ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$

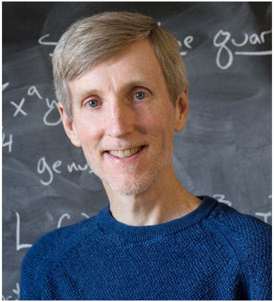
Jeremy Rouse

WAKE FOREST UNIVERSITY

VaNTAGe seminar
June 22, 2021

Acknowledgements

- The work I'm going to speak about is joint with Drew Sutherland and David Zureick-Brown.



Definitions

- Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

- If $E/\mathbb{Q}$ is an elliptic curve, let $E[n] = \{Q \in E(\overline{\mathbb{Q}}) : nQ = 0\} \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

- If n is a positive integer, define $\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(n)$.

Mazur's Program B

- If ℓ is a prime, let $\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell) = \varprojlim \mathrm{GL}_2(\ell^k)$.
- Let $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim \mathrm{GL}_2(n)$.

B. Given a number field K and a subgroup H of $\mathrm{GL}_2 \hat{\mathbb{Z}} = \prod_p \mathrm{GL}_2 \mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\bar{K}/K)$ into $H \subset \mathrm{GL}_2 \hat{\mathbb{Z}}$.

Prime level

• If $E/\mathbb{Q}$ is an elliptic curve, ℓ is an odd prime, and $\rho_{E,\ell}$ is not surjective, the image is contained in a maximal subgroup of $\mathrm{GL}_2(\ell)$. The options are:

(i) Borel subgroups, those of the shape $\left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\}$,

(ii) Normalizers of Cartan subgroups. Cartan subgroups are subgroups isomorphic to $\mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ or $\mathbb{F}_{\ell^2}^\times$.

(iii) Exceptional subgroups (projective image A_4, S_4 or A_5).

Results

Theorem (Serre, 1972)

If $\ell \geq 17$ is prime, the image of $\rho_{E,\ell}$ cannot be contained in an exceptional subgroup.

Theorem (Mazur, 1978)

The largest prime ℓ for which $\rho_{E,\ell}(G_{\mathbb{Q}})$ is contained in a Borel subgroup is 163.

Theorem (Bilu-Parent-Rebolledo, 2013)

If $\ell \geq 17$, the image cannot be contained in the normalizer of a split Cartan subgroup.

Applications of Galois representations - 1/4

• Suppose ℓ is an odd prime and $a^\ell + b^\ell = c^\ell$ with $abc \neq 0$. Let

$$E : y^2 = x(x - a^\ell)(x + b^\ell).$$

• This elliptic curve has full 2-torsion. Level-lowering gives that if $\rho_{E,\ell}$ is irreducible, it must arise from a modular form of level 2. This contradiction proves Fermat's last theorem.

• There are a number of other applications of this technique: proving that 0, 1, 8 and 144 are the only perfect powers in the Fibonacci sequence, solving generalized Fermat equations, etc.

Applications of Galois representations - 2/4

• Let p be an odd prime and suppose that $N \in \{2, 3, 7\}$ is a quadratic non-residue mod p. Let $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ and σ the non-trivial automorphism of K.

• Suppose that E/K is an elliptic curve with a cyclic N-isogeny $\lambda : E \to E^{\sigma}$ defined over K so that $\lambda(E[N]) = (\ker \lambda)^{\sigma}$.

Theorem (Shih, 1978)

Assume the notation above. Then $K(E[p])/\mathbb{Q}$ is Galois. If $\rho_{E,p}(G_K) = \{g \in \mathrm{GL}_2(p) : \det(g) \in \left(\mathbb{F}_p^{\times}\right)^2\}$, then $\mathrm{PSL}_2(\mathbb{F}_p)$ is a quotient of $\mathrm{Gal}(K(E[p])/\mathbb{Q})$.

Applications of Galois representations - 3/4

• Properties of the Weil pairing imply that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$. When are they equal?

