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

Andrew V. Sutherland

Massachusetts Institute of Technology

arXiv:2160.11141

with Jeremy Rouse and David Zureick-Brown
and an appendix with John Voight

October 24, 2021

Mazur's "Program B" (1976)

In the course of preparing my lectures for this conference, I found a proof of the following theorem, conjectured by Ogg (conjecture 1 [17b]):

THEOREM 1. *Let* Φ *be the torsion subgroup of the Mordell-Weil group of an elliptic curve* E, *over* $\mathbb{Q}$. *Then* Φ *is isomorphic to one of the following* 15 *groups:*

$$\mathbb{Z}/m\cdot\mathbb{Z} \quad \text{for} \quad m \leq 10 \quad \text{or} \quad m = 12$$

$$\mathbb{Z}/2\cdot\mathbb{Z} \times \mathbb{Z}/2\nu\cdot\mathbb{Z} \quad \text{for} \quad \nu \leq 4 \quad .$$

$\vdots$

Theorem 1 also fits into a general program:

B. *Given a number field* K *and a subgroup* H *of* $GL_2\hat{\mathbb{Z}} = \prod_p GL_2\,\mathbb{Z}_p$ *classify all elliptic curves* $E_{/K}$ *whose associated Galois representation on torsion points maps* $\mathrm{Gal}(\overline{K}/K)$ *into* $H \subset GL_2\hat{\mathbb{Z}}$.

Galois representations attached to elliptic curves

Let E be an elliptic curve over a number field K.
For each $N \geq 1$ the action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on $E[N]$ yields a Galois representation

$$\rho_{E,N}\colon G_K \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) =: \mathrm{GL}_2(N).$$

Choosing a compatible system of bases and taking the inverse limit yields

$$\rho_E\colon G_K \to \varprojlim \mathrm{GL}_2(N) \simeq \mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \prod \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Theorem (Serre 1972)

If E/k is a non-CM elliptic curve then $\rho_E(G_K)$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

There are infinitely many possibilities for $\rho_E(G_K)$, but for fixed K (or even fixed $[K:\mathbb{Q}]$) one expects only finitely many nonsurjective projections to $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to arise as E/K varies over non-CM elliptic curves and ℓ varies over primes. We consider $K = \mathbb{Q}$.

Motivations and applications

- Generalize Mazur's torsion and isogeny theorems (Mazur's "Program B").
- Diophantine problems (FLT++, perfect power Fibonacci/Lucas, . . .).
- Correct constants in asymptotics conjectures (Lang-Trotter, Koblitz-Zywina, . . .).
- Factoring integers (ECM-friendly curves).
- Inverse Galois problems ($\mathrm{PSL}_2(\mathbb{F}_p)$ for certain p, arithmetic equivalence).
- Local-global questions about elliptic curves (isogenies, torsion, . . .).
- Arithmetic dynamics (e.g. primes dividing some $a_n = (a_{n-1}a_{n-3} + a_{n-2}^2)/a_{n-4}$).
- Arithmetic statistics modulo p (cyclicity, prime order, $\#E(\mathbb{F}_p) \bmod m$, . . .).
- Arithmetic statistics of torsion fields (for $E/\mathbb{Q}$ and $E/\mathbb{Q}_\ell$).

See Rouse's VaNTAGe talk for more details on four of these, or click a highlighted link.

Coming soon to a desktop/laptop/tablet/phone near you!

Complex multiplication and reduction of abelian varieties

Talks every other Tuesday at 1pm Eastern:

- 10/26 Noam Elkies
- 11/9 Wanlin Li
- 11/23 Ananth Shankar
- 12/7 Jacob Tsimerman
- 12/14 Ben Moonen
- 1/18 Valentijn Karemaker

Zoom links on our website and researchseminars.org the day before the talk.
Lectures from previous series are available on our YouTube channel.

Prime level ℓ

Let E be an elliptic curve over $\mathbb{Q}$.
We have $\det(\rho_E(\mathrm{Frob}_p)) = p$ for every prime p, therefore $\det(\rho_E(G_\mathbb{Q})) = \widehat{\mathbb{Z}}^\times$.

If $\rho_{E,\ell}(G_\mathbb{Q}) \neq \mathrm{GL}_2(\ell)$ then it lies in a maximal subgroup of $\mathrm{GL}_2(\ell)$:

- a Borel subgroup $B(\ell)$ (conjugate to the subgroup of upper triangular matrices);
- the normalizer of Cartan subgroup (a maximal abelian subgroup), which is either split ($\simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$) or nonsplit ($\simeq \mathbb{F}_{\ell^2}^\times$);[1]
- a subgroup with projective image isomorphic to A_4, S_4, or A_5 (the cases A_4 and A_5 cannot occur over $\mathbb{Q}$).

Note that $\rho_{E,\ell}(G_k) \leq B(\ell)$ if and only if E admits a k-rational ℓ-isogeny.[2]

---

[1] For $\ell = 2$ the normalizer of the nonsplit Cartan is not a maximal subgroup because it is equal to $\mathrm{GL}_2(2)$.
[2] All inclusions and equalities of subgroups of GL_2 are understood to be up to GL_2-conjugacy.

