A database of modular curves

Andrew V. Sutherland

Massachusetts Institute of Technology

June 23, 2025

Background and context

The Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation created a database of modular curves that is now in the beta version of the L-functions and Modular Forms Database, to be expanded prior to LuCaNT. Contributors include:

> Nikola Adžaga, Eran Assaf, Jennifer Balakrishnan, Barinder Banwait, Alexander Betts, Raymond van Bommel, Shiva Chidambaram, Garen Chiloyan, Edgar Costa, Alex Cowan, Harris Daniels, Maarten Derickx, Juanita Duque-Rosero, Noam Elkies, Sachi Hashimoto, Daniel Hast, Kate Finnerty, Aashraya Jha, Asimina Hamakiotes, Steve Huang, Eray Karabiyik, Timo Keller, Jean Kieffer, Jun Bo Lau, Guido Maria Lido, David Lowry-Duda, Alvaro Lozano-Robledo, Kimball Martin, Pietro Mercuri, Philippe Michaud-Jacobs, Grant Molnar, Steffen Müller, Filip Najman, Ekin Ozman, Oana Padurariu, Bjorn Poonen, David Roe, Rakvi, Jeremy Rouse, Ciaran Schembri, Padmavathi Srinivasan, Sam Schiavone, Bianca Viray, John Voight, Borna Vukorepa, Benjamin York, and David Zywina.

This project has many disparate components, but they are all tied together by a common group-theoretic scaffold inspired by Mazur's Program B.

Mazur's 1976 lectures on *Rational points on modular curves*

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:

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

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

$$\vdots$$

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. The action of Gal_k on $E[N]$ yields

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

After choosing a compatible system of bases, taking the inverse limit yields

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

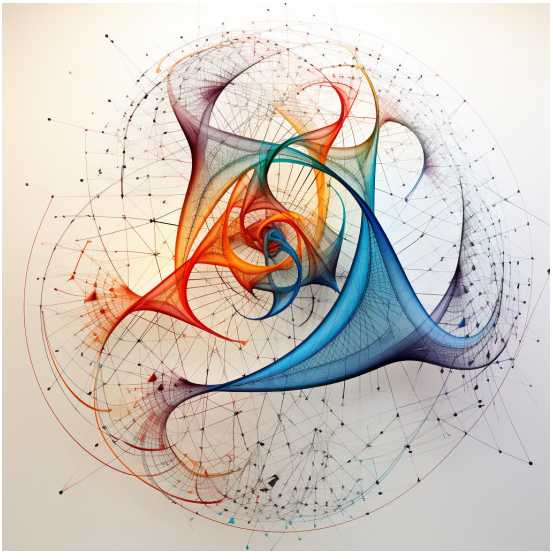
Note that ρ_E and its image are defined only up to GL_2-conjugacy.
In this talk we always work up to GL_2-conjugacy.

Theorem (Serre 1972)

If E/k is a non-CM elliptic curve then $\rho_E(\mathrm{Gal}_k)$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.
When $k = \mathbb{Q}$ the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_k)]$ is divisible by 2.

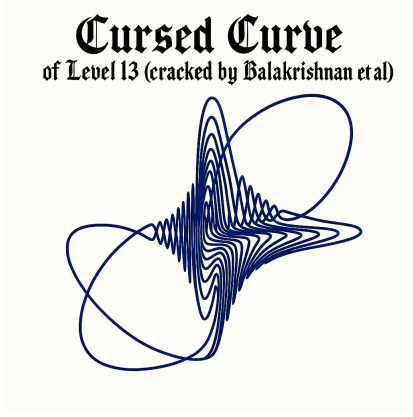
For any fixed k one expects the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_k)]$ to be bounded for non-CM E/k.
For $k = \mathbb{Q}$ the bound 2736 has been conjectured (see Zywina 2022).

