Rational points on modular star quotients $X_0(N)^*$ of genus two

Oana Păduraru (MPIM Bonn)
joint with Nikola Adžaga, Shiva Chidambaram, and Timo Keller,
and with Francesca Bianchi

Winter Workshop Chabauty–Kim, Heidelberg

February 16th, 2024

Outline

Definition of $X_0(N)$

Definition

For $N \in \mathbb{Z}_{\geq 1}$, we have the moduli space/modular curve over $\mathbb{C}$

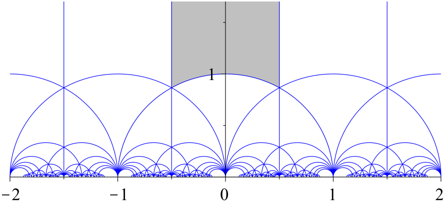
$$Y_0(N) := \{\text{isomorphism classes } (E, \iota) |\, \iota : E \to E', \ker(\iota) \cong \mathbb{Z}/N\mathbb{Z}\}.$$

$$X_0(N) := Y_0(N) \cup \{\text{cusps}\}.$$

The curve $X_0(N)$ is defined over $\mathbb{Z}\left[\frac{1}{N}\right]$, so one may consider the set $X_0(N)(\mathbb{Q})$.

Revisiting $X_0(N)$

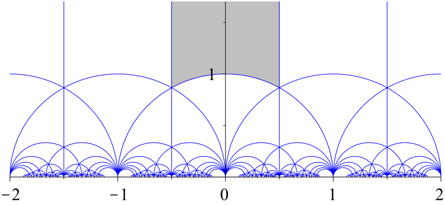
$$\mathcal{H} := \{x + iy | x, y \in \mathbb{R}, y > 0\}, \quad \mathcal{H}^* := \{x + iy | x, y \in \mathbb{R}, y > 0\} \cup \mathbb{Q} \cup \{i\infty\}.$$



fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

Revisiting $X_0(N)$

$$\mathcal{H} := \{x + iy | x, y \in \mathbb{R}, y > 0\}, \quad \mathcal{H}^* := \{x + iy | x, y \in \mathbb{R}, y > 0\} \cup \mathbb{Q} \cup \{i\infty\}.$$



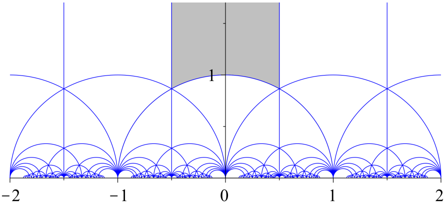
fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

Möbius transformation $$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}, \quad \forall z \in \mathcal{H}^*.$$

Revisiting $X_0(N)$

$$\mathcal{H} := \{x + iy \mid x, y \in \mathbb{R}, y > 0\}, \quad \mathcal{H}^* := \{x + iy \mid x, y \in \mathbb{R}, y > 0\} \cup \mathbb{Q} \cup \{i\infty\}.$$



fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

$$Y_0(N)(\mathbb{C}) \simeq \Gamma_0(N)\backslash\mathcal{H}, \quad X_0(N)(\mathbb{C}) \simeq \Gamma_0(N)\backslash\mathcal{H}^*.$$

Atkin–Lehner involutions

We say that $d|N$ is a Hall divisor if $\gcd(d, N/d) = 1$, which we denote by $d \parallel N$.

Definition

For each Hall divisor $d \parallel N$, consider the matrices of the form

$$\begin{pmatrix} dx & y \\ Nz & dw \end{pmatrix}, \quad \text{with } x, y, z, w \in \mathbb{Z} \quad \text{and determinant } d.$$

Then each of these matrices define a unique involution of $X_0(N)$, which is called the *Atkin–Lehner involution* and is denoted by w_d. In particular, if $d = N$, then w_N is called the *Fricke involution*.

Quotients of $X_0(N)$

Let $d \parallel N$ be a Hall divisor of N.
The action of the Atkin–Lehner involution w_d on $Y_0(N)$ is given by

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

This extends uniquely to $X_0(N)$ by the valuative criterion for properness.

We will consider the following quotients:

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

Outline

Moduli space of $\mathbb{Q}$-curves

The quotient

$$X_0(N)^* := X_0(N)/W_0(N)$$

is itself a moduli space. For N squarefree, the lifts in $X_0(N)$ of every non-cuspidal point in $X_0(N)^*(\mathbb{Q})$ correspond to $\mathbb{Q}$-curves defined over multi-quadratic extensions of $\mathbb{Q}$.

A $\mathbb{Q}$-curve is an elliptic curve defined over a Galois extension $K/\mathbb{Q}$ which is isogenous to all of its Galois conjugates.