Results and conjectures for prime level ℓ

Theorem (Serre 1972)

For $\ell > 13$ the projective image of $\rho_{E,\ell}$ is not S_4.

Theorem (Mazur 1978)

For $\ell > 163$ we have $\rho_{E,\ell}(G_{\mathbb{Q}}) \not\leq B(\ell)$, and if E is non-CM this holds for $\ell > 37$.

Theorem (Bilu, Parent, Rebolledo 2013)

For $\ell > 13$ we have $\rho_{E,\ell}(G_{\mathbb{Q}}) \not\leq N_{\rm sp}(\ell)$ if E is non-CM.

Conjecture (S 2015, Zywina 2015)

There are $3, 7, 15, 16, 7, 11, 2, 2$ proper subgroups of $\mathrm{GL}_2(\ell)$ that arise as $\rho_{E,\ell}(G_{\mathbb{Q}})$ for non-CM $E/\mathbb{Q}$ for $\ell = 2, 3, 5, 7, 11, 13, 17, 37$ respectively, and none for any other ℓ.

Subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$

To identify open subgroups $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ (up to conjugacy) we assign them unique labels.

Definition

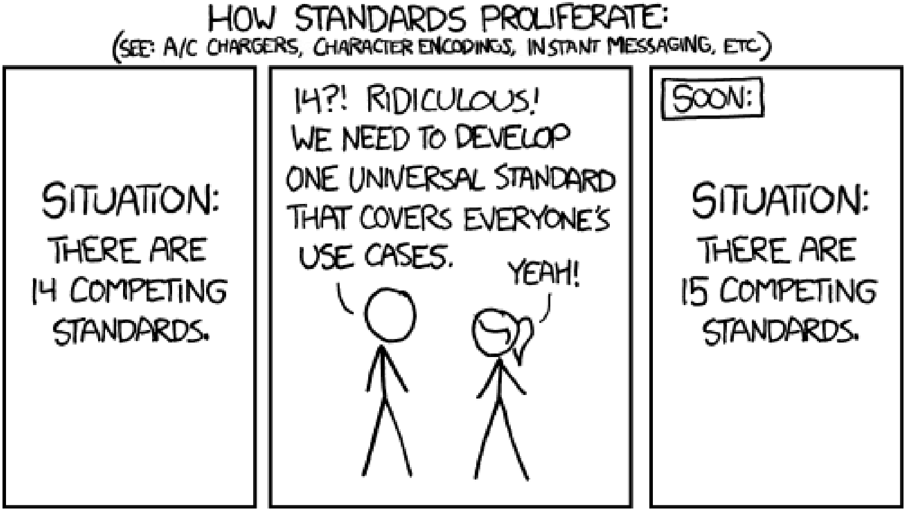
When $\det(H) = \widehat{\mathbb{Z}}^\times$ these labels have the form `N.i.g.n`, where N is the level, i is the index, g is the genus, and n is a tiebreaker given by ordering the subgroups of $\mathrm{GL}_2(N)$.

Example

- The Borel subgroup $B(13)$ has label `13.14.0.1`.
- The normalizer of the split Cartan $N_{\mathrm{sp}}(13)$ has label `13.91.3.1`.
- The normalizer of the nonsplit Cartan $N_{\mathrm{ns}}(13)$ has label `13.78.3.1`.
- The maximal S_4 exceptional group $S_4(13)$ has label `13.91.3.2`.

When $N = \ell^e$ we can also view these as labels of subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Obligatory XKCD cartoon



Results

Definition

A point $P \in X_H(K)$ is exceptional if $X_H(K)$ is finite and P corresponds to a non-CM E/K.

Theorem (Rouse, S, Zureick-Brown 2021)

Let ℓ be a prime, let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let $H = \rho_{E,\ell^\infty}(G_\mathbb{Q})$.
Exactly one of the following is true:

1. *$X_H(\mathbb{Q})$ is infinite and H is listed in (S, Zywina 2017);*
2. *X_H has a rational exceptional point listed in Table 1;*
3. *$H \leq N_{\mathrm{ns}}(3^3), N_{\mathrm{ns}}(5^2), N_{\mathrm{ns}}(7^2), N_{\mathrm{ns}}(11^2)$, or $N_{\mathrm{ns}}(\ell)$ for some $\ell > 13$;*
4. *H is a subgroup of `49.179.9.1` or `49.196.9.1`.*

We conjecture that cases (3) and (4) never occur.
If they do, the exceptional points have very large heights (e.g. $10^{10^{200}}$ for $X_{\mathrm{ns}}^+(11^2)(\mathbb{Q})$).

