Rational points on quotients of modular curves by Atkin-Lehner involutions

Nikola Adžaga

University of Zagreb

Representation Theory XVII, Dubrovnik

Rational Points on Modular Curves

- For $N \in \mathbb{Z}_{>0}$, the modular curve $X_1(N)$ classifies elliptic curves together with a point of order N.
- Similarly, $X_0(N)$ classifies pairs (E, C_N) of elliptic curves E together with a cyclic subgroup C_N of order N.
  This point can also be viewed as an isogeny $\iota \colon E \to E' := E/C_N$ with cyclic kernel of order N.

- Mazur (1977): Computation of $X_1(p)(\mathbb{Q})$.
- Mazur (1978): Computation of $X_0(p)(\mathbb{Q})$.

Low-degree Points on Modular Curves of Prime Level p

- Kamienny–Merel–Oesterlé (1990's): Let $[K:\mathbb{Q}] = d > 5$. Then $X_1(p)(K)$ consists only of cusps if $p > (3^{d/2}+1)^2$.
- Kamienny, Merel, Derickx–Kamienny–Stein–Stoll (2021): Computation of $X_1(p)(K)$ for $[K:\mathbb{Q}] \leq 7$.

- Open problem: Computation of $X_0(p)(K)$ for *all* K quadratic?

Atkin-Lehner Quotients

Let d be a divisor of N with $(d, N/d) = 1$.
The Atkin-Lehner involution w_d is given by

$$w_d \colon (E, C_N) \mapsto (E/C_d, (C_N + E[d])/C_d).$$

Consider the quotients

$$\begin{aligned} X_0(N)^+ &:= X_0(N)/w_N, \\ X_0(N)^* &:= X_0(N)/\langle w_d : (d, N/d) = 1 \rangle. \end{aligned}$$

Elkies' conjecture: there are only finitely many positive integers N such that $X_0(N)^*(\mathbb{Q})$ has an exceptional point (Rational points on $X_0(N)^*$ correspond to $\mathbb{Q}$-curves.)

Pictorial Example of an Atkin-Lehner Involution

Let $N = pq$ be a product of two distinct primes.
A point on $X_0(N)$ is represented by (E, C_N) or, equivalently, by an isogeny $\iota\colon E \to E/C_N$, where C_N is a cyclic subgroup.

$$
\begin{tikzcd}
 & E \arrow[dl, bend right, "\phi"'] \arrow[dr, bend left, "\psi"] \arrow[dd, "\iota"] & \\
E/C_p \arrow[ur, bend right, "\phi^\vee"'] \arrow[rr, dashed, "w_p(\iota)"'] \arrow[dr] & & E/C_q \arrow[ul, bend left, "\psi^\vee"] \arrow[dl] \\
 & E' \cong E/C_N &
\end{tikzcd}
$$

The Chabauty-Coleman Method

The setup:

1. Let g be the genus of X and r the Mordell-Weil rank of its Jacobian J
2. Use a basepoint $x_0 \in X(\mathbb{Q})$ to embed $X \hookrightarrow J, x \mapsto [x - x_0]$.
3. Let p be a prime of good reduction for X.

- If $r < g$, we use the classical Chabauty-Coleman method: There exists an $0 \neq \omega \in \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1)$ such that

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_1 := \left\{ x \in X(\mathbb{Q}_p) : \int_{x_0}^{x} \omega = 0 \right\} \subseteq X(\mathbb{Q}_p).$$

- The set $X(\mathbb{Q}_p)_1$ is finite and computable if we know a finite index subgroup G of $J(\mathbb{Q})$.

The Quadratic Chabauty Method

- Same setup.
- There is a global p-adic height $h\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$, which decomposes into local heights

$$h = h_p + \sum_{\ell \neq p} h_\ell.$$

- $\rho = h - h_p$ is locally analytic, and the h_ℓ have finite image on $X(\mathbb{Q})$ depending on the reduction at ℓ.
- If $r = g$, we use the quadratic Chabauty method (depending on modularity):

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_2 := \left\{x \in X(\mathbb{Q}_p) : h(x) - h_p(x) \in \Upsilon\right\} \subseteq X(\mathbb{Q}_p),$$

where $\Upsilon = \{0\}$ if all $h_\ell = 0$ for $\ell \neq p$.