The modular curve X_H



The modular curve X_H

$$y^4+5x^4-6x^2y^2+6x^3z+26x^2yz+10xy^2z-10y^3z-32x^2z^2-40xyz^2+24y^2z^2+32xz^3-16yz^3=0$$



The modular curve X_H

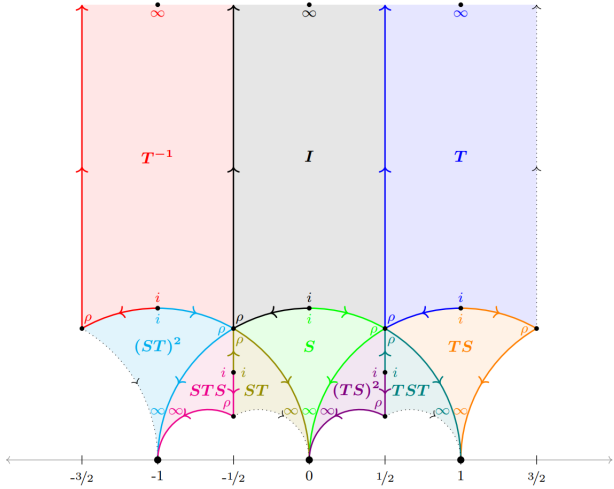
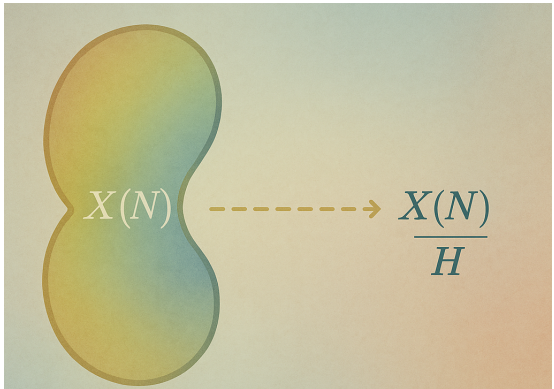


Figure 1: $\mathcal{H}^*/\Gamma$

The modular curve X_H



The quotient of the 'big' modular curve $X(N)$ by a subgroup H of its automorphism group $GL(2,Z/NZ)$.

The modular curve X_H

Definition (Deligne, Rapoport 1973)

For each open $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The modular curves X_H and Y_H are coarse spaces for the stacks $\mathcal{M}_H$ and $\mathcal{M}_H^0$ parametrizing elliptic curves E with H-level structure: equivalence classes $[\iota]_H$ of isomorphisms $\iota\colon E[N] \xrightarrow{\sim} \mathbb{Z}(N)^2$, where $\iota \sim \iota'$ if $\iota = h \circ \iota'$ for some $h \in H$.

- 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 (the cusps) 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 $\pi_N(H) \cap \mathrm{SL}_2(N)$.
  If $\det(H) \neq \widehat{\mathbb{Z}}^\times$ then X_H is not geometrically connected, but it is a curve over $\mathbb{Q}$.
- For E/k with $j(E) \neq 0, 1728$ we have $\rho_{E,N}(\mathrm{Gal}_k) \leq H \iff (E, [\iota]_H) \in Y_H(k)$.

Subgroup inclusions $H \leq H'$ induce morphisms $X_H \to X_{H'}$.
In particular, every X_H is equipped with a map $j\colon X_H \to X(1)$ to the j-line $X(1) \simeq \mathbb{P}^1$.

The three fundamental invariants: level, index, genus

For each (conjugacy class of) open $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ we define the following invariants.

- the level $n(H)$ is the least N for which H contains the kernel of $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(N)$.
- the index $i(H)$ is the positive integer $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : H] = [\mathrm{GL}_2(N) : H(N)]$.
- the genus $g(H)$ is the nonnegative integer

$$g(H) \coloneqq g(\Gamma) \coloneqq 1 + \frac{i(\Gamma)}{12} - \frac{e_2(\Gamma)}{4} - \frac{e_3(\Gamma)}{3} - \frac{e_\infty(\Gamma)}{2} \qquad \big(\Gamma := \pm H(N) \cap \mathrm{SL}_2(N)\big),$$

where $i(\Gamma) := [\mathrm{SL}_2(N) : \Gamma]$ counts right Γ-cosets in $\mathrm{SL}_2(N)$, e_2 and e_3 count 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 $e_\infty(\Gamma)$ counts $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$-orbits of $\Gamma \backslash \mathrm{SL}_2(N)$.

When $\det(H) = \widehat{\mathbb{Z}}^\times$ and $-I \in H$, the level $n(H)$ controls the bad primes of X_H, the index $i(H)$ is the degree of the map $X_H \to X(1)$, and $g(H)$ is the genus of of $X_H/\mathbb{Q}$.

If $H' \leq H$ then $n(H) | n(H')$ and $i(H) | i(H')$ and $g(H) \leq g(H')$.