label	level	notes	j-invariants/models of exceptional points
16.64.2.1	2^4	$N_{\mathrm{ns}}(16)$	$-2^{18}\cdot 3\cdot 5^3\cdot 13^3\cdot 41^3\cdot 107^3/17^{16}$, $-2^{21}\cdot 3^3\cdot 5^3\cdot 7\cdot 13^3\cdot 23^3\cdot 41^3\cdot 179^3\cdot 409^3/79^{16}$
16.96.3.335	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$257^3/2^8$
16.96.3.343	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$17^3\cdot 241^3/2^4$
16.96.3.346	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$2^4\cdot 17^3$
16.96.3.338	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	2^{11}
32.96.3.230	2^5	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$-3^3\cdot 5^3\cdot 47^3\cdot 1217^3/(2^8\cdot 31^8)$
32.96.3.82	2^5	$H(8)\subsetneq N_{\mathrm{sp}}(8)$	$3^3\cdot 5^6\cdot 13^3\cdot 23^3\cdot 41^3/(2^{16}\cdot 31^4)$
25.50.2.1	5^2	$H(5)=N_{\mathrm{ns}}(5)$	$2^4\cdot 3^2\cdot 5^7\cdot 23^3$
25.75.2.1	5^2	$H(5)=N_{\mathrm{sp}}(5)$	$2^{12}\cdot 3^3\cdot 5^7\cdot 29^3/7^5$
7.56.1.2	7	$\subsetneq N_{\mathrm{ns}}(7)$	$3^3\cdot 5\cdot 7^5/2^7$
7.112.1.2	7	$-I\notin H$	$y^2+xy+y=x^3-x^2-2680x-50053$, $y^2+xy+y=x^3-x^2-131305x+17430697$
11.60.1.3	11	$\subsetneq B(11)$	$-11\cdot 131^3$
11.120.1.8	11	$-I\notin H$	$y^2+xy+y=x^3+x^2-30x-76$
11.120.1.9	11	$-I\notin H$	$y^2+xy=x^3+x^2-2x-7$
11.60.1.4	11	$\subsetneq B(11)$	-11^2
11.120.1.3	11	$-I\notin H$	$y^2+xy=x^3+x^2-3632x+82757$
11.120.1.4	11	$-I\notin H$	$y^2+xy+y=x^3+x^2-305x+7888$
13.91.3.2	13	$S_4(13)$	$2^4\cdot 5\cdot 13^4\cdot 17^3/3^{13}$, $-2^{12}\cdot 5^3\cdot 11\cdot 13^4/3^{13}$, $2^{18}\cdot 3^3\cdot 13^4\cdot 127^3\cdot 139^3\cdot 157^3\cdot 283^3\cdot 929/(5^{13}\cdot 61^{13})$
17.72.1.2	17	$\subsetneq B(17)$	$-17\cdot 373^3/2^{17}$
17.72.1.4	17	$\subsetneq B(17)$	$-17^2\cdot 101^3/2$
37.114.4.1	37	$\subsetneq B(37)$	$-7\cdot 11^3$
37.114.4.2	37	$\subsetneq B(37)$	$-7\cdot 137^3\cdot 2083^3$

Table 1. All known exceptional groups, j-invariants, and points of prime power level.

Unresolved cases

label	level	group	genus
`27.243.12.1`	3^3	$N_{\mathrm{ns}}(3^3)$	12
`25.250.14.1`	5^2	$N_{\mathrm{ns}}(5^2)$	14
`49.1029.69.1`	7^2	$N_{\mathrm{ns}}(7^2)$	69
`49.147.9.1`	7^2	$\left\langle \begin{pmatrix} 16 & 6 \\ 20 & 45 \end{pmatrix}, \begin{pmatrix} 20 & 17 \\ 40 & 36 \end{pmatrix} \right\rangle$	9
`49.196.9.1`	7^2	$\left\langle \begin{pmatrix} 42 & 3 \\ 16 & 31 \end{pmatrix}, \begin{pmatrix} 16 & 23 \\ 8 & 47 \end{pmatrix} \right\rangle$	9
`121.6655.511.1`	11^2	$N_{\mathrm{ns}}(11^2)$	511

Arithmetically maximal groups of level ℓ^n with $\ell \leq 13$ for which $X_H(\mathbb{Q})$ is unknown; each has rank $=$ genus, rational CM points, no rational cusps, and no known exceptional points.

Summary of ℓ-adic images of Galois for non-CM $E/\mathbb{Q}$.

ℓ	2	3^*	5^*	7^*	11^*	13	17^*	37^*	other*
subgroups	1208	47	25	17	8	12	3	3	1
exceptional subgroups	7	0	2	2	6	1	2	2	0
unexceptional subgroups	1201	47	23	15	2	11	1	1	1
max level	32	27	25	7	11	13	17	37	1
max index	96	72	120	112	120	91	72	114	1
max genus	3	0	2	1	1	3	1	4	0

Summary of the $H \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ which occur as $\rho_{E,\ell^\infty}(G_\mathbb{Q})$ for some non-CM elliptic curve $E/\mathbb{Q}$. Starred primes depend on the conjecture that cases (3) and (4) of our theorem do not occur.

In particular, we conjecture that there are $1207, 46, 24, 16, 7, 11, 2, 2$ proper subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ that arise as $\rho_{E,\ell^\infty}(G_\mathbb{Q})$ for non-CM $E/\mathbb{Q}$ for $\ell = 2, 3, 5, 7, 11, 13, 17, 37$ and none for any other ℓ.