Theorem (González-Jiménez, Lozano-Robledo, 2016)

If $E/\mathbb{Q}$ is an elliptic curve and $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n \leq 5$.

Theorem (Daniels, Lozano-Robledo)

If E is an elliptic curve and $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$ is an abelian extension of $\mathbb{Q}$ with $m \neq n$, then $m, n \in \{1, 2, 3, 4, 6\}$.

Applications of Galois representations - 4/4

- Suppose that $E/\mathbb{Q}$ is an elliptic curve, $\alpha \in E(\mathbb{Q})$, and ℓ is a prime number. What is the density of primes p for which the order of $\alpha \in E(\mathbb{F}_p)$ is coprime to ℓ?

- The order is determined by the image of $\omega_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^2 \rtimes \mathrm{GL}_2(\mathbb{Z}_\ell)$.

- If E does not have CM, $\ell = 2$ and $\alpha + T$ is not twice a point in $E(\mathbb{Q})$ for any $T \in E(\mathbb{Q})_{\mathrm{tors}}$, then the density of odd order reductions is $\geq 1/224$.

Definition

- Let H be a subgroup of $\mathrm{GL}_2(N)$ containing $-I$. The modular curve Y_H parametrizes elliptic curves with H-level structure.

- An H-level structure on $E/\overline{k}$ is an equivalence class $[\iota]_H$ where $\iota : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ is an isomorphism. We say $\iota \sim \iota'$ if $\iota = h \circ \iota'$ for some $h \in H$.

- The curve Y_H can be compactified by adding cusps X_H^∞ and one obtains a smooth projective curve $X_H = Y_H \cup X_H^\infty$.

Properties of modular curves (1/2)

• The curve X_H is geometrically connected if and only if $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

• Suppose E/k is an elliptic curve with $j(E) \neq 0, 1728$. Then, there is an isomorphism $\iota : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that $(E, [\iota]_H) \in Y_H(k)$ if and only if the image of $\rho_{E,N}$ is contained in a subgroup of $\mathrm{GL}_2(N)$ conjugate to H.

• If $H \subseteq H'$ are two subgroups, there is an induced morphism $X_H \to X_{H'}$ sending H-level structures to H'-level structures.

Properties of modular curves (2/2)

- The curve X_H has good reduction at primes not dividing N.

- If J_H is the Jacobian of X_H, Hecke operators act as endomorphisms of J_H.

Theorem (R, Sutherland, Voight, Zureick-Brown)

If $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ *is surjective, every simple factor of* J_H *is isogenous to* J_f*, for some weight* 2 *newform* f *for* $\Gamma_0(N^2) \cap \Gamma_1(N)$.

Subgroup labels

- Let H be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. We define the level of H to be the smallest positive integer N so that H contains all $M \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ with $M \equiv I \pmod{N}$.

- We assign a label to H of the form $N.i.g.n$, where N is the level of H, $i = [\mathrm{GL}_2(\hat{\mathbb{Z}}) : H]$, $g(H) =$ genus of X_H, and n is a tiebreak.

- We identify H with its image under $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(N)$.

- From Faltings's theorem, we know $X_H(\mathbb{Q})$ is finite if $g(H) \geq 2$.

Non-split Cartan subgroups (1/2)

- Let $\ell > 2$ be a prime and ϵ be a quadratic non-residue modulo ℓ.

- The ring $(\mathbb{Z}/\ell^n\mathbb{Z})[\sqrt{\epsilon}]$ is a free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 2. This gives an embedding $(\mathbb{Z}/\ell^n\mathbb{Z})[\sqrt{\epsilon}]^\times \to \mathrm{GL}_2(\ell^n)$. The image is a non-split Cartan subgroup.

- Let $N_{ns}(\ell^n)$ be its normalizer. Concretely,

$$N_{ns}(\ell^n) = \left\{ \begin{bmatrix} a & b\epsilon \\ \pm b & \pm a \end{bmatrix} : a, b \in \mathbb{Z}/\ell^n\mathbb{Z}, (a, b) \neq (0, 0) \right\}.$$

Let $X_{\mathrm{ns}}^+(\ell^n) = X_{N_{ns}(\ell^n)}$.