Low genus $X_0^+(N)$ for prime levels N

joint work with Arul, Beneish, Chen, Chidambaram, Keller, Wen

Modular interpretation of $X_0^+(N)(\mathbb{Q})$

The modular curve $X_0^+(N)$ parametrizes pairs of elliptic curves together with a cyclic isogeny of degree N.

The $\mathbb{Q}$-rational points on $X_0^+(N)$ are

- cusp
- CM points
- the exceptional points

The canonical models of $X_0^+(N)$ were found in Galbraith's thesis and his subsequent work. Crucial: $\Omega^1(X_0(N)) \cong S_2(\Gamma_0(N))$.

Curves $X_0^+(N)$ typically satisfy that the rank of their Jacobian r is equal to their genus g.

Finding our levels

Proposition

Denote by $g_0^+(N)$ the genus of $X_0^+(N)$. Then

$$g_0^+(N) \geq \frac{N - 5\sqrt{N} + 4}{24} - \frac{\sqrt{N}}{\pi}(\ln(16N) + 2).$$

This lower bounds exceeds 6 when $N > 13300$.

Our levels

For prime level N, the curve $X_0^+(N)$ has genus 4 if and only if

$$N \in \{137, 173, 199, 251, 311\}.$$

It has genus 5 if and only if

$$N \in \{157, 181, 227, 263\},$$

and it has genus 6 if and only if

$$N \in \{163, 197, 211, 223, 269, 271, 359\}.$$

QC: assumptions and input

Input:

- a plane affine patch $Y : Q(x, y) = 0$ of a modular curve $X/\mathbb{Q}$ that satisfies $r = g \geq 2$ and is monic in y
- a prime p of good reduction for $X/\mathbb{Q}$ such that the Hecke operator T_p generates $\mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Canonical models – genus 2 and 3

Genus 2 curves are hyperelliptic curves.

Genus 3 curve is a hyperelliptic curve or a smooth plane quartic.

The set of $\mathbb{Q}$-rational points on genus 2 and 3 curves $X_0^+(N)$ for prime N was provably determined by Balakrishnan–Dogra–Müller–Tuitman–Vonk [2].

Canonical models – genus 4 – 6

Hyperelliptic curves can have arbitrary genus, but the curves $X_0^+(N)$ of genus $4-6$ for prime N are not hyperelliptic.

Genus 4 curve is an intersection of a quadric and a cubic in $\mathcal{P}^3$.

Genus 5 curve is a complete intersection of 3 quadrics in $\mathcal{P}^4$.

(Our) genus 6 curve is a complete intersection of 6 quadrics in $\mathcal{P}^5$.

From canonical models to plane models I

Start: the image of $X_0^+(N)$ in $\mathcal{P}^{g-1}$.

Goal: a suitable plane model.

We find two rational maps $\tau_x, \tau_y \colon X_0^+(N) \to \mathcal{P}^1$ such that the product

$$\tau_x \times \tau_y \colon X_0^+(N) \to \mathcal{P}^1 \times \mathcal{P}^1$$

is a birational map onto its image.

From canonical models to plane models II

Compose with the Segre embedding $\mathcal{P}^1 \times \mathcal{P}^1 \to \mathcal{P}^3_{[w:x:y:z]}$, and then project from the point $[1: 0: 0: 0]$ onto the plane $w = 0$.

$$\varphi' \colon X_0^+(N) \xrightarrow{\tau_x \times \tau_y} \mathcal{P}^1 \times \mathcal{P}^1 \xrightarrow{\text{Segre}} \mathcal{P}^3_{[w:x:y:z]} \xrightarrow{\text{projection}} \mathcal{P}^2_{[x:y:z]}.$$

From canonical models to plane models III

Write $\tau_x(q) = [x_1(q) : x_2(q)]$ and $\tau_y(q) = [y_1(q) : y_2(q)]$. Then the equation for φ' is

$$\varphi' \colon q \mapsto [(x_1 y_2)(q) \colon (x_2 y_1)(q) \colon (x_2 y_2)(q)].$$

