A database of modular curves

Andrew V. Sutherland
Massachusetts Institute of Technology

April 11, 2023
Background and context

Last year the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation launched a project to create a database of modular curves to become part of the $L$-functions and Modular Forms Database. Contributors include:


This project has several components. Today I will talk about just one of them, which is 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 $\phi$ be the torsion subgroup of the Mordell-Weil group of an elliptic curve $E$, over $\mathbb{Q}$. Then $\phi$ is isomorphic to one of the following 15 groups:

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

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

...:

Theorem 1 also fits into a general program:

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

Let $E$ be an elliptic curve over a number field $k$. The action of $\text{Gal}_k$ on $E[N]$ yields

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

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

$$\rho_E: \text{Gal}_k \rightarrow \varprojlim \text{GL}_2(N) \simeq \text{GL}_2(\hat{\mathbb{Z}}) \simeq \prod \text{GL}_2(\mathbb{Z}_\ell).$$

Note that $\rho_E$ and its image are defined only up to $\text{GL}_2$-conjugacy.

In this talk we will always work up to $\text{GL}_2$-conjugacy.

**Theorem (Serre 1972)**

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

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

**Definition (Deligne, Rapoport 1973)**

For each open $H \leq \text{GL}_2(\hat{\mathbb{Z}})$. 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 $\iota : E[N] \xrightarrow{\sim} \mathbb{Z}(N)^2$, 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 $X_H^\infty$ of $Y_H$ in $X_H$ (the cusps) is finite étale over $\mathbb{Z}[\frac{1}{N}]$.
- If $\det(H) = \hat{\mathbb{Z}}^\times$ 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 $\Gamma_H \subseteq \text{SL}_2(\mathbb{Z})$ the preimage of $\pi_N(H) \cap \text{SL}_2(N)$. If $\det(H) \neq \hat{\mathbb{Z}}^\times$ 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 $\rho_{E,N}(\text{Gal}_k) \leq H \iff (E, [\iota]_H) \in Y_H(k)$.

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

Three fundamental invariants: level, index, genus

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

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

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

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

When $\det(H) = \hat{\mathbb{Z}}^\times$ 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 $g(H) \leq g(H')$. 
Coarse and fine subgroups

**Definition**

Open $H \leq \text{GL}_2(\hat{\mathbb{Z}})$ 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 $H = \pm H'$.

Each coarse $H$ 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 $\rho_E(\text{Gal}_k) = H$, the quadratic twist $\tilde{E}/k$ by the fixed field of $\rho_E^{-1}(H')$ has Galois image $\rho_{\tilde{E}}(\text{Gal}_k) = H'$.

**Example**

The elliptic curve 14.a4 corresponds to a point on $X_1(3)$, a quadratic refinement of $X_0(3)$. Every twist has a rational 3-isogeny, but only 14.a4 has a rational 3-torsion point.
The determinant map

For $E/k$ the composition $\text{det} \circ \rho_E : \text{Gal}_k \to \hat{\mathbb{Z}}^\times$ factors through $\text{Gal}(k^{\text{cyc}}/k)$. For $E/\mathbb{Q}$ we have $\text{det} \circ \rho_E = \chi_{\text{cyc}}$, where $\chi_{\text{cyc}} : \text{Gal}_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character.

For $E/k$ the image $\rho_E(\text{Gal}_k)$ lies in the subgroup $\text{det}^{-1}(\chi_{\text{cyc}}(\text{Gal}_k))$ of index $[k \cap \mathbb{Q}^{\text{cyc}} : \mathbb{Q}]$. For $E/\mathbb{Q}$ the Kronecker-Weber theorem implies that if $H_E := \rho_E(\text{Gal}_{\mathbb{Q}})$ then

$$[H_E, H_E] = H_E \cap \text{SL}_2(\hat{\mathbb{Z}})$$

which is a non-trivial constraint: for most $H \in \text{GL}_2(\hat{\mathbb{Z}})$ we have $[H, H] < H \cap \text{SL}_2(\hat{\mathbb{Z}})$.

If $E/k$ has image $H_E := \rho_E(\text{Gal}_k)$ then its base change to $k^{\text{cyc}}$ has image $H_E \cap \text{SL}_2(\hat{\mathbb{Z}})$.

If $\Gamma_H := H \cap \text{SL}_2(\hat{\mathbb{Z}}) = H' \cap \text{SL}_2(\hat{\mathbb{Z}}) =: \Gamma_{H'}$ then $X_H/\mathbb{Q}^{\text{cyc}} \simeq X_{H'}/\mathbb{Q}^{\text{cyc}}$.