Steps of the proof

1. Compute the set $\mathcal{S}$ of **arithmetically maximal** subgroups of ℓ-power level for $\ell \leq 37$ (for all $\ell > 37$ we already know $N_{\mathrm{ns}}(\ell)$ is the only possible exceptional group).
2. For $H \in \mathcal{S}$ check for **local obstructions** and compute the **isogeny decomposition** of the Jacobian of X_H and the analytic ranks of all its simple factors.
3. For $H \in \mathcal{S}$ **compute equations** for X_H and $j_H \colon X_H \to X(1)$ (if needed). In several cases we can prove $X_H(\mathbb{Q})$ is empty without a model for X_H.
4. For $H \in \mathcal{S}$ with $-I \in H$ **determine the rational points** in $X_H(\mathbb{Q})$ (if possible). In several cases we are able to exploit recent progress by others ($\ell = 13$ for example).
5. For $H \in \mathcal{S}$ with $-I \notin H$ **compute equations** for the universal curve $\mathcal{E} \to U$, where $U \subseteq X_H$ is the locus with $j(P) \neq 0, 1728, \infty$.

Arithmetically maximal groups

Definition

We say that an open subgroup $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is arithmetically maximal if

a. $\det(H) = \widehat{\mathbb{Z}}^\times$ (necessary for $\mathbb{Q}$-points),
b. a conjugate of $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$ lies in H (necessary for $\mathbb{R}$-points),
c. $j(X_H(\mathbb{Q}))$ is finite but $j(X_{H'}(\mathbb{Q}))$ is infinite for $H \subsetneq H' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Arithmetically maximal groups H arise as maximal subgroups of an H' with $X_{H'}(\mathbb{Q})$ infinite.

Theorem (S, Zywina 2017)

For $\ell = 2, 3, 5, 7, 11, 13$ there are $1208, 47, 23, 15, 2, 11$ subgroups $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of ℓ-power level with $X_H(\mathbb{Q})$ infinite, and only $H = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ for $\ell > 13$.

This allows us to compute explicit upper bounds on the level and index of arithmetically maximal subgroup of prime power level ℓ and we can then exhaustively enumerate them.

Arithmetically maximal groups

Let $\mathcal{S}_\ell^\infty(\mathbb{Q})$ denote the set of open $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of ℓ-power level with $j(X_H(\mathbb{Q}))$ infinite.
Let $\mathcal{S}_\ell(\mathbb{Q})$ denote the set of arithmetically maximal H of ℓ-power level.

ℓ	2	3	5	7	11	13	17	19	23	29	31	37
level bound	64	81	125	49	121	169	17	19	23	29	31	37
index bound	192	729	625	1372	6655	728	153	285	276	1015	496	2109
subgroups	11091	469	111	144	141	54	18	25	17	64	45	100
$\#\mathcal{S}_\ell^\infty(\mathbb{Q})$	1208	47	23	15	2	11	1	1	1	1	1	1
$\#\mathcal{S}_\ell(\mathbb{Q})$	130	19	14	10	6	10	3	4	3	4	3	4
max level	32	27	125	49	121	169	17	19	23	29	31	37
max index	96	729	625	1372	6655	182	153	285	276	1015	496	2109
max genus	7	43	36	94	511	3	7	14	15	63	30	142

Summary of arithmetically maximal $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of ℓ-power level for $\ell \le 37$.

Counting points on modular curves

For any field k of characteristic coprime to N, the noncuspidal k-rational points on $X_1(N)$ correspond to elliptic curves E/k with a rational point of order N.

Example

Over $\mathbb{F}_{37}$ there are 4 elliptic curves with a rational point of order 13:

$$\begin{aligned} y^2 &= x^3 + 4, & y^2 &= x^3 + 33x + 33, \\ y^2 &= x^3 + 8x, & y^2 &= x^3 + 24x + 22. \end{aligned}$$

What is $\#X_1(13)(\mathbb{F}_{37})$?

The genus 2 curve `169.1.169.1` is a smooth model for $X_1(13)$:

$$y^2 + (x^3 + x + 1)y = x^5 + x^4.$$

It has 23 rational points over $\mathbb{F}_{37}$. Where do these 23 points come from?

The modular curve X_H

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. The least N for which H contains the kernel of $\pi_N\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(N)$ is the level of H; it suffices to specify $\pi_N(H) \subseteq \mathrm{GL}_2(N)$.

Definition (Deligne, Rapoport 1973)

The modular curves X_H and Y_H are coarse spaces for the stacks $\mathcal{M}_H$ and $\mathcal{M}_H^0$ that parameterize elliptic curves E with H-level structure, by which we mean an equivalence class $[\iota]_H$ of isomorphisms $\iota\colon E[N] \to \mathbb{Z}(N)^2$, where $\iota \sim \iota'$ if $\iota = h \circ \iota'$ for some $h \in H$.

