


Computing Galois images of Picard curves

§1. Setup

C - smooth projective curve of genus 3 / $\mathbb{Q}$.

$J = \text{Jac}(C)$. $S = \{\text{bad primes}\}$

$J_{\overline{\mathbb{Q}}}$ is simple & $\text{End}^0(J_{\overline{\mathbb{Q}}}) = E = \mathbb{Q}(\sqrt{D})$ $D > 0$

$\overline{\rho}_\ell: G_{\mathbb{Q}} \longrightarrow \text{Aut}(J[\ell]) = \text{GSp}(6, \mathbb{F}_\ell)$.

Ex: $C: y^3 = x^4 + ax^2 + bx + c$ Picard curve.

$\text{Aut}(C_{\overline{\mathbb{Q}}}) \supseteq \langle [\zeta_3]: (x, y) \mapsto (x, \zeta_3 y) \rangle$

$\text{End}(J_{\overline{\mathbb{Q}}}) \supseteq \mathbb{Z}[\zeta_3] \subseteq \mathbb{Q}(\zeta_3) = E$.

$\ell \equiv 1 \pmod{3}$ $J[\ell] = J[\lambda_1] \oplus J[\lambda_2]$ into maximal isotropic subspaces

$\ell = \lambda_1, \lambda_2$. $\overline{\rho}_\ell|_E = \begin{bmatrix} \overline{\rho}_{\lambda_1} & \\ & \overline{\rho}_{\lambda_2} \end{bmatrix}$ where $\overline{\rho}_{\lambda_2} = \chi \otimes \overline{\rho}_{\lambda_1}^{-t}$

$\ell \equiv 2 \pmod{3}$ Hermitian form $\langle, \rangle: J[\ell] \times J[\ell] \rightarrow \mathbb{F}_\ell^2$

$\mathbb{F}_\ell^2 = \mathbb{F}_\ell[\alpha]$ where $\alpha^2 \in \mathbb{F}_\ell$. $\langle v, w \rangle = (\alpha v, w) + \alpha (v, w)$

$\overline{\rho}_\ell(G_{E(\zeta_\ell)}) \subseteq \begin{cases} \text{GL}(3, \mathbb{F}_\ell) & \text{if } \ell \equiv 1 \pmod{3} \\ \text{GU}(3, \mathbb{F}_\ell) & \text{if } \ell \equiv 2 \pmod{3} \end{cases} = C_{\text{Sp}(6, \mathbb{F}_\ell)}([\zeta_3])$

$[\zeta_3] \in \text{Sp}(6, \mathbb{F}_\ell)$ ($\because \langle \alpha P, \alpha P \rangle = \langle P, \alpha^2 \alpha P \rangle = (\deg \alpha) \langle P, P \rangle$)

$\text{Im}(\overline{\rho}_\ell) \subseteq N_{\text{GSp}(6, \mathbb{F}_\ell)}([\zeta_3])$

Claim: $\overline{P}(G_{E(\mathbb{G}_\ell)}) \subseteq \begin{cases} GL(3, \mathbb{F}_\ell) & \text{if } \left(\frac{-D}{\ell}\right) = 1 \\ GU(3, \mathbb{F}_\ell) & \text{if } \left(\frac{-D}{\ell}\right) = -1 \end{cases}$

(Wall 1963, 2015): conjugacy classes in symplectic groups.

(Franceschi-Liebeck-O'Brien 2024):

Explicit centralizers in finite classical groups
in terms of factorization type of characteristic polynomial

(Burness-Giudici 2016): Classical groups, derangements and primes.

Defn: We say $\overline{P}$ is surjective, if this is an equality.
Otherwise, we say that ℓ is a non-maximal prime.

Q: For a given curve, Can we find all non-maximal primes?

Q: Can we compute $\overline{P}_\ell(G_\Phi)$ for these primes?

§2. Main result

Thm (C-Goodman)

∃ an efficient algorithm, guaranteed to terminate,
which takes

input: the curve C

output: a finite set of primes containing all
non-maximal primes.

Remarks (to say)

1. input really only need the set of bad primes,
and L-polynomials at primes upto a bound.
2. output first we produce a big set that includes
 $\{\text{all primes up to } \gamma\} \cup \{\text{bad primes}\} \cup \{\text{all primes dividing various quantities we compute}\}$

Then, we weed out extraneous primes
by sampling more L-polys.

3. efficient < a sec per curve 4 million Picard curves
in 15 h as 128 parallel jobs
4. bottleneck Fast computation of L-polys.
We use (Asif-Fite-Pentland)'s method for Picard curves.
5. To answer Q2 we have a probabilistic method to compute
image, but it does not work very well
in the reducible case

First output = $S \cup \{2, 5, 7\} \cup \{\text{primes } x \text{ dividing } \ast\}$

Final output after pruning = a small subset of first output
 $\cup$
 $\{\text{non-maximal primes}\}$.

