Rational points on hyperelliptic Atkin-Lehner quotients of modular curves

Nikola Adžaga (Zagreb), Shiva Chidambaram (MIT),
Timo Keller (Hannover), and Oana Padurariu (Boston)

ANTS-XV 2022

August 12, 2022

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.

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 kernel cyclic of order N.

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 kernel cyclic of order N.
- Mazur (1977): Computation of $X_1(p)(\mathbb{Q})$.

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

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 kernel cyclic of order N.
- Mazur (1977): Computation of $X_1(p)(\mathbb{Q})$.
- Mazur (1978): Computation of $X_0(p)(\mathbb{Q})$.
- Kamienny–Merel–Oesterlé (1990's): Let $[K : \mathbb{Q}] = d > 5$. Then $X_1(p)(K)$ consists only of cusps if $p > (3^{d/2} + 1)^2$.

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 kernel cyclic of order N.
- Mazur (1977): Computation of $X_1(p)(\mathbb{Q})$.
- Mazur (1978): Computation of $X_0(p)(\mathbb{Q})$.
- 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 $[K : \mathbb{Q}] \leq 7$.

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

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

Atkin-Lehner Quotients

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

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

Consider the quotients

$$X_0(N)^+ := X_0(N)/w_N,$$
$$X_0(N)^* := X_0(N)/\langle w_d : (d, N/d) = 1 \rangle.$$

Atkin-Lehner Quotients

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

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

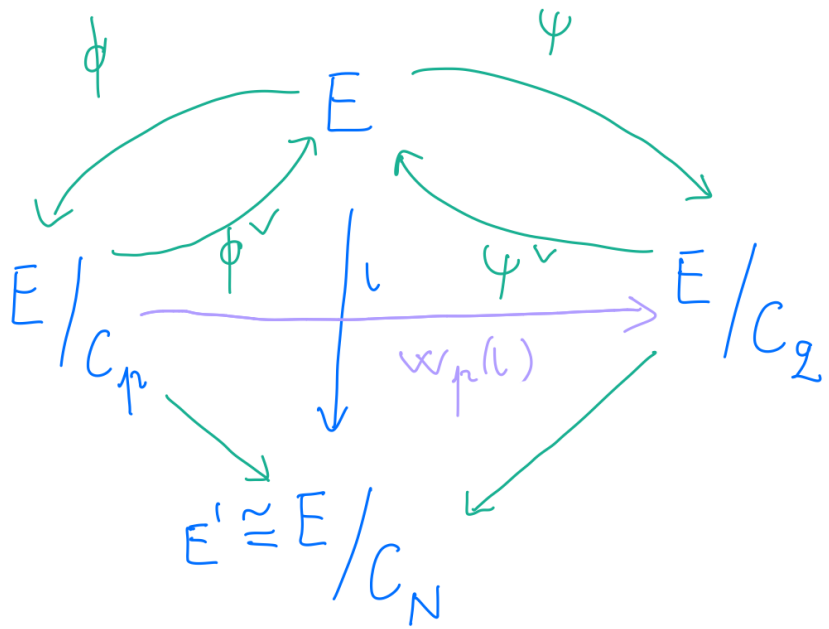
Consider the quotients

$$X_0(N)^+ := X_0(N)/w_N,$$
$$X_0(N)^* := X_0(N)/\langle w_d : (d, N/d) = 1\rangle.$$

- Rational points on $X_0(N)^*$ correspond to $\mathbb{Q}$-curves.
- Knowing $X_0(N)^+(\mathbb{Q})$ is helpful for determining all quadratic points on $X_0(N)$.
- Elkies' conjecture: For $N \gg 0$, $X_0(N)^*(\mathbb{Q})$ consists only of cusps and CM points.

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.



Atkin-Lehner involution w_p

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

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.			