A fourth fundamental invariant: Gassmann class

For subgroups H_1 and H_2 of a finite group G the following are equivalent:

- $\#(H_1 \cap C) = \#(H_2 \cap C)$ for every conjugacy class $C \subseteq G$.
- There is a conjugacy-class-preserving bijection of sets $H_1 \leftrightarrow H_2$.
- The permutation characters $\chi_{H_1} : G \to \mathbb{Z}$ and $\chi_{H_2} : G \to \mathbb{Z}$ coincide.
- The G-sets $[H_1\backslash G]$ and $[H_2\backslash G]$ are isomorphic as K-sets for every cyclic $K \leq G$.
- The permutation modules $\mathbb{Q}[H_1\backslash G]$ and $\mathbb{Q}[H_2\backslash G]$ are isomorphic as $\mathbb{Q}[G]$-modules.

Subgroups that satisfy any of these equivalent conditions are Gassmann equivalent.[1]

Open $H_1, H_2 \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ are Gassmann equivalent if $H_1(N), H_2(N) \leq \mathrm{GL}_2(N)$ are Gassmann equivalent for any N divisible by the levels of H_1 and H_2.

Proposition

For Gassmann equivalent $H_1, H_2 \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ *we have* $\mathrm{Jac}(X_{H_1}) \sim \mathrm{Jac}(X_{H_2})$.

[1] See [S21] for more on arithmetic equivalence.

Coarse and fine subgroups

Definition

Open $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contain $-I$ are coarse groups; those that do not are fine groups.
A quadratic refinement of a coarse group H is a fine group H' for which $H = \pm H'$.

A typical coarse subgroup H has infinitely many quadratic refinements H', all of which satisfy:

- $n(H)|n(H')$, $i(H') = 2i(H)$, $g(H') = g(H)$.
- $X_{H'} \simeq X_H$ (as curves); in particular $L(X_{H'}, s) = L(X_H, s)$ and $X_{H'}(k) \leftrightarrow X_H(k)$.
- $j(X_{H'}(k)) = j(X_H(k))$ for every $k/\mathbb{Q}$.

If H' is a quadratic refinement of H and E/k has Galois image $\rho_E(\mathrm{Gal}_k) = H$,
the quadratic twist $\tilde{E}/k$ by the fixed field of $\rho_E^{-1}(H')$ has Galois image $\rho_{\tilde{E}}(\mathrm{Gal}_k) = H'$.

Example

The elliptic curve `14.a4` corresponds to a point on $X_1(3)$, a quadratic refinement of $X_0(3)$.
Quadratic twists have a rational 3-isogeny, but only `14.a4` has a rational 3-torsion point.

Labels

Coarse groups $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(H) = \widehat{\mathbb{Z}}^\times$ have labels of the form `N.i.g.c.n`:

- N, i, g are the level, index, genus of H, respectively;
- c identifies the Gassmann class of H among those with label prefix `N.i.g`;
- n identifies the conjugacy class of H for those with label prefix `N.i.g.c`.

Fine groups $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(H) = \widehat{\mathbb{Z}}^\times$ have labels of the form `N.i.g-M.c.m.n`:

- N, i, g are the level, index, genus of H, respectively;
- M, c, m are components of the label `M.j.g.c.m` of $\pm H$;
- n identifies the conjugacy class of H for those with label prefix `N.i.g-M.c.m`.

Gassmann classes are ordered by lexicographically sorting characters via their values on conjugacy classes of elements ordered by similarity invariant.

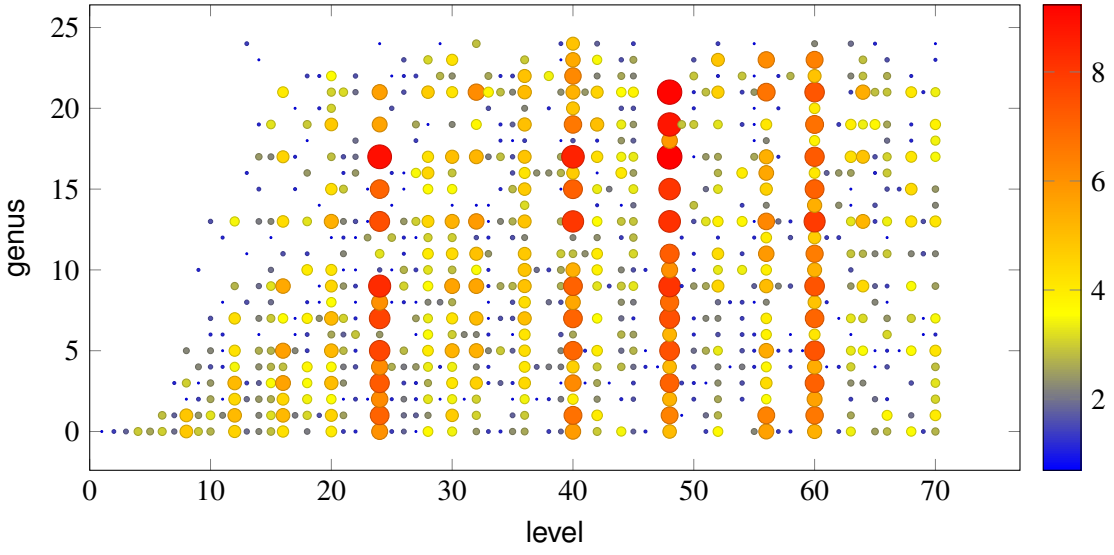
Conjugacy classes of subgroups are ordered by their canonical generators, as computed by the function `GL2CanonicalGenerators` in `gl2base.m`.