We say that a point in $X_0(N)^*(\mathbb{Q})$ is *exceptional* if it is neither a cusp, nor a CM point.

The star quotient $X_0(N)^*$

Determining rational points on $X_0(N)^*$ may help solve some interesting problems in number theory, for example Balakrishnan, Dogra, Müller, Tuitman, and Vonk computed $X_0(13^2)^*(\mathbb{Q})$ and thus solved a case of Serre's uniformity conjecture for Galois images of elliptic curves.

We are interested in provably computing all the rational points on $X_0(N)^*$.

Elkies' conjecture: For $N \gg 0$, $X_0(N)^*(\mathbb{Q})$ consists only of cusps and CM points.

Hyperelliptic $X_0(N)^*$

We start with the case of hyperelliptic curves.

Theorem (Hasegawa)

There are 64 values of N for which $X_0(N)^*$ is hyperelliptic. Of these, there are only 7 of genus $g \geq 3$, namely $N = 136, 171, 207, 252, 315$ $(g = 3)$, 176 $(g = 4)$, and 279 $(g = 5)$.

Computing rational points: the Chabauty–Coleman method

- Use a basepoint $b \in X(\mathbb{Q})$ to embed $X \hookrightarrow J, x \mapsto [x - b]$.
- 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

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

- Choose ω to be a linear combination of a basis of $\mathrm{H}^0(X, \Omega^1)$, which annihilates a finite index subgroup G of $J(\mathbb{Q})$.
- The set $X(\mathbb{Q}_p)_1$ is finite and computable if we know a finite index subgroup G of $J(\mathbb{Q})$.

Computing rational points: the quadratic Chabauty method

There have been developments in extending the range of applicability of the Chabauty–Coleman method.

One of the most successful extensions is the quadratic Chabauty method, which works under the condition

$$r < g + \rho(J) - 1,$$

where $\rho(J)$ is the rank of the Néron–Severi group of J over $\mathbb{Q}$.

Overview: the Quadratic Chabauty method

Range of applicability:

- bielliptic quadratic Chabauty: Balakrishnan and Dogra made one level of Kim's program explicit for genus 2 curves X for which $J(\mathbb{Q})$ is isogenous to a product of elliptic curves $E_1 \times E_2$ with $\mathrm{rk}(E_1(\mathbb{Q})) = \mathrm{rk}(E_2(\mathbb{Q})) = 1$;
- quadratic Chabauty for modular curves: Balakrishnan, Dogra, Müller, Tuitman, and Vonk developed quadratic Chabauty explictly to compute $X_0(13^2)^+(\mathbb{Q})$.

The Quadratic Chabauty Method

- Same setup as Chabauty–Coleman, but

$$\cancel{r < g}, \quad r < g + \rho(J) - 1.$$

- 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_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):

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

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

Back to Hasegawa's classification

Recall that Hasegawa classified the levels N for which $X_0(N)^*$ is hyperelliptic. The hardest case is determining the set of rational points in the genus 2 case, as the higher genus cases can be tackled using the Chabauty–Coleman method.

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

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.			

Rank is 0 or 1, we can use classical Chabauty–Coleman

Balakrishnan–Dogra–Müller–Tuitman–Vonk using quadratic Chabauty

Arul–Müller using quadratic Chabauty

Bars–González–Xarles using elliptic curve Chabauty

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

Filling the gap

Theorem (Adžaga-Chidambaram-Keller-P.)

Let N be one of the following integers:

$$\{133, 134, 146, 147, 166, 177, 205, 206, 213, 221, 255, 266, 287, 299, 330\}.$$

Then $X_0(N)^*(\mathbb{Q})$ only consists of the known points of small height. Moreover, we classify the rational points into cusps, CM points and exceptional points.

Exceptional isomorphisms

If

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

the curves can be addressed using the following 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 persisting cases are

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

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 $\rho(J) > 1$:

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

$X_0(N)^*$ of genus at least 3

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

- 136, 171, 207, 252, 315 ($g = 3$),
- 176 ($g = 4$),
- 279 ($g = 5$).

In all of these cases we have that $g > \mathrm{rk}(\mathrm{Jac}(X_0(N)^*(\mathbb{Q})))$, and we were able to apply the classical Chabauty–Coleman method.

Outline

1. Motivation
2. Modular star quotient $X_0(N)^*$
3. Bielliptic quadratic Chabauty
4. The Mordell–Weil sieve

Bielliptic curves

Definition

We say that a curve $X/\mathbb{Q}$ is bielliptic over $\mathbb{Q}$ if there exists a degree two map $X \to E$ defined over $\mathbb{Q}$ to an elliptic curve $E/\mathbb{Q}$.