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

Bars, González, and Xarles (2019) using elliptic curve Chabauty

Balakrishnan et al. (2021) using quadratic Chabauty

Arul and Müller (2022) using quadratic Chabauty

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

Main Result

Theorem (BDMTV, BGX, AM, and ACKP)

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

Main Result

Theorem (BDMTV, BGX, AM, and ACKP)

Let N be such that $X_0(N)^*$ is hyperelliptic.
Then $X_0(N)^*(\mathbb{Q})$ only consists 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.

Exceptional Isomorphisms

If

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

then the curves can be addressed using the observation

$$X_0(2p)^* \cong X_0(p)^* = X_0(p)^+ \quad \text{for } p \in \{67, 73, 103\}.$$

Note that

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

thus the remaining cases are

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

The Chabauty-Coleman Method

- Let g be the genus of X (not necessarily modular) and r the Mordell-Weil rank of its Jacobian J (more precisely, its p-adic closure).

The Chabauty-Coleman Method

- Let g be the genus of X (not necessarily modular) and r the Mordell-Weil rank of its Jacobian J (more precisely, its p-adic closure).
- Use a basepoint $x_0 \in X(\mathbb{Q})$ to embed $X \hookrightarrow J, x \mapsto [x - x_0]$.

The Chabauty-Coleman Method

- Let g be the genus of X (not necessarily modular) and r the Mordell-Weil rank of its Jacobian J (more precisely, its p-adic closure).
- Use a basepoint $x_0 \in X(\mathbb{Q})$ to embed $X \hookrightarrow J, x \mapsto [x - x_0]$.
- Let p be a prime of good reduction for X.

The Chabauty-Coleman Method

- Let g be the genus of X (not necessarily modular) and r the Mordell-Weil rank of its Jacobian J (more precisely, its p-adic closure).
- Use a basepoint $x_0 \in X(\mathbb{Q})$ to embed $X \hookrightarrow J, x \mapsto [x - x_0]$.
- 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

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

- Choose ω to be a linear combination of a basis of $\mathrm{H}^0(X, \Omega^1)$, which annihilates a generating set of G.
- The analytic 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

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

- $h - h_p$ is locally analytic, and the h_ℓ have finite image on $X(\mathbb{Q})$ depending on the reduction at ℓ.
- If $r = g$ and the Néron-Severi rank of $\mathrm{Jac}(X)$ is > 1, 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 $\ell \neq p$.

Quadratic Chabauty: Computation of Local Heights

Type $I_{1\text{-}1\text{-}0}$ of Namikawa–Ueno

- `genus2reduction` shows: The special fibers of a regular semistable model are irreducible.
  So its dual graph has exactly one vertex.

Quadratic Chabauty: Computation of Local Heights

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

- `genus2reduction` shows: The special fibers of a regular semistable model are irreducible.
  So its dual graph has exactly one vertex.
- The local heights h_ℓ for $\ell \neq p$ factor through the vertices of the dual graph (Betts–Dogra). So they are trivial,
  and we need to solve $h(x) - h_p(x) = 0$ on $X(\mathbb{Q}_p)$.

Quadratic Chabauty: Computation of Local Heights

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

- `genus2reduction` shows: The special fibers of a regular semistable model are irreducible.
  So its dual graph has exactly one vertex.
- The local heights h_ℓ for $\ell \neq p$ factor through the vertices of the dual graph (Betts–Dogra). So they are trivial,
  and we need to solve $h(x) - h_p(x) = 0$ on $X(\mathbb{Q}_p)$.
- So we can treat the cases in red using quadratic Chabauty because they satisfy $r = g$ and have Néron-Severi rank $g > 1$:

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

The Mordell-Weil Sieve

Assume that one can compute $J(\mathbb{Q})$.

For a finite set S of good primes and an integer $M > 1$, consider the commutative diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/MJ(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \prod_{\ell \in S} X(\mathbb{F}_\ell) & \xrightarrow{\beta} & \prod_{\ell \in S} J(\mathbb{F}_\ell)/MJ(\mathbb{F}_\ell) \end{array}$$

Conjecturally, one can always choose S and M such that the Mordell-Weil sieve computes $X(\mathbb{Q})$.