Non-split Cartan subgroups (2/2)

Theorem (Chen, 2004)

Up to isogeny,

$$J(X_{\mathrm{ns}}^{+}(\ell^n)) \simeq \prod_f J_f$$

where the product runs over all weight 2 newforms for $\Gamma_0(\ell^{2r})$, $0 \leq r \leq n$ with trivial character and the sign of $L(f, s)$ equal to -1.

Arithmetically maximal

- We say $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N is *arithmetically maximal* if
  - $\det(H) = \hat{\mathbb{Z}}^\times$,
  - H contains an element conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ in $\mathrm{GL}_2(N)$, and
  - $X_H(\mathbb{Q})$ is finite but $X_K(\mathbb{Q})$ is infinite for every K properly containing H.

- Our focus is on understanding $X_H(\mathbb{Q})$ for prime-power level H.

Modular curves example (1/3)

- The subgroup $N_{\mathrm{ns}}(5)$ is an index 10 maximal subgroup of $\mathrm{GL}_2(5)$.

- It has label `5.10.0.1`. The corresponding modular curve $X_{\mathrm{ns}}^{+}(5)$ has genus zero and is isomorphic to $\mathbb{P}^1$.

- If $E/\mathbb{Q}$ is an elliptic curve and $j(E) \neq 0, 1728$, then $\rho_{E,5}(G_{\mathbb{Q}}) \subseteq N_{\mathrm{ns}}(5)$ if and only if there is a rational number t so that

$$j(E) = \frac{2^{12}5^4(t-10)(t^2+5t+10)^3}{(t^2-20)^5}.$$

Modular curves example (2/3)

- The subgroup $H = \left\langle \begin{bmatrix} 3 & 4 \\ 0 & 12 \end{bmatrix}, \begin{bmatrix} 10 & 19 \\ 13 & 0 \end{bmatrix} \right\rangle \subset \mathrm{GL}_2(25)$ is an index 5 subgroup of $N_{\mathrm{ns}}(5)$.

- It has label `25.50.2.1`. The corresponding modular curve is

$$X_H : y^2 = 25x^6 + 20x^5 + 50x^4 + 50x^3 + 25x^2 + 50x - 15.$$

- The Jacobian J_H is isogenous to J_f, where f is the newform with LMFDB label `625.2.a.a`. This means that $J_H/\mathbb{Q}$ has analytic rank 2.

Modular curves example (3/3)

- The two points at infinity on X_H are rational, and their images on the j-line are $j = 0$ and $j = 2^4 \cdot 3^2 \cdot 5^7 \cdot 23^3$.

- If $E/\mathbb{Q}$ is an elliptic curve with $j(E) = 2^4 \cdot 3^2 \cdot 5^7 \cdot 23^3$, then $\rho_{E,5^\infty}(G_{\mathbb{Q}})$ has index 50 in $\mathrm{GL}_2(\mathbb{Z}_5)$.

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The only rational points on X_H are the two points at infinity.

2015 results about $\ell = 2$

Theorem (R, Zureick-Brown, 2015)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve, $H = \operatorname{im} \rho_{E,2^\infty}(G_\mathbb{Q})$ and $\overline{H} = \langle H, -I \rangle$. Then, either

- $[\mathrm{GL}_2(\mathbb{Z}_2) : \overline{H}] \leq 48$ *or*
- *$j(E)$ is in the following list:*

$$2^{11}, \quad 2^4 \cdot 17^3, \quad 4097^3/2^4, \quad 257^3/2^8, \quad -857985^3/62^8,$$
$$919425^3/496^4, \quad -3 \cdot 18249920^3/17^{16},$$
$$-7 \cdot 1723187806080^3/79^{16}.$$