What's in the database (coming soon)

level/index/genus constraints	coarse	fine	total
$N \leq 70$	804 450	7 361 885	8 166 335
$N \leq 1000$ prime power	584 661	3 954 166	4 538 827
$g \leq 6,\ N < 840$	613 696	6 582 027	7 195 723
$g \leq 12,\ N < 480$	390 416	5 334 650	5 725 066
$g \leq g(X_1(N)),\ i \vert i(X_1(N)),\ N < 120$	783 941	11 891 829	12 675 770
$g \leq g(X_0(N)),\ i \vert i(X_0(N)),\ N < 360,\ -I \in H$	1 678 612	0	1 678 612
	4 855 776	35 124 557	39 980 333

The counts in each row exclude groups in rows above, so there is no overlap.

Coarse modular curves $X_H/\mathbb{Q}$ of level $N \leq 70$ and genus $g \leq 24$



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

For any fixed g there are only finitely many open $\Gamma \leq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ containing $-I$ with $g(\Gamma) = g$. You can find complete lists for $g \leq 24$ in the Cummins–Pauli database.[2]

By contrast, $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ contains infinitely many coarse subgroups of every genus.

For open $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(H) = \widehat{\mathbb{Z}}^\times$, the index and genus of H depend only on $\Gamma := H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$, but the levels of H and Γ may differ.

For distinct H, H' of the same level N with common intersection in $\mathrm{SL}_2(N)$, the curves X_H, $X_{H'}$ are not isomorphic. They typically have non-isgoenous Jacobians and different sets of rational points (in particular, one may be empty when the other is not!).

Example

For the groups $H =$ `15.60.2.c.1` and `15.60.2.d.1`, $H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ has CP label $15\mathrm{D}^2$.
The first X_H has no $\mathbb{Q}$-points and rank 1 $\mathrm{Jac}(X_H) \sim$ `75.c` $\times$ `225.c`.
The second $X_H = X_{ns}^+(15)$ has 6 rational $\mathbb{Q}$-points and rank 2 $\mathrm{Jac}(X_H) \sim$ `225.a` $\times$ `225.c`.

[2] Cummins and Pauli consider Γ up to $\mathrm{GL}_2(\mathbb{Z})$-conjugacy, not $\mathrm{GL}_2(\widehat{\mathbb{Z}})$-conjugacy.

Rational points on X_H

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N (which we may view as $H \leq \mathrm{GL}_2(N)$).

Definition

The set $Y_H(\bar{k})$ consists of equivalence classes $(E, [\iota]_H)$, where $(E, [\iota]_H) \sim (E', [\iota']_H)$ if there is an isomorphism $\phi\colon E \to E'$ for which $\phi_N\colon E[N] \to E'[N]$ satisfies $\iota \sim \iota' \circ \phi_N$.

Each $\sigma \in \mathrm{Gal}_K$ induces $\sigma^{-1}\colon E^\sigma[N] \xrightarrow{\sim} E[N]$ via $(x : y : z) \mapsto (\sigma^{-1}(x) : \sigma^{-1}(y) : \sigma^{-1}(z))$.
We have a Gal_k-action on $Y_H(\bar{k})$: $(E, [\iota]_H \mapsto (E^\sigma, [\iota \circ \sigma^{-1}]_H)$, and define $Y_H(k) := Y_H(\bar{k})^{\mathrm{Gal}_k}$.