Observations

(Drew): ~ 3 million Picard curves
 with good reduction outside $\{2, 3, 5, 7\}$.

l	# curves with	
	$\overline{P}_l$ reducible	l non-maximal
2	many 279	many 279
5	381	381
7		
13	5	5

- All 5 curves with $\overline{P}_{13}$ reducible are twists of
 $C: y^3 = 243x^4 + 338x^3 - 147x^2 - 387x - 142$

Note: $J[l]$ has a cyclic subgroup $\simeq E$ of order l .

§3. Known results for $g \leq 2$

Thm (Serre)

For non-CM elliptic curves $E/\mathbb{Q}$,

$\rho_l: G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_l)$ is surjective $\forall l \gg 0$.

$\mathbb{Q}$ (Serre)

Is 37 a uniform upper bound for non-maximal primes?

Thm (Mazur) For $l > 37$, $X_0(l)$ has only cusp/CM rational points.

Thm (Bilu-Parent-Rebolledo) For $l > 13$, $\rho_l(G_{\mathbb{Q}}) \not\subseteq$ Normalizer of split Cartan.

Thm (Zywina '22) Algorithm to find non-maximal primes for given E

Conj (Zywina '22)

13 is a uniform upper bound if we exclude the 4 j -invs coming from non-CM ratl points on $X_0(17), X_0(37)$.

Thm (Diolefait '02) Algorithm to find non-maximal primes for given A .

Thm (Banwait-Brumer-Kim-Klagsbrun-Mayle-Srinivasan-Vogt) Theoretical uniform upper bound $\exp(N^{\frac{1}{2}+\epsilon})$.

+ Sage implementation.

Largest non-maximal prime they find is 31.

[vBC-G-K] verify this in our work on computing isogeny classes.

§4. Ideas in proof

Classification of Maximal subgroups of $GL(3, \mathbb{F}_\ell)$
 $GU(3, \mathbb{F}_\ell)$

a) Reducible

b) Normalizer of split Cartan

$$GL(1, \mathbb{F}_\ell)^3 \rtimes S_3$$

$$GU(1, \mathbb{F}_\ell)^3 \rtimes S_3$$

c) Normalizer of non-split Cartan

$$GL(1, \mathbb{F}_{\ell^3}) \rtimes (\mathbb{Z}/3)$$

$$GU(1, \mathbb{F}_{\ell^3}) \rtimes (\mathbb{Z}/3)$$

d) Exceptional groups with proj. image $\simeq ASL_2(\mathbb{F}_3)$
for $\ell \equiv \pm 4, \pm 7 \pmod 9$.

a) Thm (Raynaud)

Let $n \geq 5$.

A_K attains semistable reduction over $K(A[n])$

at all primes $v \nmid n$

Thm (Grothendieck)

A has semistable
reduction at v



I_v acts unipotently on
 $T_\ell A$, $\ell \neq \text{res. char of } v$.

Suppose $\exists \lambda \mid l$ and $\chi : G_E \rightarrow \mathbb{F}_\lambda^\times$ is a 1-dim factor of $\overline{\rho}_\lambda|_E$

Consider $\beta \mid p$, with $p \nmid N$. Let $\beta = (\gamma)$

$\Phi_\beta \in \mathbb{Q}_E[x]$ - char poly of Frob_β . $\deg \Phi_\beta = 3$

Key: $\Phi_\beta(\chi(\text{Frob}_\beta)) = 0 \pmod{\lambda}$

so, $\Phi_\beta^{(n)}(\chi^n(\text{Frob}_\beta)) = 0 \pmod{\lambda}$

where $P^{(n)}(x) = \text{Res}(P(T), x - T^n)$

Using semistable reduction over $E(A[n])$, n prime ≥ 5 , $n \neq l$

For $v \nmid l$, $\chi^{e(n)}|_{I_v} = 1$ where $e(n) = \begin{cases} \exp(GL(3, \mathbb{F}_n)) \\ \exp(GU(3, \mathbb{F}_n)) \end{cases}$

$\Rightarrow \chi^{72}|_{I_v} = 1$

For $v \mid l$, $\chi|_{I_v} = \begin{cases} 1, \chi_l & \text{if } l \equiv 1 \pmod{3} \\ 1, \theta_2, \theta_2^l, \chi_l & \text{otherwise} \end{cases}$