When $x_2(q), y_2(q) \neq 0$, this is just

$$\varphi' \colon q \mapsto [(x_1/x_2)(q) : (y_1/y_2)(q) : 1].$$

The image $\mathcal{C}'_N := \varphi'(X_0^+(N))$ will be a curve given by an equation of the form

$$Q_0(x,z)y^d + Q_1(x,z)y^{d-1} + \cdots + Q_d(x,z) = 0,$$

Multiply by Q_0^{d-1} to get

$$(Q_0(x,z)y)^d + Q_1(x,z)(Q_0(x,z)y)^{d-1} + \cdots + Q_0(x,z)^{d-1}Q_d(x,z) = 0,$$

After substitution $y = Q_0(x,z)y$, the affine patch given by $z = 1$ will have an equation $Q(x,y) = 0$ where $Q(x,y)$ is a polynomial over $\mathbb{Q}$ monic in y, suitable for QC.

From canonical models to plane models – An example

Canonical model for $X_0^+(137)$ is

$$XY + WY + 2Y^2 + 2WZ + XZ + 6YZ + 3Z^2 = 0,$$

$$X^3 + WX^2 + 6X^2Z - 2XY^2 - 5XYZ + XZW + 13XZ^2 + 2Y^3$$
$$+ 3WY^2 + W^2Y + 3WYZ - 6YZ^2 + ZW^2 - 4Z^2W + 14Z^3 = 0,$$

The map we use is given by
$x_1 = Z, x_2 = Y,\ y_1 = 42Z, y_2 = W + X + 2Y + Z.$

QC application

Our `model_equation_finder` takes this map as an input, together with the canonical model.

The image curve is

$$\begin{aligned} y^3 &+ (50x^3 + 32x^2 - 4x - 3)y^2 \\ &+ (966x^6 + 1377x^5 + 459x^4 - 115x^3 - 66x^2 + x + 2)y \\ &+ (7056x^9 + 16128x^8 + 12744x^7 + 2856x^6 \\ &\quad - 1239x^5 - 678x^4 - 35x^3 + 28x^2 + 4x) = 0. \end{aligned}$$

Classification of points on $X_0^+(137)$

Nine known rational points are

Cusp, $[1: 0: 0: 0]$
$D = -4$, $[2: -4: -3: 2]$
$D = -7$, $[2: -1: -2: 1]$
$D = -8$, $[1: -1: 0: 0]$
$D = -11$, $[1: 1: -1: 0]$
$D = -16$, $[2: 0: -1: 0]$
$D = -19$, $[1: -2: -1: 1]$
$D = -28$, $[0: 1: 2: -1]$
Exceptional, $[19: 2: -16: 4]$

Using the plane model $Q = 0$ and prime 5, QC confirms that the images of these 9 points are the only $\mathbb{Q}$-rational points outside the disk at infinity.

The main result on $X_0^+(N)$

Theorem (AABCCKW, 2022+)

For prime level N, the only curves $X_0^+(N)$ of genus 4 that have exceptional rational points are $X_0^+(137)$ and $X_0^+(311)$. For prime level N, there are no exceptional rational points on curves $X_0^+(N)$ of genus 5 and 6.

Comment about exceptional points

Bars and Gonzalez have determined the automorphism group of $X_0(N)^*$:

Theorem (Bars–Gonzalez, 2021)

Let N be a square-free integer such that the curve $X_0(N)^*$ has genus greater than 3 and is not bielliptic, i.e. $N \neq 370$. Then, the group $\mathrm{Aut}(X_0(N)^*)$ is not trivial if and only if $N \in \{366, 645\}$. (In both cases, the order of this group is 2 and the genus of the quotient curve by the non trivial involution is 2.)

For our (prime) levels, already Baker and Hasegawa (2003) determined this group.

Hyperelliptic curves $X_0(N)^*$

joint work with Chidambaram, Keller, Padurariu

All Hyperelliptic Quotients

Theorem (Hasegawa, 1997)

There are 64 values of N for which $X_0(N)^*$ is hyperelliptic.