- $Y_H(\bar{k}) = \{(j(E), \alpha) : \alpha = Hg\mathcal{A}_E\}$ with $\mathcal{A}_E := \{\varphi_N : \varphi \in \mathrm{Aut}(E_{\bar{k}})\}$, and $Y_H(k) = Y_H(\bar{k})^{G_k}$.
- $X_H^\infty(k) = \{\alpha \in H\backslash \mathrm{GL}_2(N)/U(N) : \alpha^{\chi_N(G_K)} = \alpha\}$ where $U(N) := \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), -1\rangle$.
- $\rho_{E,N}(G_k) \le H \implies \exists \alpha (j(E), \alpha) \in Y_H(k)$ and $(j(E), \alpha) \in Y_H(k) \implies \exists \tilde{E} \rho_{\tilde{E},N}(G_k) \le H$.
- $H \le H'$ induces $X_H \to X_{H'}$; in particular, we have a map $j\colon X_H \to X(1)$ to the j-line.
- For $k = \mathbb{F}_q$, to compute $\#X_H(k) = \#Y_H(k) + \#X_H^\infty(k)$ count double cosets fixed by G_k.

The 23 $\mathbb{F}_{37}$-rational points on $X_1(13)$

Example

The four elliptic curves $E/\mathbb{F}_{37}$ with rational points of order 13 have j-invariants $0, 16, 26, 35$ (note that $1728 \equiv 26 \bmod 37$), and $\mathcal{A}_E$ is cyclic of order $6, 2, 4, 2$.

The 168 right $\mathrm{GL}_2(13)$-cosets of $B_1(13)$ correspond to the 168 points of order 13 in $E[13]$; For each E, exactly 12 are fixed by π_E, as are the corresponding double cosets. No other double cosets are fixed, so we get $12/6 + 12/2 + 12/4 + 12/2 = $ 17 non-cuspidal rational points.

The double coset space $B_1(13)\backslash \mathrm{GL}_2(13)/U(13)$ partitions $B_1(13)\backslash \mathrm{GL}_2(13)$ as $2^6 26^6$. The partitions of size 26 are fixed by $\chi_{13}(\sigma_{37}) = \left(\begin{smallmatrix} 11 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so we have 6 rational cusps.

We thus have $\#X_1(13)(\mathbb{F}_{37}) = 17 + 6 = 23$.

Computing the action of Frobenius

Theorem (Duke, Tóth 2002)

Let $E/\mathbb{F}_q$ be an elliptic curve, and let π_E denote its Frobenius endomorphism. Define $a := \operatorname{tr}\pi_E = q + 1 - \#E(\mathbb{F}_q)$ and $R := \operatorname{End}(E) \cap \mathbb{Q}(\pi_E)$, let $\Delta := \operatorname{disc}(R)$ and $\delta := \Delta \bmod 4$, and let $b := \sqrt{(a^2 - 4q)/\Delta}$ if $\Delta \neq 1$ and $b := 0$ otherwise. The integer matrix

$$A_\pi := \begin{pmatrix} (a + b\delta)/2 & b \\ b(\Delta - \delta)/4 & (a - b\delta)/2 \end{pmatrix}$$

gives the action of π_E on $E[N]$ for all $N \geq 1$.

We can compute A_π for all $E/\mathbb{F}_q$ by enumerating solutions (a, v, D) to the norm equation

$$4q = a^2 - v^2 D,$$

and making appropriate adjustments for $j(E) = 0, 1728$ and supersingular $E/\mathbb{F}_q$.
We then count the double cosets fixed by A_π with multiplicity $h(D)$.

A trivial (but still very useful) example

Consider the following arithmetically maximal group of level 49 and genus 12:

$$H := \langle \left(\begin{smallmatrix} 41 & 1 \\ 1 & 8 \end{smallmatrix}\right), \left(\begin{smallmatrix} 37 & 3 \\ 11 & 26 \end{smallmatrix}\right) \rangle \subseteq \mathrm{GL}_2(49),$$

which has label `49.168.12.1`.

None of the double cosets in $H\backslash \mathrm{GL}_2(49)/U(49)$ are fixed by $\chi_{49}(\sigma_2)$, so $\#X_H^\infty(\mathbb{F}_2) = 0$.

For the five elliptic curves $E/\mathbb{F}_2$, no double cosets in $H\backslash \mathrm{GL}_2(49)/\mathcal{A}_E$ are fixed by A_π.
It follows that $\#Y_H(\mathbb{F}_2) = 0$, and therefore $\#X_H(\mathbb{F}_2) = 0$.

The curve X_H has good reduction away from 7, and in particular at 2, so $X_H(\mathbb{Q}) = \emptyset$

There is thus no elliptic curve $E/\mathbb{Q}$ whose 7-adic image lies in H.

The same holds over any number field that has a prime with residue field $\mathbb{F}_2$.

