Modular Curves and Finite Groups: Building Connections Via Computation

David Roe

Department of Mathematics
MIT

January 11, 2023
Simons Collaboration on
Arithmetic Geometry, Number Theory, and Computation
Annual Meeting

Groups

Lewis Combes, John Jones, Jen Paulhus, David Roberts, Manami Roy, Sam Schiavone, Andrew Sutherland

Modcurve: 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

Modcurve: Database

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

Modcurve: 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

Modcurve: Modular Abelian Varieties

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

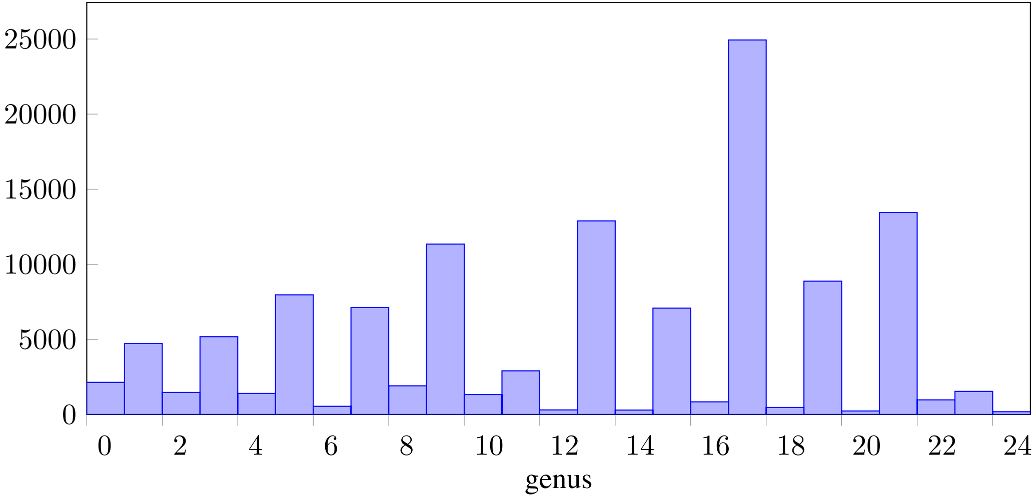
Demo

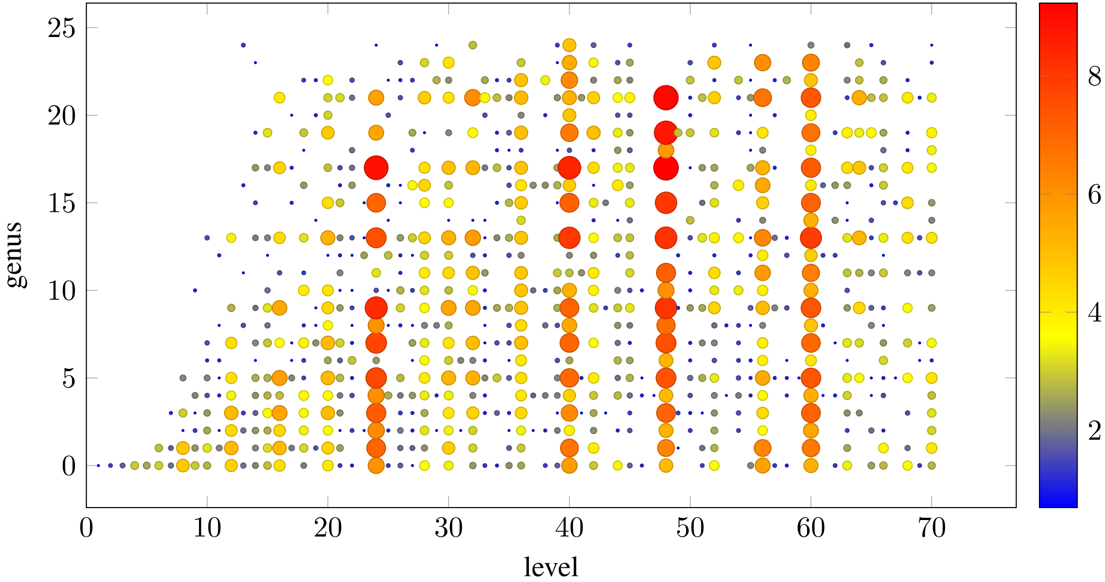
https://alpha.lmfdb.org/ModularCurve/Q/

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

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	$\approx$ 270 000	$\approx$ 3 800 000	$\approx$ 4 100 000
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
10
20
30
40
50
60
70
0
5
10
15
20
25
2
4
6
8