If $H(N) \cap \text{SL}_2(N) = H'(N) \cap \text{SL}_2(N)$ with $n(H), n(H') | N$ then $X_H/\mathbb{Q}(\zeta_N) \simeq X_{H'}/\mathbb{Q}(\zeta_N)$. 
Subgroups of $GL_2(\hat{\mathbb{Z}})$ vs subgroups of $SL_2(\hat{\mathbb{Z}})$

For any fixed $g$ there are only finitely many open $\Gamma \leq SL_2(\hat{\mathbb{Z}})$ containing $-I$ with $g(\Gamma) = g$. You can find complete lists for $g \leq 24$ in the Cummins–Pauli database.¹

By contrast, $GL_2(\hat{\mathbb{Z}})$ contains infinitely many coarse subgroups of every genus.

For open $H \leq GL_2(\hat{\mathbb{Z}})$ with $\det(H) = \hat{\mathbb{Z}}^\times$, the index and genus of $H$ depend only on $\Gamma := H \cap SL_2(\hat{\mathbb{Z}})$, but the levels of $H$ and $\Gamma$ may differ.

For distinct $H, H'$ of the same level $N$ with common intersection in $SL_2(N)$, 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 $15.60.2.d.1$, $H \cap SL_2(\hat{\mathbb{Z}})$ has CP label $15D^2$. The first $X_H$ has no $\mathbb{Q}$-points and rank 1 $\text{Jac}(X_H) \sim 75.c \times 225.c$. The second $X_H = X_{ns}^+(15)$ has 6 rational $\mathbb{Q}$-points and rank 2 $\text{Jac}(X_H) \sim 225.a \times 225.c$.

¹Cummins and Pauli consider $\Gamma$ up to $GL_2(\mathbb{Z})$-conjugacy, not $GL_2(\hat{\mathbb{Z}})$-conjugacy.
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:

$$y^2 = x^3 + 4, \quad y^2 = x^3 + 33x + 33,$$
$$y^2 = x^3 + 8x, \quad y^2 = x^3 + 24x + 22.$$ 

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 $\mathbb{F}_{37}$. Precisely where do these 23 points come from?
Rational points on $X_H$

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

**Definition**

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

Each $\sigma \in \text{Gal}_K$ induces $\sigma^{-1}: E^\sigma[N] \sim E[N]$ via $(x : y : z) \mapsto (\sigma^{-1}(x) : \sigma^{-1}(y) : \sigma^{-1}(z))$.

We have a $\text{Gal}_k$-action on $Y_H(\overline{k})$: $(E, [\iota]_H) \mapsto (E^\sigma, [\iota \circ \sigma^{-1}]_H)$, and define $Y_H(k) := Y_H(\overline{k})^{\text{Gal}_k}$.

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

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

We now define $X_H(\overline{k}) := Y_H(\overline{k}) \sqcup X_H^\infty(\overline{k})$, and $X_H(k) := X_H(\overline{k})^{\text{Gal}_k} = Y_H(k) \sqcup X_H^\infty(k)$. 
The 23 $\mathbb{F}_{37}$-rational points on $X_1(13)$

For $X_1(13)$ we have $H = \{(\frac{1}{1} \ast)\}$. Let $U := \langle (\frac{1}{0} \frac{1}{1}) \rangle$.

Example

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

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

The double coset space $\pm H(13) \backslash \text{GL}_2(13)/U(13)$ partitions $\pm H(13) \backslash \text{GL}_2(13)$ as $1^6 13^6$. The partitions of size 13 are fixed by $\chi_{13}(\sigma_{37}) = (\frac{1}{1} \frac{1}{0})$, so we have 6 rational cusps.

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

Counting $\mathbb{F}_q$-points on $X_H$

**Theorem (Duke, Tóth 2002)**

Let $E/\mathbb{F}_q$ be an elliptic curve, and let $\pi_E$ denote its Frobenius endomorphism. Define $a := \text{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$ and $R := \text{End}(E) \cap \mathbb{Q}(\pi_E)$, let $\Delta := \text{disc}(R)$ and $\delta := \Delta \mod 4$, 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 $\pi_E$ on $E[N]$ for all $N \geq 1$.

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

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

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 $h(D)$. 
The algorithm

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

1. Compute the permutation character $\chi_H : \text{GL}_2(N) \to \mathbb{Z}$ counting $H$-cosets fixed by $g$. which is equal to $[\text{GL}_2(N) : H] \#(H \cap [g]) / \# [g]$ where $[g]$ is the conjugacy class of $g$.

