$ with coefficients in $\mathbb{Q}$, and having no repeated roots.

- The map $[\zeta_3] : (x, y) \mapsto (x, \zeta_3 y)$ is an automorphism of C. So we have $\mathbb{Z}[\zeta_3] \subseteq \mathrm{End}(J)$.
- $[\zeta_3]$ preserves Weil pairing, so gives an element in $\mathrm{Sp}(6)$ with characteristic polynomial $(t^2 + t + 1)^3$.
- The image of $\overline{\rho}$ lies inside the normalizer of $[\zeta_3]$ in $\mathrm{GSp}(6, \ell)$. We say that $\overline{\rho}$ is surjective if this is an equality. In this case

$$\overline{\rho}(G_{\mathbb{Q}(\zeta_{3\ell})}) = \begin{cases} \mathrm{GL}(3, \mathbb{F}_\ell) & \text{if } \ell = 1 \mod 3 \\ \mathrm{GU}(3, \mathbb{F}_\ell) & \text{if } \ell = 2 \mod 3. \end{cases}$$

  Otherwise, we say that ℓ is exceptional or non-maximal.

Question

For a given Picard curve C, can we find all exceptional primes ℓ?

The Normalizer of $[\zeta_3]$ in $GSp(6, \ell)$

- $\ell = 1 \mod 3$: If $\ell\mathbb{Z}[\zeta_3] = \lambda_1\lambda_2$, then $J[\ell] = J[\lambda_1] \oplus J[\lambda_2]$ as $G_{\mathbb{Q}(\zeta_3)}$-representations.
  The normalizer is $(\mathrm{GL}(3, \ell) \times \mathbb{F}_\ell^\times) \rtimes \langle\gamma\rangle$, where

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

  and γ swaps the two isotropic 3-dim subspaces $J[\lambda_1]$ and $J[\lambda_2]$.

- $\ell = 2 \mod 3$: As $G_{\mathbb{Q}(\zeta_3)}$-representations, $J[\ell]$ can be thought of as a 3-dim representation V over $\mathbb{F}_{\ell^2}$;
  and the symplectic pairing becomes a hermitian form on V.
  The normalizer is $\Delta U(3, \ell) \rtimes \langle \mathrm{Frob} \rangle$. where $\Delta U(3, \ell)$ is the group of similarities of a hermitian form.

What's known for elliptic curves?

Theorem (Serre's open image theorem)

For a non-CM elliptic curve E over a number field K, the ℓ-torsion representation $\overline{\rho}_{E,\ell} : G_K \to \mathrm{Aut}(E[\ell]) = \mathsf{GL}(2, \mathbb{F}_\ell)$ is surjective for all but finitely many primes ℓ.

Serre's uniformity conjecture

For elliptic curves over $\mathbb{Q}$, the ℓ-torsion representation is surjective whenever $\ell > 37$.

- A stronger uniformity conjecture and an algorithm to find exceptional primes - Zywina.
- Algorithms to find ℓ-adic Galois images - Sutherland, Zywina, Rouse–Zureick-Brown–Sutherland

What's known for $g = 2$?

Serre's open image theorem

If $A/\mathbb{Q}$ is a principally polarized abelian surface with $\mathrm{End}(A) = \mathbb{Z}$, then $\overline{\rho}_{A,\ell}$ is surjective for all but finitely many primes ℓ.

- No uniform bound (analogous to 37 for $g = 1$) conjectured.

- [Die02]: algorithm to find exceptional primes for a given $A/\mathbb{Q}$. The algorithm computes a non-zero integer M for each class of maximal subgroup H of $\mathrm{GSp}(4)$, such that:

$$\overline{\rho}_{A,\ell}(G_{\mathbb{Q}}) \subseteq H \quad \Longrightarrow \quad \ell | M.$$

- [BBK$^+$23]: Sage implementation + theoretical uniform bound $\exp(N^{1/2+\epsilon})$ in terms of conductor N (assuming GRH).
- Largest exceptional prime they find is 31 for the Jacobian of $C : y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45$. [vBCCK23]: confirm by exhibiting an isogeny of degree 31^2.

Main result

Algorithm (Goodman-C)

Input: a degree 4 polynomial $f(x) \in \mathbb{Q}[x]$ with no repeated roots.
Output: A finite list of primes containing all the exceptional primes ℓ at which $\overline{\rho}_{J,\ell}$ is non-surjective.

Magma implementation at `https://github.com/shiva-chid/Picard`.

Examples

Searching in a box

We considered the curves $C : y^3 = x^4 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and $|a|, |b|, |c| \leq 100$, and $b > 0$.

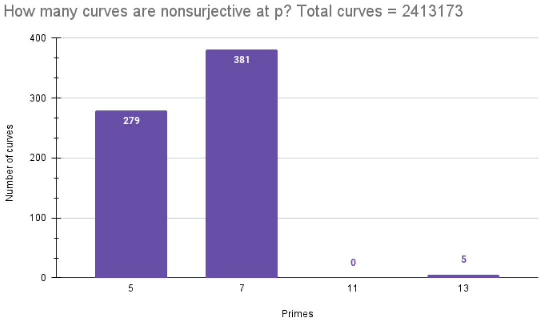
- The curve $y^3 = x^4 + 10x^2 + 8x + 13$ seems to have reducible image at $\ell = 7$, i.e.,
  $J[7]$ must have a cyclic subgroup of order 7 defined over $\mathbb{Q}(\zeta_3)$.
- No examples with an exceptional prime > 7.