Of these, there are only 7 values of N for which $X_0(N)^*$ is hyperelliptic with genus $g \geq 3$, namely

$$\begin{aligned} g = 3: &\quad 136, 171, 207, 252, 315, \\ g = 4: &\quad 176, \\ g = 5: &\quad 279. \end{aligned}$$

Genus 2 Levels

For the following levels N the curve $X_0(N)^*$ has genus 2:

67,	73,	85,	88,	93,	103,	104,	106,	107,	112,
115,	116,	117,	121,	122,	125,	129,	133,	134,	135,
146,	147,	153,	154,	158,	161,	165,	166,	167,	168,
170,	177,	180,	184,	186,	191,	198,	204,	205,	206,
209,	213,	215,	221,	230,	255,	266,	276,	284,	285,
286,	287,	299,	330,	357,	380,	390.			

Genus 2 Levels

67,	73,	85,	88,	93,	103,	104,	106,	107,	112,
115,	116,	117,	121,	122,	125,	129,	133,	134,	135,
146,	147,	153,	154,	158,	161,	165,	166,	167,	168,
170,	177,	180,	184,	186,	191,	198,	204,	205,	206,
209,	213,	215,	221,	230,	255,	266,	276,	284,	285,
286,	287,	299,	330,	357,	380,	390.			

Balakrishnan et al. using quadratic Chabauty

Bars, González, and Xarles using elliptic curve Chabauty

rank is 0 or 1, we can use classical Chabauty techniques

Arul and Müller using quadratic Chabauty

There are 15 remaining levels, which we also address in our paper.

Theorem (Stoll, 2006)

Let C be a nice curve of genus $g \geq 2$. Let r be the rank of its Jacobian over $\mathbb{Q}$. Let p be a prime of good reduction for C. If $r < g$ and $p > 2r + 2$, then

$$|C(\mathbb{Q})| \leq |C(\mathbb{F}_p)| + 2r.$$

The levels where we had to compute annihilating differentials:

N	g	r	p	$\#X_0(N)^*(\mathbb{Q})$
171	3	1	5	6
176	4	1	3	5
279	5	2	5	6

This computation is done using an implementation by Balakrishnan-Tuitman called `effective_chabauty`.

Exceptional Isomorphisms

If

$$N \in \{134, 146, 206\},$$

then the curves can be addressed using the observation

$$\begin{aligned} X_0(134)^* &\cong X_0(67)^* = X_0(67)^+ \\ X_0(146)^* &\cong X_0(73)^* = X_0(73)^+ \\ X_0(206)^* &\cong X_0(103)^* = X_0(103)^+ \end{aligned}$$

Also,

$$X_0(266)^* \cong X_0(133)^*,$$

thus the remaining cases are

$$N \in \{133, 147, 166, 177, 205, 213, 221, 255, 287, 299, 330\}.$$

Overview of methods used

Method	Levels N
Classical Chabauty	88, 104, 112, 116, 117, 121, 135, 136, 153, 168, 171, 176, 180, 184, 198, 204, 276, 279, 284, 380
Exceptional isomorphisms	134, 146, 206, 266
Elliptic curve quotient	207, 252, 315
Elliptic curve Chabauty	147, 255, 330
Quadratic Chabauty	$G = \{133, 177, 205, 213, 221, 287, 299\}$

Table: Levels N and methods we applied to determine $X_0(N)^*(\mathbb{Q})$

Quadratic Chabauty: Computation of Local Heights

Namikawa and Ueno (1973) classified possible reductions of genus 2 curves. Liu (1994, 1996) has, together with Cohen, implemented the computation of the reduction types in Sage. For levels $N \in G$ and each prime $l \mid N$ we get:

Figure: Type $\mathrm{I}_{1\text{-}1\text{-}0}$ of Namikawa–Ueno

- `genus2reduction` shows: The special fibers of a regular semistable model have only one component.
- The local heights h_ℓ for $\ell \neq p$ are trivial (Betts–Dogra), and we need to solve $h(x) - h_p(x) = 0$ on $X(\mathbb{Q}_p)$.

Other methods used

- Mordell-Weil Sieve: use local information for additional primes
- quotients: finding rank 0 elliptic curve which is a quotient of the starting curve
- Elliptic curve Chabauty: using higher genera coverings in hope of getting $r < g$

Main Result on $X_0(N)^*$

Theorem 1 (ACKP, 2022)

Let N be such that $X_0(N)^*$ is hyperelliptic. Then $X_0(N)^*(\mathbb{Q})$ consists only of the known points of small height.

