Modular Curves and Finite Groups: Building Connections Via Computation

David Roe

Department of Mathematics
MIT

March 2, 2023
COmputations and their Uses in Number Theory
CIRM - Luminy

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

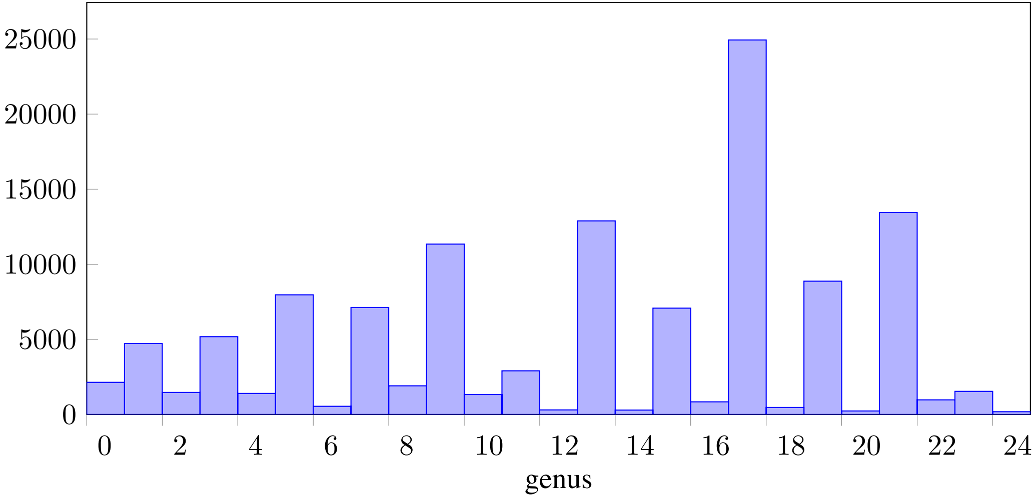
Demo

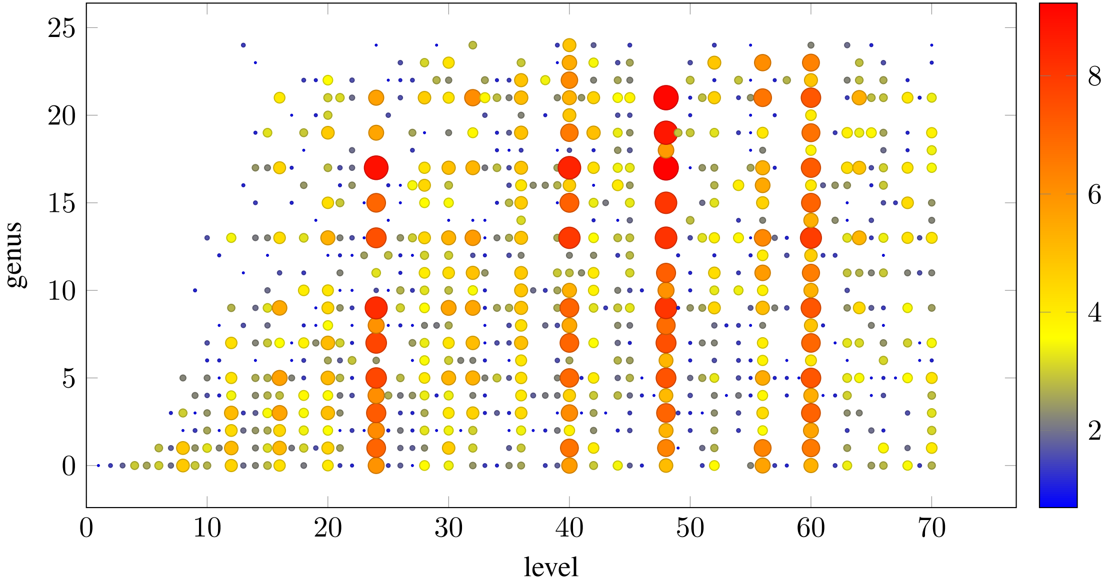
`https://alpha.lmfdb.org/ModularCurve/Q/`

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	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
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	$\approx 200,000,000$
Number of characters	11 067 588	$\approx 50,000,000$
Maximum order	2 000	$47! \approx 2.58 \cdot 10^{59}$
Most common orders	256, 1728, 384, 1344,	256, 1728, 384, 1344,
	960, 1600, 576, 1440	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 $\mathbb{Q}$.
- Three basic ingredients of the label: level, index, genus (plus tiebreakers).
- First stage: for each level, find the lattice of subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.
- Second stage: match with modular forms using point counts modulo primes.
- After the group theoretic computations: models, j-map, gonality, rational points.

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.

More demo

1. Classic search
2. Level 13
3. Point search
4. Trigonal curves
5. Homepage

Groups in the LMFDB

Sources

- SmallGroup, TransitiveGroup, SimpleGroup, finite integral matrix groups, others. `groupnames.org` was great motivation.
- Representations: polycyclic, permutation, and matrix groups (avoid finitely presented).

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, unpredictable runtime.
- Found plenty of bugs in Magma, including a 30 year old one.

Hashing

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.

Groups of order 1536

- 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. Search on size of automorphism group
2. Interesting groups
3. Subgroup search
4. 144.124

Questions?