Arithmetically maximal modular curves with local obstructions

label	level	generators	p	rank	genus
`16.48.2.17`	2^4	$\begin{pmatrix} 11 & 9 \\ 4 & 13 \end{pmatrix}, \begin{pmatrix} 13 & 5 \\ 4 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 9 \\ 12 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 9 \\ 0 & 5 \end{pmatrix}$	$3, 11$	0	2
`27.108.4.5`	3^3	$\begin{pmatrix} 4 & 25 \\ 6 & 14 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 3 & 1 \end{pmatrix}$	$7, 31$	0	4
`25.150.4.2`	5^2	$\begin{pmatrix} 7 & 20 \\ 20 & 7 \end{pmatrix}, \begin{pmatrix} 22 & 2 \\ 13 & 22 \end{pmatrix}$	2	0	4
`25.150.4.7`	5^2	$\begin{pmatrix} 24 & 24 \\ 0 & 18 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 0 & 23 \end{pmatrix}$	$3, 23$	4	4
`25.150.4.8`	5^2	$\begin{pmatrix} 8 & 4 \\ 0 & 23 \end{pmatrix}, \begin{pmatrix} 16 & 7 \\ 0 & 8 \end{pmatrix}$	2	0	4
`25.150.4.9`	5^2	$\begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 3 & 18 \\ 0 & 14 \end{pmatrix}$	2	0	4
`49.168.12.1`	7^2	$\begin{pmatrix} 39 & 6 \\ 36 & 24 \end{pmatrix}, \begin{pmatrix} 11 & 9 \\ 24 & 2 \end{pmatrix}$	2	3	12
`13.84.2.2`	13	$\begin{pmatrix} 3 & 7 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 12 & 4 \\ 0 & 12 \end{pmatrix}$	2	0	2
`13.84.2.3`	13	$\begin{pmatrix} 9 & 2 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 0 & 7 \end{pmatrix}$	3	0	2
`13.84.2.4`	13	$\begin{pmatrix} 8 & 12 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 8 & 3 \\ 0 & 9 \end{pmatrix}$	2	0	2
`13.84.2.6`	13	$\begin{pmatrix} 9 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 11 & 3 \\ 0 & 10 \end{pmatrix}$	3	0	2

Arithmetically maximal H of ℓ-power level for which $X_H(\mathbb{F}_p)$ is empty for some $p \neq \ell \leq 37$.

Decomposing the Jacobian of X_H

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N and let J_H denote the Jacobian of X_H.

Theorem (Rouse, S, Voight, Zureick-Brown 2021)

Each simple factor A of J_H is isogenous to A_f for a weight-2 eigenform f on $\Gamma_0(N^2) \cap \Gamma_1(N)$.

If we know the q-expansions of the eigenforms in $S_2(\Gamma_0(N^2) \cap \Gamma_1(N))$ we can uniquely determine the decomposition of J_H up to isogeny using linear algebra and point-counting. It suffices to work with the trace form $\mathrm{Tr}(f)$ (the sum of the Galois conjugates of f)

$$\mathrm{Tr}(f)(q) := \sum_{n=1}^{\infty} \mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}(a_n(f))q^n$$

since the integers $a_n(\mathrm{Tr}(f))$ uniquely determine $L(A_f, s)$ and the isogeny class of A_f.

By strong multiplicity one (Soundararajan 2004), the $a_p(\mathrm{Tr}(f))$ for enough $p \nmid N$ suffice.

Decomposing J_H and determining its analytic rank

Let $\{[f_1],\ldots,[f_m]\}$ be the Galois orbits of the weight-2 eigenforms for $\Gamma_0(N^2)\cap\Gamma_1(N)$. Then

$$L(J_H,s)=\prod_{i=1}^{m}L(A_{f_i},s)^{e_i}$$

for some unique vector of nonnegative integers $e(H):=(e_1,\ldots,e_i)$.

Let $T(B)\in\mathbb{Z}^{n\times m}$ have columns $[a_1(\mathrm{Tr}(f_i)),a_2(\mathrm{Tr}(f_i)),\ldots,a_p(\mathrm{Tr}(f_i)),\ldots]$ for good $p\le B$.
Let $a(H;B):=[g(H),a_2(H),\ldots,a_p(H),\ldots]$, with $a_p(H):=p+1-\#X_H(\mathbb{F}_p)$, for good $p\le B$.

For all sufficiently large B the $\mathbb{Q}$-linear system

$$T(B)x=a(H;B),$$

has the unique solution $x=e(H)$; for all the relevant H this happens with $B\le 3000$.
We can then compute the analytic rank of J_H as $\mathrm{rk}(J_H)=\sum e_i\,\mathrm{rk}(f_i)$ using the LMFDB.

An equationless Mordell-Weil sieve

We used standard techniques to determine $X_H(\mathbb{Q})$ for many arithmetically maximal H, including descent and variations of Chabauty's method, as well as leveraging prior work.

But in a few cases we had to do something different, including the group `121.605.41.1`.

In this case the curve X_H has local points everywhere, and analytic rank = genus = 41.

