Modular Curves in the LMFDB

David Roe

Department of Mathematics
MIT

September 21, 2023
Modular curves and Galois representations

Rational Points

Nikola Adÿaga, Jennifer Balakrishnan, Shiva Chidambaram, Garen Chiloyan, Daniel Hast, Timo Keller, Alvaro Lozano-Robledo, Pietro Mercuri, Philippe Michaud-Jacobs, Steffen Mller, Filip Najman, Ekin Ozman, Oana Padurariu, Bianca Viray, Borna Vukorepa

Database

Barinder Banwait, Jean Kieffer, David Lowry-Duda, Andrew Sutherland

Equations

Eran Assaf, Shiva Chidambaram, Edgar Costa, Juanita Duque-Rosero, Aashraya Jha, Grant Molnar, Bjorn Poonen, Rakvi, Jeremy Rouse, Ciaran Schembri, Padmavathi Srinivasan, Sam Schiavone, John Voight, David Zywina

Modular Abelian Varieties

Edgar Costa, Noam D. Elkies, Sachi Hashimoto, Kimball Martin

Demo

https://beta.lmfdb.org/ModularCurve/Q/

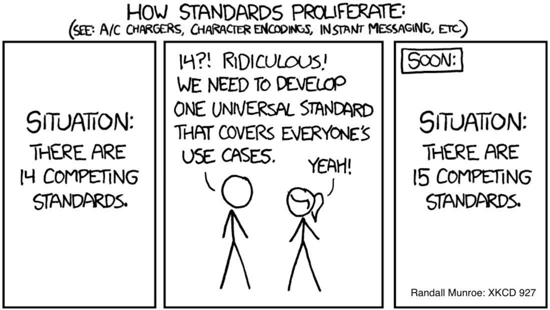
Modular Curves

- Classically, modular curves are associated to congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$, which acts on the upper half plane (the modular curve is the quotient* as a Riemann surface).
- We associate to each (conjugacy class of) open subgroup H in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ a moduli space whose points* correspond to elliptic curves with adelic Galois representation having image inside H.
- We restrict to H with surjective determinant so that the resulting curve X_H is defined over $\mathbb{Q}$.
- The *level* of H is the smallest so that H is the full preimage of its reduction modulo N.
- The *index* of H is the index inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$.
- The *genus* of H is the genus of X_H.
- A subgroup H is *coarse* if it contains $-I$, and *fine* otherwise.
- Connection with modular forms: the Jacobian of X_H decomposes* into a product of abelian varieties associated to weight 2 newforms.

Computation structure

1. For $200 < N \leq 400$, find all subgroups of $\mathrm{GL}_2(N)$ with surjective determinant up to conjugacy (with a bound on g, divided into coarse and fine subgroups), together with inclusion relationships.
2. For each coarse subgroup H, decompose $\mathrm{Jac}(X_H)$ into a product of modular abelian varieties (up to isogeny), each associated to a weight 2 newform.
3. Find models of various types – canonical, embedded, Weierstrass, conic – together with maps to the j-line.
4. Use group theory and models to get initial gonality bounds, then propagate along the modular maps.
5. Compute Galois images for elliptic curves over $\mathbb{Q}$ and over number fields, using the results to create a database of low-degree points.
6. Run a point search on the models found and a literature search to add more low-degree points.

Labels



Besides the classical curves such as $X_0(N)$ and $X_1(N)$, there are many labeling schemes in the literature:

1. Cummins-Pauli
2. Rouse and Zureick-Brown
3. Rouse, Sutherland, and Zureick-Brown
4. Sutherland
5. Sutherland and Zywina

We propose another, close to the RSZB label, which collects H together based on $\langle H, -I\rangle$ and breaks ties differently. It is possible to compute even for groups of level 336 where the RSZB label becomes infeasible.

Similarity invariants (Sutherland)

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

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

where the tuple of integers $\mathrm{inv}(A) := (j, z, d, t)$ 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 $zI \equiv A \pmod{p^j}$;
- $d, t \in [0, p^{e-j} - 1]$ satisfy $d \equiv \det p^{-j}(A - zI)$ and $t \equiv \operatorname{tr} p^{-j}(A - zI)$.

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

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

Lemma

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

Canonical generators (Sutherland)

Given an open $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$, 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 $\mathrm{GL}_2(N)$-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 $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N are the lexicographically minimal sequence $h_1, \ldots, h_n \in \mathrm{GL}_2(N)$ such that

- $H(N) \cap \mathrm{SL}_2(N) = \langle h_1, \ldots, h_m \rangle$ 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 $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ are the sequence $\epsilon_1 h_1, \ldots, \epsilon_n h_n$ where $h_1, \ldots, h_n$ are canonical generators for $\pm H$ and $\epsilon_1, \ldots, \epsilon_n \in \{\pm 1\}^n$ minimize $\sum_{\epsilon_i = 1} 2^{i-1}$.