Equivalently, $Y_H(\bar{k})$ is the set of pairs $(j(E), \alpha)$, with $\alpha = Hg\,\mathrm{Aut}(E_{\bar{k}}) \in H\backslash \mathrm{GL}_2 / \mathrm{Aut}(E_{\bar{k}})$, on which Gal_k acts via $(j(E), \alpha) \mapsto (j(E)^\sigma, \alpha^\sigma)$, where $\alpha^\sigma = Hg\rho_E(\sigma)\,\mathrm{Aut}(E_{\bar{k}})$.

Gal_k acts on $X_H^\infty(\bar{k}) := \pm H\backslash \mathrm{GL}_2 / \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ via $\begin{pmatrix} \chi_{\mathrm{cyc}}(\sigma) & 0 \\ 0 & 1 \end{pmatrix}$, and $X_H^\infty(k) := X_H^\infty(\bar{k})^{\mathrm{Gal}_k}$.

We now define $X_H(\bar{k}) := Y_H(\bar{k}) \sqcup X_H^\infty(\bar{k})$, and $X_H(k) := X_H(\bar{k})^{\mathrm{Gal}_k} = Y_H(k) \sqcup X_H^\infty(k)$.

Computing rational cusps (explicitly)

Given $H \leq \mathrm{GL}_2(N)$ containing $-I$ with $\det(H) = \mathbb{Z}(N)^\times$, we compute $\#X_H^\infty(\mathbb{Q})$ by counting double cosets $H \backslash \mathrm{GL}_2 / \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ fixed by all $\left(\begin{smallmatrix} g & 1 \\ 0 & 1 \end{smallmatrix}\right)$ with $g \in \mathbb{Z}(N)^\times$.

The following Magma code snippet does this:

```
R := BaseRing(H);
G := GL(2,R);
pi := CosetAction(G,H);
O := Orbits(pi(sub<G|[1,1,0,1]>));
M,cyc := MultiplicativeGroup(R);
cycgens := [G|[cyc(g),0,0,1]:g in Generators(M)];
ratcusps := [o : o in O | &and[o^g eq o :g in cycgens];
```

See the function `GL2RationalCuspCount` in `gl2base.m`.

Computing rational CM points (explicitly)

Let $E/\mathbb{Q}$ be an elliptic curve with (potential) CM by an imaginary quadratic order $\mathcal{O}$.
Let ϕ be $[\mathcal{O}_K\colon \mathcal{O}]$ if $\operatorname{disc}\mathcal{O}$ is odd and 0 otherwise, and let $\delta = (D-\phi^2)/4 \in \mathbb{Z}$.

As shown by Lozano-Robledo, for each $N \in \mathbb{Z}_{\geq 1}$, if we define

$$\mathcal{C}_{\mathcal{O}}(N) := \left\{ \left(\begin{smallmatrix} a+b\phi & b \\ \delta b & a \end{smallmatrix}\right) : a,b \in \mathbb{Z}(N), a^2+ab\phi-\delta^2 \in \mathbb{Z}(N)^\times \right\} \leq \mathrm{GL}_2(N)$$
$$\mathcal{N}_{\mathcal{O}}(N) := \left\langle \mathcal{C}_{\mathcal{O}}(N), \left(\begin{smallmatrix} -1 & 0 \\ \phi & 1 \end{smallmatrix}\right) \right\rangle$$

then $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) \leq \mathcal{N}_{\mathcal{O}}(N)$. Equality holds for all but finitely many twists of E, and we can explicitly compute the set $\mathcal{S}_{\mathcal{O}}(N)$ of subgroups of $\mathcal{N}_{\mathcal{O}}(N)$ that arise as $\rho_{E',N}(\mathrm{Gal}_{\mathbb{Q}})$ for any twist E' (including when $j(E) = 0, 1728$; see §12 of RSZB for details).

Given $H \leq \mathrm{GL}_2(N)$ we can determine the rational CM points on X_H by checking whether any $K \in \mathcal{S}_{\mathcal{O}}(N)$ is conjugate to a subgroup of H for each of the 13 $\mathcal{O}$ with $h(\mathcal{O}) = 1$.

See the function `GL2RationalCMPoints` in `gl2base.m`.