More interesting example

Let $C : y^3 = 243x^4 + 338x^3 - 147x^2 - 387x - 142$ and $J = \mathrm{Jac}(C)$.
Then $\overline{\rho}_{J,\ell}$ is surjective for all primes $\ell \neq 2, 13$.
Note: This is the largest exceptional prime we have found so far.

The image of $\overline{\rho}_{J,13}$ seems to be reducible, i.e.,
$J[13]$ must have a cyclic subgroup of order 13 defined over $\mathbb{Q}(\zeta_3)$.

Sutherland's dataset of ~ 3 million Picard curves



- Curves in the dataset have good reduction outside $\{2, 3, 5, 7\}$.
- All exceptional primes > 2 correspond to reducible images.
- All five curves with 13 as an exceptional prime are twists.
- Bias towards $1 \mod 3$ primes being exceptional, more than $2 \mod 3$ primes.

Ingredients in Proof

- Classification of maximal subgroups of low-dimensional finite classical groups - [Bray–Holt–Roney-Dougal]
- Control action of inertia group at primes λ above ℓ. Specifically,
  - Tameness
  - determinant character $\det(\overline{\rho}_{J,\lambda}) |_{I_\lambda}$ - [Goodman]
- L-polynomials of Picard curves - [Asif-Fite-Pentland]
  Example: For an elliptic curve $E/\mathbb{Q}$, the L-polynomial at p is $1 - a_p(E)t + pt^2$.

$\ell = 1 \mod 3$. 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 $0 \subsetneq U \subsetneq V$.
   The two 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 $C_3^2 \rtimes \mathrm{SL}(2, 3)$.

Test in "Field-extension" case

Suppose that $\mathrm{im}(\overline{\rho}_{J,\ell})$ lies inside $H \simeq \mathsf{GL}(1, \ell^3) \rtimes \mathrm{Gal}(\mathbb{F}_{\ell^3}|\mathbb{F}_\ell)$.

- Consider the further quotient $H \to \mathrm{Gal}(\mathbb{F}_{\ell^3}|\mathbb{F}_\ell)$. This cuts out some C_3-extension $K|\mathbb{Q}(\zeta_3)$.
- Let $\ell = \lambda\overline{\lambda}$ in $\mathbb{Z}[\zeta_3]$. If $\mathfrak{p} \subset \mathbb{Z}[\zeta_3]$ is a prime that remains inert in K, then $\mathrm{Tr}\rho_\lambda(\mathrm{Frob}_\mathfrak{p}) = 0 \mod \lambda$ and $\mathrm{Tr}\rho_{\overline{\lambda}(\mathrm{Frob}_\mathfrak{p}) = 0 \mod \overline{\lambda}}$.

Let S be the set of primes of bad reduction for the curve.
If we can show that K is unramified away from S, i.e., K is not ramified at ℓ, then:

Algorithm

1. Enumerate all C_3 field extensions $K|\mathbb{Q}(\zeta_3)$ unramified away S.
2. For each K, and primes p up to a chosen bound, calculate the product $\mathrm{Tr}\rho_\lambda(\mathrm{Frob}_\mathfrak{p}) \cdot \mathrm{Tr}\rho_{\overline{\lambda}(\mathrm{Frob}_\mathfrak{p})}$, whenever possible, from the L-polynomial at p. Let N_K be their gcd.
3. Return all prime factors of all N_K.

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

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

- 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 $\rho_\lambda |_{I_{\lambda'}}$

Proposition

Let θ_n be a fundamental character of level n.

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

$$\rho_\lambda^{ss} |_{I_{\overline{\lambda}}} = 2\mathbf{1} + \chi_\ell, \mathbf{1} + \theta_2 + \theta_2^\ell \text{ or } \theta_3 + \theta_3^\ell + \theta_3^{\ell^2}, \text{ and}$$

$$\rho_\lambda^{ss} |_{I_\lambda} = \chi_\ell \otimes \left(\rho_\lambda^{ss} |_{I_{\overline{\lambda}}}\right)^{-T}$$

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

Summary

Main result

An algorithm that takes as input a Picard curve $C : y^3 = f_4(x)$ and produces a finite set containing all exceptional primes for $\mathrm{Jac}(C)$.
Magma implementation at `https://github.com/shiva-chid/Picard`.

Future work

- For small ℓ, the distribution of characteristic polynomials seems to determine the image of $\overline{\rho}_{J,\ell}$ exactly (except in the reducible case).
- In the reducible case, we are trying to write down the explicit congruence relations with Bianchi modular forms for $\mathbb{Q}(\zeta_3)$.

Thank you

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, 2023.
arXiv:2301.02222.

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(4):503–512, 2002.
URL:
http://projecteuclid.org/euclid.em/1057864660.

Raymond van Bommel, Shiva Chidambaram, Edgar Costa, and Jean Kieffer.
Computing isogeny classes of typical principally polarized abelian surfaces over the rationals, 2023.
arXiv:2301.10118.