CFT $\Rightarrow 1 = \text{Art}_E((\gamma)_v) = \left(\prod_{v \mid l} \text{Art}_{E_v}(\gamma) \right) \cdot \text{Art}_p(\gamma) \left(\prod_{\substack{v \mid N \\ v \neq \beta}} \text{Art}_v(\gamma) \right)$

$1 = \prod_{v \mid l} \{1, \theta_2, \theta_2^l, \chi_l\}^{72} (\text{Art}_{E_v}(\gamma)) \chi^{72}(\text{Frob}_\beta) \cdot 1$

Thm: $\exists \alpha \in S_\gamma = \{1, \gamma, \bar{\gamma}, p, \bar{\gamma}^2, \bar{\gamma}^2, p\gamma, p\bar{\gamma}, p^2\}$ s.t. $\Phi_\beta^{(72)}(\alpha^{72}) = 0 \pmod{\lambda}$.

Further $\exists$ infinitely many β s.t. $\Phi_\beta^{(72)}(\alpha^{72}) \neq 0 \forall \alpha \in S_\gamma$.

b, c, d

What's inertia at l of $\bar{\rho}_l$?

(Fite 20): $\Omega: \mathbb{I}_K \longrightarrow E^\times$ algebraic Hecke character

corresponding to the compatible family $(\det \circ \bar{\rho}_\lambda)_\lambda$.

Then, Infinity type of Ω = Signature of $E \hookrightarrow \Omega(\tau)$

(Shimura '63): Signature of $E \hookrightarrow \Omega(\tau) = (2, 1)$ as otherwise,
Prop 14 if it is $(3, 0)$, then J is isogenous to E^3 for an elliptic curve E

Thm (C-Goodman) For good primes l ,

$$1) \text{ If } \left(\frac{-D}{l}\right) = 1, \text{ then } \det \circ \bar{\rho}_\lambda \big|_{\mathbb{I}_X} = \begin{cases} \chi_l^2 & \text{if } \lambda' = \lambda \\ \chi_l & \text{if } \lambda' = \bar{\lambda} \end{cases}$$

$$\text{Hence, } \bar{\rho}_\lambda^{ss} \big|_{\mathbb{I}_{\bar{\lambda}}} = \begin{cases} 2 \cdot 1 + \chi_l \\ 1 + \theta_2 + \theta_2^l \\ \theta_3 + \theta_3^l + \theta_3^{l^2} \end{cases}$$

$$2) \text{ Otherwise, } \det \circ \bar{\rho}_l \big|_{\mathbb{I}_l} = \theta_2^{2+l}$$

$$\text{Hence, } \bar{\rho}_l^{ss} \big|_{\mathbb{I}_l} = \begin{cases} 1 + \chi_l + \theta_2 \\ 2\theta_2 + \theta_2^l \end{cases}$$

and some more -

$$\begin{aligned} & \theta_6^{l+l^2+l^3} + \theta_6^{l^2(l+l^2+l^3)} + \theta_6^{l^4(l+l^2+l^3)} \\ & \theta_6^{l+l^2+l^5} + \theta_6^{l^2(l+l^2+l^5)} + \theta_6^{l^4(l+l^2+l^5)} \\ & \theta_6^{l^3+l^2+l^5} + \theta_6^{l^2(l^3+l^2+l^5)} + \theta_6^{l^4(l^3+l^2+l^5)} \end{aligned}$$

Suppose $\text{Im}(\bar{P}_\lambda) \subseteq \text{GL}_1(\mathbb{F}_{l^3}) \rtimes \mathbb{Z}/3$.

Claim: The $\mathbb{Z}/3$ -quotient of $\bar{P}_\lambda$ is unramified above l .

Pf: $\bar{P}_\lambda|_{I_\lambda}$ implies that $\text{Im}(\bar{P}_\lambda|_{I_\lambda})$ is a cyclic group of order $l^3 - 1$. The only such subgroup is $\text{GL}_1(\mathbb{F}_{l^3})$

or if $\left(\frac{-D}{l}\right) = -1$, $\text{Im}(\bar{P}_\lambda|_{I_\lambda})$ is a cyclic subgroup of order $\geq (l^3 + 1)(l - 1)$, which is only possible for $l \leq 5$

Algorithm:

- Enumerate $\mathbb{Z}/3$ -extensions $L|\mathbb{Q}(\zeta_3)$ unramified away from N .

- For each L , and $p \leq B$, compute

$$\text{Tr } P_\lambda(\text{Frob}_p) \cdot \text{Tr } P_{\bar{\lambda}}(\text{Frob}_p)$$

- This $\equiv 0 \pmod{l}$, if p is inert in $L|\mathbb{Q}(\zeta_3)$.

- Return all prime factors of gcd .