2. Compute $n_\infty := \#X_H^\infty(\mathbb{F}_q)$ by counting elements of $H \setminus \text{GL}_2(N)/\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ fixed by $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$.

3. Compute $n_0 := \#j_H^{-1}(0)$ and $n_{1728} := \#j_H^{-1}(1728)$ by computing $A_\pi$ for each twist, summing $\chi_H(A_\pi)$ values, and dividing by $\# \text{Aut}(E_\bar{k})$.

4. Compute $n_{\text{ord}} := \sum_{t, v, D} \chi_H(A(t, v, D)) h(D)$ with $(t, v, D)$ varying over solutions to $4q = t^2 - v^2 D$ with $t \perp q$ and $D < -4$.

5. Similarly compute $n_{ss}$ similarly (omitting $j(E) = 0, 1728$; see [RSZB22] for details).

6. Output $\#X_H(\mathbb{F}_q) = n_\infty + n_0 + n_{1728} + n_{\text{ord}} + n_{ss}$.

As written the running time of this algorithm is $\tilde{O}(N^3) + \tilde{O}(\sqrt{q})$. The $\tilde{O}(N^3)$ term is independent of $q$ and can be improved.
Performance comparison

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

<table>
<thead>
<tr>
<th>( B )</th>
<th>( N = 41 )</th>
<th>( N = 42 )</th>
<th>( N = 209 )</th>
<th>( N = 210 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^{12} )</td>
<td>0.1</td>
<td>0.4</td>
<td>0.2</td>
<td>0.7</td>
</tr>
<tr>
<td>( 2^{13} )</td>
<td>0.3</td>
<td>1.0</td>
<td>0.5</td>
<td>1.8</td>
</tr>
<tr>
<td>( 2^{14} )</td>
<td>0.6</td>
<td>2.5</td>
<td>1.1</td>
<td>4.8</td>
</tr>
<tr>
<td>( 2^{15} )</td>
<td>1.7</td>
<td>7.1</td>
<td>3.1</td>
<td>12.8</td>
</tr>
<tr>
<td>( 2^{16} )</td>
<td>4.8</td>
<td>19.6</td>
<td>8.9</td>
<td>35.4</td>
</tr>
<tr>
<td>( 2^{17} )</td>
<td>14.4</td>
<td>55.1</td>
<td>25.7</td>
<td>97.8</td>
</tr>
<tr>
<td>( 2^{18} )</td>
<td>43.5</td>
<td>156</td>
<td>74.3</td>
<td>274</td>
</tr>
<tr>
<td>( 2^{19} )</td>
<td>128</td>
<td>442</td>
<td>214</td>
<td>769</td>
</tr>
<tr>
<td>( 2^{20} )</td>
<td>374</td>
<td>1260</td>
<td>610</td>
<td>2169</td>
</tr>
<tr>
<td>( 2^{21} )</td>
<td>1100</td>
<td>3610</td>
<td>1760</td>
<td>6100</td>
</tr>
<tr>
<td>( 2^{22} )</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>( 2^{23} )</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>( 2^{24} )</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

(\(? = \text{did not complete within one day}; \text{the genus of } X_0(N) \text{ is } 3, 5, 19, 41 \text{ for } N = 41, 42, 209, 210\))
Decomposing the Jacobian of $X_H$

Let $H$ be an open subgroup of $\text{GL}_2(\hat{\mathbb{Z}})$ 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** $\text{Tr}(f)$ (the sum of the Galois conjugates of $f$)

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

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

By strong multiplicity one (Soundararajan 2004), the $a_p(\text{Tr}(f))$ 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 $[a_1(\text{Tr}(f_i)), a_2(\text{Tr}(f_i)), \ldots, a_p(\text{Tr}(f_i)), \ldots]$ 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 $\text{rk}(J_H) = \sum e_i \text{rk}(f_i)$ using the LMFDB.
Gassmann classes

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.²

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

Proposition

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

²I’m grateful to Alex Bartel for introducing me to this term. See [S21] for more on arithmetic equivalence.
Labels

Coarse groups $H \leq \GL_2(\hat{\mathbb{Z}})$ with $\det(H) = \hat{\mathbb{Z}}^\times$ 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 $H \leq \GL_2(\hat{\mathbb{Z}})$ with $\det(H) = \hat{\mathbb{Z}}^\times$ 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 \textit{similarity invariant}.