Subgroup enumeration (Sutherland)

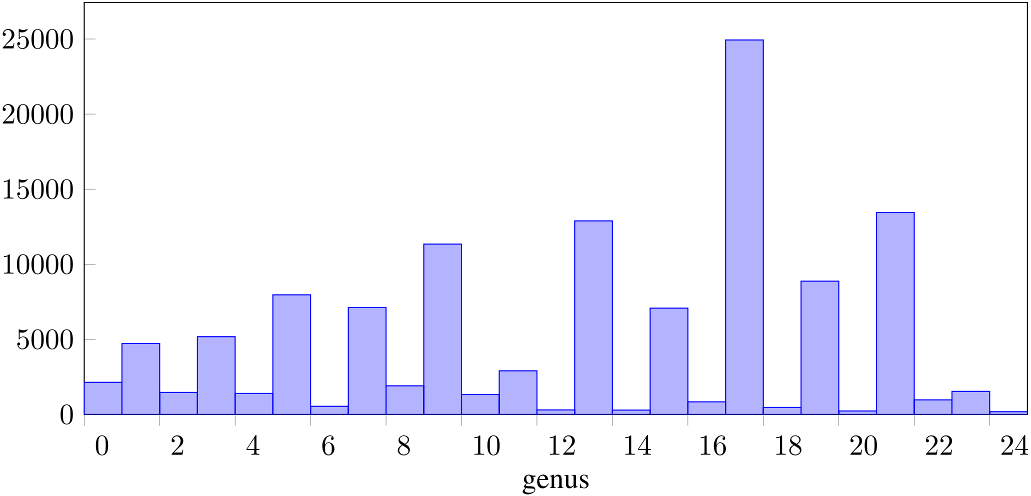
1. Compute canonical generators for $\mathrm{GL}_2(N)$, let $V_0^c = (\mathrm{GL}_2(N))$, $V_0^f = \emptyset$, and $i = 0$.
2. Compute V_{i+1}^c, V_{i+1}^f, and E_{i+1}^c as follows:
   1. For each $H \in V_i^c$ compute the maximal subgroups $H' < H$ with $\det(K) = \hat{\mathbb{Z}}^\times$.
   2. Compute signs ϵ_i for each fine maximal $F < H$ and compute canonical generators.
   3. Add distinct F to V_{i+1}^f along with generators for $F \cap K$ for each coarse maximal $K < H$.
   4. Add coarse maximal $K < H$ to V_{i+1}^c and coarse edges (K, H) to E_{i+1}^c.
3. Compute canonical generators for $H \in V_{i+1}^c$, remove duplicates, update E_{i+1}^c.
4. Compute E^f using signs from 2b and intersections from 2c, group by coarse parent.
5. Output $V^c := \bigcup_i V_i^c$, $V^f := \bigcup_i V_i^f$, $E^c := \bigcup_i E_i^c$, and E^f.

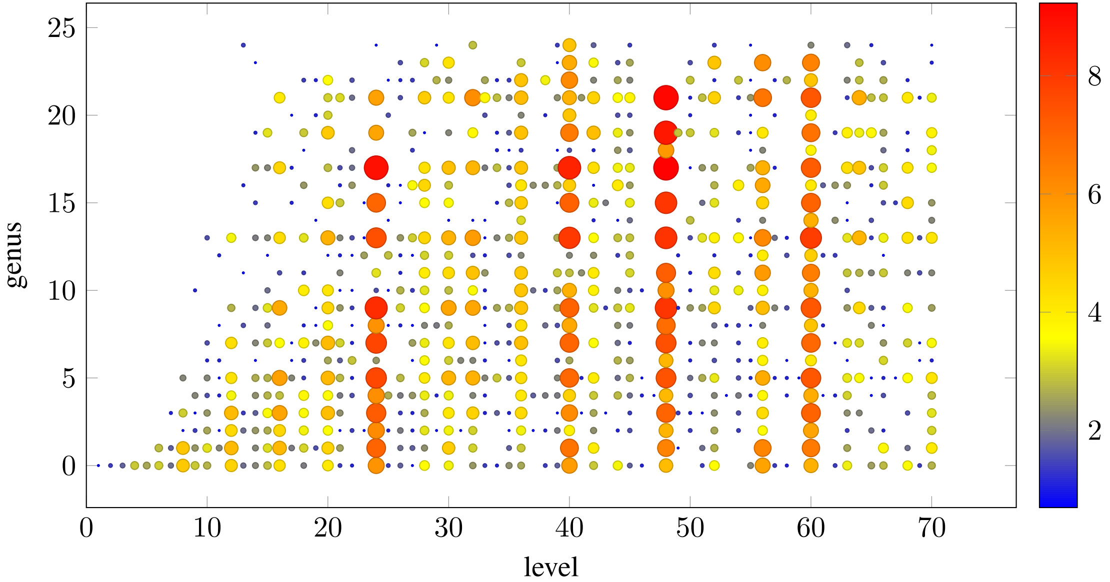
Steps 2, 3, 5 are designed to be highly parallelizable.
This description omits many details (conjugators, level-lifting, hashing, etc...).