More precisely, let N be a square-free positive integer such that $X_0(N)^*$ is of genus 2. If $X_0(N)^*$ has no exceptional rational points, then $N \in \{67, 107, 146, 167, 205, 213, 390\}$.

For each of the remaining 32 *levels* $N \in \{$73, 85, 93, 103, 106, 115, 122, 129, 133, 134, 154, 158, 161, 165, 166, 170, 177, 186, 191, 206, 209, 215, 221, 230, 255, 266, 285, 286, 287, 299, 330, 357$\}$, *there is at least one exceptional rational point.*

Comment on exceptional points

- Exceptional rational points exist on most of the hyperelliptic curves $X_0(N)^*$, but almost all of them arise as the image of a cusp or CM point under the hyperelliptic involution.
- The only curves that have an exceptional rational point not arising in this way are $X_0(129)^*$ and $X_0(286)^*$.
- Furthermore, the curve $X_0(129)^*$ has automorphisms which explain all the exceptional rational points on this curve.

Example of results: $X_0(133)^*$

It has a hyperelliptic model

$$y^2 = x^6 + 4x^5 - 18x^4 + 26x^3 - 15x^2 + 2x + 1,$$

and it satisfies $r = g = 2$, so we use quadratic Chabauty with QC primes $p \in \{5, 59\}$, additional MWS primes 109, 131, 317, 509

Point	j or $\mathbb{Q}(j)$	CM	D
$-\infty$	$\mathbb{Q}(\sqrt{2}, \sqrt{69})$	no	
$(0, -1)$	$-2^{15}\ 3^3$	yes	-19
$(0, 1)$	$-2^{15}\ 3\ 5^3$	yes	-27
$(1, -1)$	$2^4\ 3^3\ 5^3$	yes	-12
$(1, 1)$	$(48(-227 \pm 63\sqrt{13}))^3$	yes	-91
$(\frac{3}{5}, \frac{-83}{125})$	$\mathbb{Q}(\sqrt{-31}, \sqrt{-3651})$	no	
$(\frac{3}{5}, \frac{83}{125})$	0	yes	-3

Table: Rational non-cuspidal points, j-invariants, and CM discriminants D of the associated $\mathbb{Q}$-curves.

Example: Modular coverings of $X_0(133)^*$

Table: Intermediate coverings of $X_0(133) \to X_0(133)^*$ and low-degree points.

Curve	Low-degree points
$X_0(133)/\langle w_7 \rangle$	• 3 rational points. • Points over $\mathbb{Q}(\sqrt{d})$ for $d = -3, -91, 138, 113181$
$X_0(133)/\langle w_{19} \rangle$	• 2 rational points. • Points over $\mathbb{Q}(\sqrt{d})$ for $d = 2, -3, -7, -19, -31$
$X_0(133)/\langle w_{133} \rangle$	• 9 rational points. • Points over $\mathbb{Q}(\sqrt{d})$ for $d = 13, 69, -3651$
$X_0(133)$	• 4 cuspidal rational points. • Points over $\mathbb{Q}(\sqrt{d})$ for $d = -3, -19$ • Points over $\mathbb{Q}(\sqrt{d_1, d_2})$ for $(d_1, d_2) = (-7, 13), (2, 69), (-31, -3651)$

Applications and future work

- low degree points on $X_0(N)$
- higher genus $X_0^*(N)$
- (quotients of) Shimura curves

Acknowledgements

This work was supported by the Croatian Science Foundation.

This project was initiated as part of a 2020 Arizona Winter School project led by Jennifer Balakrishnan and Netan Dogra.

Literature

- J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Annals of Mathematics 189-3, 885–944, 2019
- J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, J. Vonk, *Quadratic Chabauty for modular curves: Algorithms and examples*, `https://arxiv.org/abs/2101.01862`
- F. Bars, J. González, X. Xarles, *Hyperelliptic parametrizations of $\mathbb{Q}$-curves*, The Ramanujan Journal 56-1, 103–120, 2021
- S. D. Galbraith, *Equations for Modular Curves*, PhD thesis, University of Oxford