Conjugacy classes of subgroups are ordered by their \textit{canonical generators}. These also play a key role in our algorithm for enumerating open subgroups of $\GL_2(\hat{\mathbb{Z}})$.
**Similarity invariants**

Let $p^e$ be prime power. Each $A \in M_2(p^e)$ is similar\(^3\) to a matrix of the form

$$zI + p^j \begin{pmatrix} 0 & 1 \\ -d & t \end{pmatrix},$$

where the tuple of integers $\text{inv}(A) := (j, z, d, t)$ is uniquely determined by

- $j \leq e$ is the largest integer such that $A \mod p^j$ is a scalar matrix;
- $z \in [0, p^j - 1]$ satisfies $zI = A \mod p^j$.
- $d, t \in [0, p^{e-j} - 1]$ satisfy $d = \det p^{-j}(A - zI)$ and $t = \text{tr} p^{-j}(A - zI)$.

We extend this to general moduli $N = p_1^{e_1} \cdots p_n^{e_n}$ with $p_1 < \cdots < p_n$ prime via

$$\text{inv}(A) := (\text{inv}(A \mod p_1^{e_1}), \ldots, \text{inv}(A \mod p_n^{e_n})).$$

---

**Lemma**

Matrices $A, B \in \text{GL}_2(N)$ are conjugate if and only if $\text{inv}(A) = \text{inv}(B)$.

---

\(^3A\) and $B$ are similar if $EA = BE$ for some $E \in \text{GL}_2(p^e)$. See [AOPV09] for a proof of the claims above.
Canonical generators

Given an open $H \leq \text{GL}_2(\hat{\mathbb{Z}})$ we wish to choose a representative of the conjugacy class $[H]$ that $H$ represents, and generators for it in a way the depends only on $[H]$.

We first fix an ordering of $\text{GL}_2(N)$-conjugacy classes $[g]$ (rather than sorting by similarity invariant it is better to sort by decreasing $|g|$, decreasing $\# [g]$, then by similarity invariant).

The canonical generators for coarse $H \leq \text{GL}_2(\hat{\mathbb{Z}})$ of level $N$ are the lexicographically minimal sequence $h_1, \ldots, h_n \in \text{GL}_2(N)$ such that

- $H(N) \cap \text{SL}_2(N) = \langle h_1, \ldots, h_m \rangle$ for some $m \leq n$ and $H(N) = \langle h_1, \ldots, h_n \rangle$.
- $\langle h_1, \ldots, h_i \rangle < \langle h_1, \ldots, h_{i+1} \rangle$ for $1 \leq i < n$;
- $[h_1], \ldots, [h_m]$ and $[h_{m+1}], \ldots, [h_n]$ are nondecreasing (under our fixed ordering);

The canonical generators for fine $H \leq \text{GL}_2(\hat{\mathbb{Z}})$ are the sequence $\varepsilon_1 h_1, \ldots, \varepsilon_n h_n$ where $h_1, \ldots, h_n$ are canonical generators for $\pm H$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{ \pm 1 \}^n$ minimize $\sum_{i=1}^n 2^{i-1}$. 
Subgroup enumeration

1. Compute canonical generators for $\text{GL}_2(N)$, let $V^c_0 = (\text{GL}_2(N))$, $V^f_0 = \emptyset$, and $i = 0$.

2. Compute $V^c_{i+1}$, $V^f_{i+1}$, and $E^c_{i+1}$ as follows:
   a. For each $H \in V^c_i$ compute the maximal subgroups $H' < H$ with $\det(K) = \hat{\mathbb{Z}}^\times$.
   b. Compute signs $\varepsilon_i$ for each fine maximal $F < H$ and compute canonical generators.
   c. Add distinct $F$ to $V^f_{i+1}$ along with generators for $F \cap K$ for each coarse maximal $K < H$.
   d. Add coarse maximal $K < H$ to $V^c_{i+1}$ and coarse edges $(K, H)$ to $V^c_{i+1}$.

3. Compute canonical generators for $H \in V^c_{i+1}$, remove duplicates, update $E^c_{i+1}$.

4. Increment $i$ and return to step 2 if $V^c_i$ is nonempty.

5. Compute $E^f$ using signs from 2b and intersections from 2c, group by coarse parent.

6. Output $V^c := \bigcup_i V^c_i$, $V^f := \bigcup_i V^f_i$, $E^c := \bigcup_i E^c_i$, and $E^f$.

Steps 2, 3, 5 are designed to be highly parallelizable.