Results for $\ell = 3$

Theorem (R, Sutherland, Zureick-Brown)

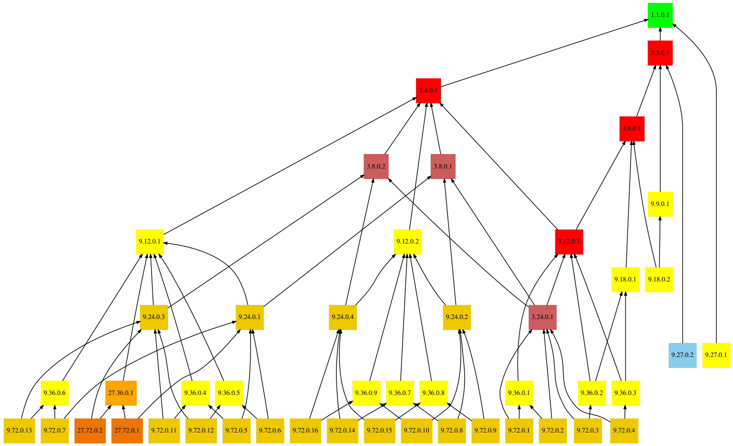
Let $E/\mathbb{Q}$ be a non-CM elliptic curve, $H = \rho_{E,3^\infty}(G_\mathbb{Q})$. Then,

- *X_H is a genus zero modular curve with infinitely many rational points, or*
- *$H \subseteq N_{\mathrm{ns}}(27)$.*

• In the first case, the index can be as large as 72 and the level as large as 27.

• We have a complete classification of $\mathrm{im}\ \rho_{E,3^\infty}$ for non-CM elliptic curves with a cyclic 3-isogeny.

3-adic images for non-CM $E/\mathbb{Q}$



Results for $\ell = 5$

Theorem

Let $E/\mathbb{Q}$ be a non-CM elliptic curve, $H = \rho_{E,5^\infty}(G_\mathbb{Q})$. Then,

- *X_H is a genus zero modular curve with infinitely many rational points, or*
- *$j(E) = 2^4 \cdot 3^2 \cdot 5^7 \cdot 23^3$ or $2^{12} \cdot 3^3 \cdot 5^7 \cdot 29^3/7^5$, or*
- *$H \subseteq N_{\mathrm{ns}}(25)$.*

• The second j-invariant listed above comes from an exceptional point on `25.75.2.1`.

Results for $\ell = 7$

Theorem

Let $E/\mathbb{Q}$ be a non-CM elliptic curve, $H = \rho_{E,7^\infty}(G_\mathbb{Q})$. Then,

- *X_H is a genus zero modular curve with infinitely many rational points, or*
- $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$, *or*
- *H is contained in a group with label 49.147.9.1 or 49.196.9.1, or*
- $H \subseteq N_{\mathrm{ns}}(49)$.

• The j-invariant above arises for an elliptic curve $E/\mathbb{Q}$ that does not have a cyclic 7-isogeny, but for which $E/\mathbb{F}_p$ does for all primes p of good reduction.

Results for $\ell = 11$

Theorem

Let $E/\mathbb{Q}$ be a non-CM elliptic curve, $H = \rho_{E,11^\infty}(G_\mathbb{Q})$. If $H \neq \mathrm{GL}_2(\mathbb{Z}_{11})$, then either

- $H = N_{\mathrm{ns}}(11)$, *or*
- $j(E) = -11^2$ *or* $-11 \cdot 131^3$, *or*
- $H \subseteq N_{\mathrm{ns}}(121)$.

- In the last case, the height of $j(E)$ is larger than about $10^{10^{200}}$.