Example: $X_0(133)^*$

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 and $M = 5^n \cdot 59^m$ to sieve out 4 and 62 fake residue discs.

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

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

Choice of QC and MWS Primes

N	QC primes	MWS primes	M'	$\#X_0(N)^*(\mathbb{Q})$	#non-CM
133	5, 59	109, 131, 317, 509	1	8	2
177	5	19	1	6	1
205	17, 61, 71	≤ 18457[1]	3	6	0
213	79	59, 149, 211, 4177	1	4	0
221	29	3, 47	1	6	1
287	19, 29	3, 5	1	4	1
299	29, 37, 43	≤ 929[2]	$3 \cdot 5$	4	1

Table: Data used to do the quadratic Chabauty computations and information on $X_0(N)^*(\mathbb{Q})$. (MWS primes means the additional primes in the Mordell-Weil sieve compared to the QC primes.)

[1] 43, 71, 179, 359, 439, 617, 661, 967, 1033, 1997, 2063, 2213, 2381, 2753, 3373, 9579, 15083, 18457

[2] 7, 59, 89, 103, 137, 317, 443, 541, 787, 929

Runtimes and Memory Usage

Table: Runtimes and memory usage for Chabauty and Mordell-Weil sieve in the cases where we applied quadratic and elliptic curve Chabauty.

N	runtime in seconds	RAM used in MB
133	110	130
177	22	130
205	546	406
213	16822	225
221	80	130
287	1533	130
299	6669	3196
147	37	85
255	47	96
330	25	85

Modular Coverings of $X_0(N)^*$

- If $X_0(N)^*(\mathbb{Q})$ is finite and known, one can compute the $\mathbb{Q}$-points for all modular coverings $X_0(N)/W'(N)$ if one knows the quotient morphisms (going down).

Modular Coverings of $X_0(N)^*$

- If $X_0(N)^*(\mathbb{Q})$ is finite and known, one can compute the $\mathbb{Q}$-points for all modular coverings $X_0(N)/W'(N)$ if one knows the quotient morphisms (going down).
- Assume $X_0(N)$ is non-hyperelliptic and given by the canonical embedding associated to $\mathrm{H}^0(X_0(N), \Omega^1) \simeq S_2(\Gamma_0(N))$ over $\mathbb{Q}$, diagonalized such that the Atkin-Lehner involutions are simultaneously diagonal with ± 1's on the diagonal.

Modular Coverings of $X_0(N)^*$

- If $X_0(N)^*(\mathbb{Q})$ is finite and known, one can compute the $\mathbb{Q}$-points for all modular coverings $X_0(N)/W'(N)$ if one knows the quotient morphisms (going down).
- Assume $X_0(N)$ is non-hyperelliptic and given by the canonical embedding associated to $\mathrm{H}^0(X_0(N), \Omega^1) \simeq S_2(\Gamma_0(N))$ over $\mathbb{Q}$, diagonalized such that the Atkin-Lehner involutions are simultaneously diagonal with ± 1's on the diagonal.
- We then compute the quotient maps

$$X_0(N) \twoheadrightarrow X_0(N)/W'(N) \hookrightarrow \mathbb{P}(1, \ldots, 1, 2, \ldots, 2)$$

for non-hyperelliptic $X_0(N)/W'(N)$ by finding relations between the q-expansions in $S_2(\Gamma_0(N))$, computing the Atkin-Lehner action, and using invariant theory.

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 $(d_1, d_2) = (-7, 13), (2, 69), (-31, -3651)$

Work in Progress

- $X_0(N)^*$ of higher genus, not hyperelliptic
  (joint with Lea Beneish and Boya Wen)
- Application to quadratic points on $X_0(N)$ for N small
- Quotients of Shimura curves

Thank you for your attention!