This description omits many details (conjugators, level-lifting, hashing, etc...).
## Lattice enumeration timings

<table>
<thead>
<tr>
<th>( N )</th>
<th>coarse groups</th>
<th>coarse edges</th>
<th>fine groups</th>
<th>fine edges</th>
<th>Magma</th>
<th>New alg (threads)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.0, 0.5, 0.5, 0.5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>0.0</td>
<td>0.1, 1.0, 1.0, 1.0</td>
</tr>
<tr>
<td>4</td>
<td>22</td>
<td>41</td>
<td>21</td>
<td>30</td>
<td>0.2</td>
<td>0.2, 1.5, 1.5, 1.6</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>19</td>
<td>6</td>
<td>4</td>
<td>0.1</td>
<td>0.2, 1.3, 1.3, 1.3</td>
</tr>
<tr>
<td>6</td>
<td>44</td>
<td>104</td>
<td>26</td>
<td>56</td>
<td>0.4</td>
<td>0.3, 1.9, 1.9, 2.0</td>
</tr>
<tr>
<td>7</td>
<td>14</td>
<td>20</td>
<td>13</td>
<td>18</td>
<td>0.1</td>
<td>0.1, 1.3, 1.3, 1.4</td>
</tr>
<tr>
<td>8</td>
<td>285</td>
<td>964</td>
<td>981</td>
<td>4764</td>
<td>939.6</td>
<td>3.4, 4.6, 4.0, 3.9</td>
</tr>
<tr>
<td>9</td>
<td>48</td>
<td>97</td>
<td>52</td>
<td>104</td>
<td>6.5</td>
<td>0.5, 2.1, 2.0, 2.1</td>
</tr>
<tr>
<td>10</td>
<td>98</td>
<td>280</td>
<td>48</td>
<td>104</td>
<td>1.8</td>
<td>0.8, 2.4, 2.4, 2.4</td>
</tr>
<tr>
<td>11</td>
<td>21</td>
<td>34</td>
<td>20</td>
<td>29</td>
<td>0.3</td>
<td>0.2, 1.4, 1.4, 1.5</td>
</tr>
<tr>
<td>12</td>
<td>767</td>
<td>3030</td>
<td>2064</td>
<td>9710</td>
<td>4066.1</td>
<td>13.2, 9.6, 6.6, 5.3</td>
</tr>
<tr>
<td>13</td>
<td>30</td>
<td>58</td>
<td>24</td>
<td>34</td>
<td>0.9</td>
<td>0.4, 1.9, 2.0, 2.1</td>
</tr>
<tr>
<td>14</td>
<td>117</td>
<td>326</td>
<td>127</td>
<td>375</td>
<td>11.0</td>
<td>1.7, 3.0, 2.6, 2.7</td>
</tr>
<tr>
<td>15</td>
<td>235</td>
<td>649</td>
<td>360</td>
<td>910</td>
<td>211.3</td>
<td>5.4, 5.3, 4.1, 3.7</td>
</tr>
<tr>
<td>16</td>
<td>1737</td>
<td>7000</td>
<td>8317</td>
<td>46944</td>
<td>256112.2</td>
<td>60.8, 36.4, 21.0, 13.9</td>
</tr>
</tbody>
</table>
Modular curves $X_H/\mathbb{Q}$ of level $N \leq 400$ and genus $g \leq 24$

<table>
<thead>
<tr>
<th>level</th>
<th>coarse $X_H/\mathbb{Q}$</th>
<th>fine $X_H/\mathbb{Q}$</th>
<th>$X_H/\mathbb{Q}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>240</td>
<td>275 184</td>
<td>5 113 941</td>
<td>5 389 125</td>
</tr>
<tr>
<td>120</td>
<td>251 423</td>
<td>2 938 971</td>
<td>3 190 394</td>
</tr>
<tr>
<td>336</td>
<td>233 684</td>
<td>4 367 741</td>
<td>4 601 425</td>
</tr>
<tr>
<td>168</td>
<td>161 247</td>
<td>2 499 153</td>
<td>2 660 400</td>
</tr>
<tr>
<td>312</td>
<td>157 819</td>
<td>2 188 045</td>
<td>2 345 864</td>
</tr>
<tr>
<td>264</td>
<td>148 031</td>
<td>2 140 707</td>
<td>2 288 738</td>
</tr>
<tr>
<td>280</td>
<td>82 433</td>
<td>947 340</td>
<td>1 029 773</td>
</tr>
<tr>
<td>48</td>
<td>43 910</td>
<td>486 297</td>
<td>530 207</td>
</tr>
<tr>
<td>360</td>
<td>28 184</td>
<td>455 652</td>
<td>483 836</td>
</tr>
<tr>
<td>24</td>
<td>23 102</td>
<td>210 057</td>
<td>233 159</td>
</tr>
<tr>
<td></td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

≈ 2 million  ≈ 23 million  ≈ 25 million
Coarse modular curves $X_{H}/\mathbb{Q}$ of level $N \leq 70$ and genus $g \leq 24$