Results for $\ell = 13$

Theorem (BC, BDMTV, K, Z)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $H = \rho_{E,13^\infty}(G_\mathbb{Q})$. Then

- *X_H is a genus zero modular curve with infinitely many rational points, or*
- *H has label `13.91.3.2` and*

$$j(E) = 2^4 \cdot 5 \cdot 13^4 \cdot 17^3/3^{13} \text{ or}$$
$$-2^{12} \cdot 5^3 \cdot 11 \cdot 13^4/3^{13} \text{ or}$$
$$13 \cdot 929 \cdot 150593365056^3/305^{13}.$$

General method

- We enumerate the arithmetically maximal subgroups H of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

- For most such H, we compute a model for X_H.

- We find all the rational points on X_H.

Fast point counting on modular curves over $\mathbb{F}_q$

- In 2015, David Zywina gave a method for counting points on $X_H/\mathbb{F}_p$ without having an equation for X_H.

- We produce a refinement of that method that counts the points on $X_H/\mathbb{F}_q$ that runs in time $\tilde{O}(q^{1/2})$ that doesn't require computing Hilbert class polynomials.

- This method allows us to compute the numerator of the zeta function for $X_H/\mathbb{F}_p$ even if the genus of X_H is moderate.

The analytic rank of J_H

- If $H \leq \mathrm{GL}_2(N)$, the simple isogeny factors of J_H have the form J_f, where f is a newform for $\Gamma_1(N^2)$ and character χ of conductor dividing N.

- Combining the fast point counting code with tabulation of newforms allows us to compute the decomposition of J_H.

- We have computed the analytic rank of J_H for every arithmetically maximal H of level ℓ^n with $\ell \leq 37$.

A genus 3 curve

- Let $X : -x^3y + x^2y^2 - xy^3 + 3xz^3 + 3yz^3 = 0$. This curve has label `27.36.3.1`. There is an automorphism $\iota : X \to X$ interchanging x and y.

- The quotient $X/\langle \iota \rangle$ is a rank one elliptic curve E. From the previous slide, $J_X \sim E \times A$ with $A/\mathbb{Q}$ having rank zero.

- We therefore have a map $\tau : X(\mathbb{Q}) \to J_X(\mathbb{Q})_{\mathrm{tors}}$ given by $\tau(P) = P - \iota(P)$. We compute $J_X(\mathbb{Q})_{\mathrm{tors}}$ and take preimages to find $X(\mathbb{Q})$.

Canonical models of modular curves (1/2)

- We use a variety of tricks to compute canonical models of higher genus modular curves by finding a basis for the space of holomorphic differentials on X_H.

- For a non-hyperelliptic curve of genus ≥ 3, the canonical ring $\bigoplus_{d \geq 0} H^0(X_H, \Omega^{\otimes d})$ is generated in degree 1.

- We find the map from X_H to the j-line by representing E_4 and E_6 as ratios of elements in the canonical ring.

Canonical models of modular curves (2/2)

• We show that E_4 is a ratio of an element of weight k and weight $k-4$ in the canonical ring if

$$k \geq \frac{2e_\infty + e_2 + e_3 + 5g - 4}{2(g-1)}.$$

• We use this method to compute the canonical models for $X_{\mathrm{ns}}^{+}(27)$, `27.729.43.1`, $X_{\mathrm{ns}}^{+}(25)$, and `25.625.36.1`.

• We can show that the modular curves corresponding to `27.729.43.1` and `25.625.36.1` have no points over $\mathbb{Q}_3$ and $\mathbb{Q}_5$, respectively.

Cases we can't handle: $X_{\mathrm{ns}}^{+}(27)$ (1/2)

• This curve has genus 12, and 8 rational CM points.

• Its Jacobian factors as a product of two simple abelian varieties of dimensions 6, each with analytic rank 6.

• There is a genus 3 modular curve X_H defined over $\mathbb{Q}(\zeta_3)$ so that $X_{\mathrm{ns}}^{+}(27) \to X_H \to X_{\mathrm{ns}}^{+}(9)$.

Cases we can't handle: $X_{\mathrm{ns}}^{+}(27)$ (2/2)

- We computed the canonical model for X_H. It has at least 13 points on it over $\mathbb{Q}(\zeta_3)$.