Reduction modulo 11 yields a map to $X_{\mathrm{ns}}^+(11)$, which is an elliptic curve of rank 1. For any set of primes S not containing 11 we have a commutative diagram

$$\begin{tikzcd}
X_H(\mathbb{Q}) \arrow[r, "\pi"] \arrow[d, "\alpha"'] & X_{\mathrm{ns}}^+(11)(\mathbb{Q}) \arrow[d, "\beta"] \\
\prod_{p\in S} X_H(\mathbb{F}_p) \arrow[r, "\pi_S"] & \prod_{p\in S} X_{\mathrm{ns}}^+(11)(\mathbb{F}_p).
\end{tikzcd}$$

We want to choose S so that the intersection of the images of β and π_S is empty.

An equationless Mordell-Weil sieve

We have the commutative diagram

$$\begin{tikzcd} X_H(\mathbb{Q}) \arrow[r, "\pi"] \arrow[d, "\alpha"'] & X_{\mathrm{ns}}^+(11)(\mathbb{Q}) \arrow[d, "\beta"] \\ \prod_{p\in S} X_H(\mathbb{F}_p) \arrow[r, "\pi_S"] & \prod_{p\in S} X_{\mathrm{ns}}^+(11)(\mathbb{F}_p). \end{tikzcd}$$

For our chosen generator $R \in X_{\mathrm{ns}}^+(11)(\mathbb{Q}) \simeq \mathbb{Z}$, we find that for $p = 13$ the image of any point in $Y_H(\mathbb{Q})$ maps to nR with $n \equiv 1, 5 \bmod 7$, which we determine by computing A_π for elliptic curves $E/\mathbb{F}_{13}$, it does not require a model for X_H the map π_S.

Similarly, for $p = 307$ any point in $Y_H(\mathbb{Q})$ maps to nR with $n \equiv 2, 3, 4, 7, 10, 13 \bmod 14$. Thus if we take $S = \{13, 307\}$ the intersection of the images of β and π_S must be empty.

Therefore $Y_H(\mathbb{Q}) = \emptyset$ (and in fact $X_H(\mathbb{Q}) = \emptyset$, there are no rational cusps).

Computing ℓ-adic images

Given a non-CM elliptic curve $E/\mathbb{Q}$ we determine $\rho_{E,\ell^\infty}(G_\mathbb{Q})$ for all primes ℓ as follows:

1. Compute a finite set S containing all ℓ for which ρ_{E,ℓ^∞} is nonsurjective (Zywina 2015).
2. Compute $A_p := A_\pi$ for good $p \le B_{\min} = 256$ and remove $\ell \in S$ for which the A_p rule out every maximal subgroup of $\mathrm{GL}_2(\ell^e)$ (where $e = 3, 2, 1, 1, \ldots$ for $\ell = 2, 3, 5, 7, \ldots$)
3. Check whether $j(E)$ is exceptional for any $\ell \in S$ (if so, record the corresponding H).
4. For all remaining $\ell \in S$:
   1. Compute A_p as needed to rule out ℓ-power H with $j(X_H(\mathbb{Q}))$ finite. (if all A_p for $p \le B_{\max} = 2^{20}$ don't suffice, compute $\rho_{\ell,\infty}(G_\mathbb{Q})$ the hard way).
   2. Having determined a set C of ℓ-power H with $j(X_H(\mathbb{Q}))$ infinite that contains $\rho_{\ell,\infty}(G_\mathbb{Q})$, use precomputed maps $j\colon X_H \to X(1)$ and universal models $\mathcal{E}_H(t)$ to determine the unique $H \in C$ of maximal index for which $\rho_{\ell,\infty}(G_\mathbb{Q}) \le H$.

Some arithmetic statistics

	nonsurjective primes									
database	2	3	5	7	11	13	17	37	none	total
LMFDB	1357468	266426	20238	3984	156	536	40	80	1467623	3058813
SW	35598552	3671444	181224	43966	2048	7444	368	1024	109142150	148168204
BHKSSW	242540	8750	400	108	0	2	44	2	238447364	238698578

	nonsurjective pairs and triples of primes								
database	$\{2,3\}$	$\{2,5\}$	$\{2,7\}$	$\{2,11\}$	$\{2,13\}$	$\{3,5\}$	$\{3,7\}$	$\{2,3,5\}$	$\{2,3,7\}$
LMFDB	53168	3354	800	148	44	788	240	564	240
SW	424566	38790	11044	2048	640	10832	3272	7904	3272
BHKSSW	382	154	62	2	22	42	16	32	16

Table: Summary of ℓ-adic image data for non-CM elliptic curves $E/\mathbb{Q}$ of conductor up to 500000 in the LMFDB, Stein-Watkins (SW), and Balakrishnan-Ho-Kaplan-Spicer-Stein-Weigandt (BHKSSW) databases. Nonsurjective counts may include curves that are also nonsurjective at another prime.

Bonus slides!