Counting rational $\mathbb{F}_q$-points on X_H (explicitly)

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

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

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

We compute $A_E = A(t, v, d)$ for all $E/\mathbb{F}_q$ by enumerating solutions (t, v, D) to

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

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

Counting rational $\mathbb{F}_q$-points on X_H (explicitly)

Given $H \leq \mathrm{GL}_2(N)$ containing $-I$ and a prime power q, compute $\#X_H(\mathbb{F}_q)$ as follows:

1. Compute the permutation character $\chi_H : \mathrm{GL}_2(N) \to \mathbb{Z}$ counting H-cosets fixed by g. which is equal to $[\mathrm{GL}_2(N) : H]\#(H \cap [g])/\#[g]$ where $[g]$ is the conjugacy class of g.
2. Compute $n_\infty := \#X_H^\infty(\mathbb{F}_q)$ by counting elements of $H \backslash \mathrm{GL}_2(N)/\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ fixed by $\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
3. Compute $n_0 := \#j_H^{-1}(0)$ and $n_{1728} := \#j_H^{-1}(1728)$ by computing A_π for each twist, summing $\chi_H(A_\pi)$ values, and dividing by $\#\operatorname{Aut}(E_{\bar{k}})$.
4. Compute $n_{\mathrm{ord}} := \sum_{t,v,D} \chi_H(A(t,v,D))h(D)$ with (t,v,D) varying over solutions to $4q = t^2 - v^2 D$ with $t \perp q$ and $D < -4$.
5. Similarly compute n_{ss} (omitting $j(E) = 0, 1728$; see [RSZB22] for details).
6. Output $\#X_H(\mathbb{F}_q) = n_\infty + n_0 + n_{1728} + n_{\mathrm{ord}} + n_{\mathrm{ss}}$.

See the function `GL2PointCount` in `gl2points.m`.

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 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 trace forms $\mathrm{Tr}(f)$ (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 the Jacobian of X_H

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 $p \leq B$.
Let $a(H; B) := [g(H), a_2(H), \ldots, a_p(H), \ldots]$, where $a_p(H)p + 1 - \#X_H(\mathbb{F}_p)$, for good $p \leq B$.

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

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

has the unique solution $x = e(H)$.

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.

Gonality bounds via point-counting

Definition

The gonality $\mathrm{gon}(X)$ of a nice curve X/k, is the minimal degree of a map to $\mathbb{P}^1_k$.
Let $d(X)$ be the least integer d for which X has infinitely many degree-d points.

Proposition (Abramovich–Harris, Frey)

For any nice curve X we have $d(X) \leq \mathrm{gon}(X) \leq 2d(X)$.
Proof: See Kadets' talk.

For modular curves X_H with $-I \in H$, the map $X_H \to X(1) \simeq \mathbb{P}^1$ has degree $i(H) \geq \mathrm{gon}(X_H)$.
If $g(X_H) > 1$ then $\mathrm{gon}(X_H) \leq 2g-2$, which improves to $\mathrm{gon}(X_H) \leq g$ when $X_H(\mathbb{Q}) \neq 0$.

We also have $\mathrm{gon}(X_H) \geq \frac{325}{32768}[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})]$ due to Abramovich (via Kim–Sarnak).
For every prime power q coprime to the level of H we have

$$\#X_H(\mathbb{F}_q) \leq \mathrm{gon}(X_H)\#X(1)(\mathbb{F}_q) \qquad \Longrightarrow \qquad \mathrm{gon}(X_H) \geq \#X_H(\mathbb{F}_q)/(q+1)$$

Gonality bounds via subgroup lattices

If $-I \in K \leq H$ then $\mathrm{gon}(X_H) \leq \mathrm{gon}(X_K) \leq [H : K]\,\mathrm{gon}(X_H)$. (see Poonen).
This allows us to propagate gonality bounds through lattices of subgroups. Even better:

Theorem (Castelnuovo–Severi inequality, Poonen, Najman–Orlić)

Let X, Y, Z be geometrically integral curves over $\mathbb{Q}$ with non-constant maps $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ of degrees d_Y, d_Z. Assume that there is no morphism $X \to X'$ of degree > 1 through which both maps factor. Let g_X, g_Y, g_Z be the genera of X, Y, Z respectively. Then

$$g_X \leq d_Y g_Y + d_Z g_Z + (d_Y - 1)(d_Z - 1) \tag{1}$$

Applying this to $X = X_K$, $Y = X_H$, $Z = X(1)$, if $d_Y = [H : K]$ is coprime to $\mathrm{gon}(X_K)$ then

$$\mathrm{gon}(X_K) \geq \frac{g(X_K) - [H : K]g(X_H)}{[H : K] - 1} + 1.$$

The gonality bounds of Kadets–Vogt may also be applicable.

Thank you for listening!