- We found a $D \in \mathrm{Div}^0(X_H)$ whose image in J_H has order 3 and used this to construct an étale cover of X_H.

- Each twist of the 9 twists of this étale cover maps to an elliptic curve over $\mathbb{Q}(\zeta_3)$, but one such elliptic curve has rank 2.

Cases we can't handle: $X_{\mathrm{ns}}^{+}(25)$

- We computed the canonical model for this curve. It has 8 rational CM points.

- The Jacobian factors as a product of three abelian surfaces, and one dimension 8 abelian variety.

- If there were a map from $X_{\mathrm{ns}}^{+}(25) \to C$ for a genus two curve C, we could probably use that to provably find the rational points on $X_{\mathrm{ns}}^{+}(25)$.

Cases we can't handle: 49.147.9.1

- This curve is a degree 7 cover of $X_{\mathrm{ns}}^{+}(7) \simeq \mathbb{P}^1$. We have a simple plane model of degree 7.

- Point searching finds a single rational point above $j = 0$.

- The Jacobian is irreducible with analytic rank 9. The torsion subgroup is trivial, and the curve does not have any automorphisms over $\mathbb{Q}$.

Cases we can't handle: 49.196.9.1

• This curve is a degree 7 cover of $X_{\mathrm{sp}}^{+}(7) \simeq \mathbb{P}^1$. We have a simple plane model of degree 7.

• Point searching finds a single rational point above $j = 0$.

• The Jacobian has analytic rank 9 and factors as the product of two abelian varieties of dimension 3 and 6. The torsion subgroup is trivial, and there are no automorphisms defined over $\mathbb{Q}$.

Cases we can't handle: $X_{\mathrm{ns}}^{+}(17)$ (1/3)

• Pietro Mercuri and René Schoof computed a canonical model for the genus 6 curve $X = X_{\mathrm{ns}}^{+}(17)$.

• By Chen's result, if $f \in S_2(\Gamma_0(17^2))$ is a newform with sign -1, then A_f is a factor of $J(X)$.

• Thus, there is a map $X_{\mathrm{ns}}^{+}(17) \to E$ where
$E : y^2 + xy + y = x^3 - x^2 - 199x - 510$.

• The degree of $X_0(289) \to E$ is 72. What's the degree of $X_{\mathrm{ns}}^{+}(17) \to E$?

Cases we can't handle: $X_{\text{ns}}^{+}(17)$ (2/3)

• Using a Math. Comp. paper of Cremona from 1995, we compute that the degree is 9.

• We can guess the induced map on differentials $\phi^* : \Omega_E \to \Omega_X$ and using this produce the morphism $\phi : X \to E$.

• We have $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \langle P, T \rangle$.

• The Mordell-Weil sieve shows that if $Q \in X(\mathbb{Q})$ and $\phi(Q) = kP + rT$, then either $(k, r) \in \{(-2, 0), (-1, 0), (-1, 1), (0, 0)\}$ or $|k| > 6.9 \cdot 10^{40}$.

Cases we can't handle: $X_{\mathrm{ns}}^{+}(17)$ (3/3)

• We can use the non-trivial torsion subgroup to construct an étale double cover $Y \to X$.

• This Y has genus 11 and the five-dimensional "new" piece is irreducible.

• The map $Y \to E$ ensures that $J(Y)$ has a rational 2-torsion point. Can we use this to compute the rank of $J(Y)$?

Summary

• We develop new methods to count points on $X_H/\mathbb{F}_q$ and compute the decomposition of $J(X_H)$.

• We provably find all the rational points on X_H for all ℓ-power level arithmetically maximal subgroups, with the following exceptions:

$X_{\text{ns}}^{+}(27)$, $X_{\text{ns}}^{+}(25)$, $X_{\text{ns}}^{+}(49)$, $X_{\text{ns}}^{+}(121)$, `49.147.9.1`, and `49.196.9.1`.