Fun facts about X_H

- X_H is a smooth proper $\mathbb{Z}[\frac{1}{N}]$-scheme with open subscheme Y_H.
  The complement X_H^∞ of Y_H in X_H is finite étale over $\mathbb{Z}[\frac{1}{N}]$.
- If $\det(H) = \widehat{\mathbb{Z}}^\times$ the generic fiber of X_H is a nice curve $X_H/\mathbb{Q}$, and $X_H(\mathbb{C})$ is the Riemann surface $X_{\Gamma_H} := \Gamma_H \backslash \mathcal{H}^*$, with $\Gamma_H \subseteq \mathrm{SL}_2(\mathbb{Z})$ the preimage of $\pi_N(H) \cap \mathrm{SL}_2(N)$.
  Note: $X_{\Gamma_H} = X_{\Gamma_{H'}} \not\Rightarrow X_H = X_{H'}$, and the levels of X_{Γ_H} and X_H may differ.
- The genus of each geometric connected component of X_H can be computed as

$$g(H) = g(\Gamma_H) = 1 + \frac{i(\Gamma_H)}{12} - \frac{e_2(\Gamma_H)}{4} - \frac{e_3(\Gamma_H)}{3} - \frac{e_\infty(\Gamma_H)}{2},$$

  where $\Gamma_H := \pm H \cap \mathrm{SL}_2(N)$, $i(\Gamma_H) := [\mathrm{SL}_2(N) : \Gamma_H]$, e_2 and e_3 count Γ_H-cosets fixed by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, respectively, and $e_\infty(\Gamma_H)$ counts $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$-orbits of $\Gamma_H \,\mathrm{SL}_2(N)$.
- If $\det(H) \neq \widehat{\mathbb{Z}}^\times$ then X_H is not geometrically connected, but it is a curve over $\mathbb{Q}$, and there is an abelian variety $J_H/\mathbb{Q}$ given by the (sheafification of) the functor $\mathrm{Pic}^0 X_H$.
  Note: The simple isogeny factors of J_H may have dimension greater than $g(H)$.

Computing canonical models of modular curves

- For a non-hyperelliptic curve of genus $g \geq 3$ the canonical ring $\mathcal{R}_H := \oplus_{d \geq 0} H^0(X_H, \Omega^{\otimes d})$ is generated in degree $d = 1$.

- To compute $j_H \colon X_H \to X(1)$ we represent E_4 and E_6 as ratios of elements of $\mathcal{R}_H$.

- We show that E_4 is a rational of an element of weight k and weight $k - 4$ whenever

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

- We used this method to compute canonical models for many curves of large genus.

- This notably includes `27.729.43.1` and `25.625.36.1`, and we were able to use these models to show they have no points over $\mathbb{Q}_3$ and $\mathbb{Q}_5$, respectively.

Quadratic twists

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and suppose $-I \in H$.

If $\rho_E(G_k) \leq H$ for an elliptic curve E/k, then $\rho_{E'}(G_k) \leq H$ for every quadratic twist $\tilde{E}$ of E.

Provided $j(E) \neq 0, 1728$, this means that

$$(E, [\iota]_H) \in X_H(k) \Longleftrightarrow j(E) \in j_H(X_H).$$

For each $H' < H$ with $\langle H', -I\rangle = H$ there is a unique $\tilde{E}$ with $\rho_{\tilde{E}}(G_k)$ H-conjugate to H'.

When $-I \in H$ it suffices to determine exceptional j-invariants, but
when $-I \notin H$ we want to identify the quadratic twists $\tilde{E}$.

If we let U be the complement of the cusps and preimages of $j = 0, 1728$ on X_H.
There is a universal curve $\mathcal{E} \to U$ such that for $j(E) \neq 0, 1728$ we have $\rho_{E,N}(G_{\mathbb{Q}}) \leq H$
if and only if $E \simeq \mathcal{E}_t$ for some $t \in U(K)$. For $U \simeq \mathbb{A}^1$, $\mathcal{E}\colon y^2 = x^3 + a(t)x + b(t)$ with $t \in \mathbb{Z}[t]$.

Performance comparison

Time to compute $\#X_0(N)(\mathbb{F}_p)$ for all primes $p \leq B$ in seconds.

	trace formula in Pari/GP v2.11				point-counting via moduli			
B	$N = 41$	42	209	210	$N = 41$	42	209	210
2^{12}	0.1	0.4	0.2	0.7	0.0	0.0	0.0	0.0
2^{13}	0.3	1.0	0.5	1.8	0.0	0.0	0.1	0.0
2^{14}	0.6	2.5	1.1	4.8	0.1	0.1	0.1	0.1
2^{15}	1.7	7.1	3.1	12.8	0.2	0.2	0.2	0.2
2^{16}	4.8	19.6	8.9	35.4	0.4	0.4	0.6	0.5
2^{17}	14.4	55.1	25.7	97.8	1.1	0.9	1.5	1.2
2^{18}	43.5	156	74.3	274	2.8	2.6	4.0	3.3
2^{19}	128	442	214	769	7.8	7.0	11.0	9.1
2^{20}	374	1260	610	2169	22.2	19.8	31.1	26.2
2^{21}	1100	3610	1760	6100	69.0	61.3	91.8	77.9
2^{22}					213	187	263	228
2^{23}					665	579	762	678
2^{24}					2060	1790	2220	1990