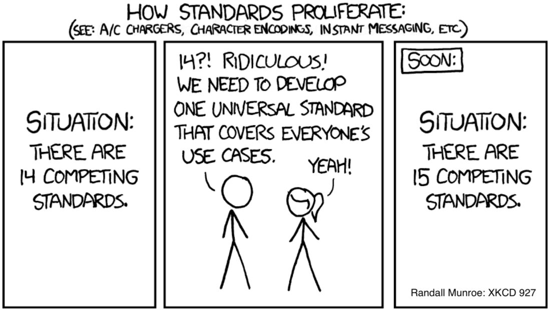
Groups in the LMFDB

	Now	Soon
Number of groups	257 936	544 802
Number of subgroups	86 898 708	?
Number of characters	11 067 588	?
Maximum order	2 000	$47! \approx 2.58 \cdot 10^{59}$
Most common orders	256, 1728, 384, 1344, 960, 1600, 576, 1440	256, 1728, 384, 1344, 960, 163840, 1600, 576
Sources	Small	Small, transitive, Lie type perfect, sporadic, $\subseteq \mathrm{GL}_n(\mathbb{F}_q)$ $\subseteq S_{15}$, $\subseteq \mathrm{GL}_2(\mathbb{Z}/N)$

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.
- Connection with modular forms: the Jacobian of X_H decomposes* into a product of abelian varieties associated to weight 2 newforms.

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.

Models

Once the subgroup lattice inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ 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 $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ 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 $\gamma(X) \leq d\gamma(Y)$,
  2. If $X \to Y$ dominant then $\gamma(Y) \leq \gamma(X)$,
  3. (Castelnuovo-Severi) If $X \to Y$ has degree d, $X \to \mathbb{P}^1$ has degree γ and $\gcd(d, \gamma) = 1$ then
$$\gamma \geq \frac{g(X) - dg(Y)}{d - 1} + 1.$$
- 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

Groups!

- Arise as: Galois groups and representations, automorphism groups of curves and lattices, component groups, in modular curves! Also in other areas of math.
- Come with additional structure (linear or permutation presentations) which change notion of equivalence.
- For abstract groups, different notions of smallness: cardinality, (transitive) permutation degree, (irreducible) linear degree (over a specific ring or field)
- Many existing tables: SmallGroup, TransitiveGroup, SimpleGroup, finite integral matrix groups, others. `groupnames.org` was great motivation.
- Representations: polycyclic, permutation, and matrix groups (avoid finitely presented).

Groups in the LMFDB

What we add

- Searchable
- Online
- Subgroup lattice gives access to relationships between groups
- Compute some harder invariants, like character tables
- Combine different sources

Difficulties

- Collecting groups up to abstract isomorphism
- For abelian groups (and others), helpful to work up to automorphism rather than conjugacy.
- Structuring code to gracefully handle timeouts and errors
- Found plenty of bugs in Magma, including a 30 year old one.

Hashing

Powerful tool for determining isomorphism classes. Need a hash that is isomorphism invariant and fast, with few collisions.

Primary hash

1. If order is identifiable by GAP or Magma, use IdentifyGroup.
2. If abelian, use abelian invariants.
3. Otherwise, use the orders and EasyHash for the maximal subgroups (up to conjugacy), where
4. EasyHash is the multiset of (order, size) for conjugacy classes.
5. Combine into a 64 bit integer.

Secondary invariants

Primary or easy hashes of Sylow subgroups, derived series, minimal normal subgroups, maximal quotients, character degrees were sometimes helpful.

Hashing (continued)

- Primary hash is clearly isomorphism invariant.
- Fast enough to compute hashes for the 408,641,062 groups of order 1536.
- Very low collision rate: 408,597,690 distinct values, with maximum cluster size 72.

Group demo

1. Boolean properties
2. Interesting groups
3. Subgroup search
4. Dynamically generated group pages
5. 144.124

Questions?