Modular curves $X_H/\mathbb{Q}$ of level $N \le 400$ and genus $g \le 24$

level	coarse $X_H/\mathbb{Q}$	fine $X_H/\mathbb{Q}$	$X_H/\mathbb{Q}$
240	275 184	5 113 941	5 389 125
336	233 684	4 367 741	4 601 425
120	251 423	2 938 971	3 190 394
168	161 247	2 499 153	2 660 400
312	157 819	2 188 045	2 345 864
264	148 031	2 140 707	2 288 738
280	82 433	947 340	1 029 773
48	43 910	486 297	530 207
360	28 184	455 652	483 836
24	23 102	210 057	233 159
$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$\approx$ 2 million	$\approx$ 23 million	$\approx$ 25 million

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





genus
level
0
5
10
15
20
25
0
10
20
30
40
50
60
70
2
4
6
8

Models

Once the subgroup lattice inside $\mathrm{GL}_2(N)$ is computed, we compute models (for small enough genus):

1. First, compute a canonical or embedded* model of X_H by looking for relations between modular forms.
2. Then, try various strategies to find a plane model:
   1. Pick three (small) linear combinations of the coordinates and look for relations of increasing degree (as modular forms).
   2. Use Magma's representation of the function field to drop the dimension, then project (starting from rational cusps).
   3. For small genus, compute a gonal map to $\mathbb{P}^1$ and use it together with a product of coordinates to get a map to $\mathbb{P}^2$.
3. For pointless genus 0 curves, use the classification of genus 0 subgroups of $\mathrm{SL}_2(N)$ and express as a twist of a fixed curve.
4. If elliptic or hyperelliptic over $\mathbb{Q}$, use Magma to find Weierstrass model.
5. When hyperelliptic but not over $\mathbb{Q}$, express as a double cover of a pointless conic.

Maps between models

As moduli spaces, inclusions $H_1 \subset H_2$ induce modular maps $X_{H_1} \to X_{H_2}$. In particular, every X_H has a map to $X(1)$ which we call the j-map.

- When genus 0 or 1, or hyperelliptic, compute this map using the fact that the coordinates on the canonical or embedded model of X_H are defined in terms of modular forms.
- Maps between canonical models can be defined using linear polynomials, so search for linear relations when possible. Otherwise, find an absolute j-map.
- When constructing other models, track the maps.

Gonality

- Gonality bounds initially come from Abramovich (upper) and point counting via modular forms (lower).
- We can propagate these using three inequalities (applied to modular maps):
  1. If $X \to Y$ dominant has degree d then $\gamma(X) \le d\gamma(Y)$,
  2. If $X \to Y$ dominant then $\gamma(Y) \le \gamma(X)$,
  3. (Castelnuovo-Severi) If $X \to Y$ has degree d, $X \to \mathbb{P}^1$ has degree γ and $\gcd(d, \gamma) = 1$ then

$$\gamma \ge \frac{g(X) - dg(Y)}{d - 1} + 1.$$

- After improving gonalities using models, can propagate again.

Rational points

The current collection of rational and low-degree points comes from several sources:

1. Cusps, with orbits (and fields of definition) derived from the group theory and cyclotomic fields.
2. Computation of adelic Galois images for elliptic curves over $\mathbb{Q}$ (propagated using modular maps)
3. Computation of mod-ℓ Galois images for elliptic curves of number fields (propagated using modular maps)
4. For each N and CM discriminant D, computation of the minimal H of level N with CM of discriminant D (propagated using modular maps)
5. For a small set of curves, hand curated j-invariants from the literature.

Notably, we haven't yet run any kind of point search on the models we've found. Coming soon....

More demo

1. Classic search
2. Level 13
3. Point search
4. Genus vs rank
5. Trigonal curves
6. Models
7. More models
8. Lattice
9. j-map

We need you!

We hope for this database to serve as a repository of knowledge about specific modular curves. You can help in several ways.

1. Contribute to annotations for modular curves, describing connections with the literature and special features (talk to me for an LMFDB account).
2. Contribute better models (with maps to the j-line), gonality bounds, collections of low degree points, or regimes where low degree points are provably complete (with references).
3. Algorithmic advances: generalize Zywina's `OpenImage` code to number fields, or optimize canonical models to run faster for level larger than 70.
4. Help expand the scope: (modular) automorphism groups, degrees of maps to elliptic curves (bielliptic, trielliptic, etc), exceptional isomorphisms, Atkin-Lehner quotients.

Questions?