If X is bielliptic and has genus 2, then it admits a model of the form

$$X : y^2 = a_6x^6 + a_4x^4 + a_2x^2 + a_0.$$

Furthermore, $\mathrm{Jac}(X) \sim E_1 \times E_2$, where E_1 and E_2 are elliptic curves given by the following Weierstrass equations:

$$E_1 \colon y^2 = x^3 + a_4x^2 + a_2a_6x + a_0a_6^2,$$
$$E_2 \colon y^2 = x^3 + a_2x^2 + a_4a_0x + a_6a_0^2.$$

There are degree 2 maps $\varphi_i \colon X \to E_i$ given on affine points by

$$\varphi_1(x, y) = (a_6x^2, a_6y), \qquad \varphi_2(x, y) = (a_0x^{-2}, a_0yx^{-3}).$$

Methods to compute $X(\mathbb{Q})$

Let $X/\mathbb{Q}$ be a genus 2 curve which is bielliptic over $\mathbb{Q}$. Then

- Faltings' theorem: $X(\mathbb{Q})$ is finite.
- If $\operatorname{rk} E_1(\mathbb{Q}) = 0$ or $\operatorname{rk} E_2(\mathbb{Q}) = 0$, then we can easily compute $X(\mathbb{Q})$.
- If $\operatorname{rk} E_i(\mathbb{Q}) \geq 1$ for $i \in \{1, 2\}$, then to provably compute $X(\mathbb{Q})$ we can consider methods such as local obstructions, two-cover descent, elliptic curve Chabauty.
- If $\operatorname{rk} E_i(\mathbb{Q}) = 1$ for $i \in \{1, 2\}$, then the bielliptic quadratic Chabauty method may be applied.

Bielliptic quadratic Chabauty

Consider $X/\mathbb{Q}$ a bielliptic genus 2 curve

$$X : y^2 = x^6 + a_4x^4 + a_2x^2 + a_0.$$

Let p is a prime of good ordinary reduction for X.

Theorem (Balakrishnan–Dogra)

Define $Q_i \in E_i(\overline{\mathbb{Q}})$ *by* $Q_1 = (0, \sqrt{a_0})$ *and* $Q_2 = (0, a_0)$*. Suppose* $\operatorname{rk} E_1(\mathbb{Q}) = \operatorname{rk} E_2(\mathbb{Q}) = 1$*. Then the sets* Ω_1, Ω_2 *are finite, where:*

$$\Omega_i = \{ \sum_{\ell \neq p} (h_\ell^{E_i}(\varphi_i(z_\ell) + Q_i) + h_\ell^{E_i}(\varphi_i(z_\ell) - Q_i) - 2h_\ell^{E_{3-i}}(\varphi_{3-i}(z_\ell))) : \\ (z_\ell) \in \prod_{\ell \neq p} X(\mathbb{Q}_\ell) \backslash \{\varphi_i^{-1}(\pm Q_i)\}\}.$$

Bielliptic quadratic Chabauty revisited

Theorem (Bianchi–P.)

One can replace the computation of Ω_1, Ω_2 with the computation of a single set Ω. Moreover, this new set Ω does not depend on $Q_1 = (0, \sqrt{a_0}) \in E_1(\overline{\mathbb{Q}})$ and $Q_2 = (0, a_0) \in E_1(\mathbb{Q})$.

- We provide a precision analysis to guarantee correctness of the results.
- We used bielliptic quadratic Chabauty in conjuction with the Mordell-Weil sieve on more than 300 bielliptic genus 2 curves from the LMFDB.

$X_0(166)^*$

A priori, we know the curve $X_0(166)^*$ has minimal model

$$y^2 + (-x^3 - 1)y = -x^4 + 2x^3 - x^2,$$

which has 2 and 83 as primes of bad reduction. The reduction type leads to trivial height contribution from $\ell = 83$, but we might obtain a nonzero contribution from $\ell = 2$.

$X_0(166)^*$

A priori, we know the curve $X_0(166)^*$ has minimal model

$$y^2 + (-x^3 - 1)y = -x^4 + 2x^3 - x^2,$$

which has 2 and 83 as primes of bad reduction. The reduction type leads to trivial height contribution from $\ell = 83$, but we might obtain a nonzero contribution from $\ell = 2$.

But, surprisingly, $X_0(166)^*$ is a bielliptic curve

$X_0(166)^*$

A priori, we know the curve $X_0(166)^*$ has minimal model

$$y^2 + (-x^3 - 1)y = -x^4 + 2x^3 - x^2,$$

which has 2 and 83 as primes of bad reduction. The reduction type leads to trivial height contribution from $\ell = 83$, but we might obtain a nonzero contribution from $\ell = 2$.

But, surprisingly, $X_0(166)^*$ is a bielliptic curve

$$X_0(166)^* : y^2 = x^6 + 2x^4 + 17x^2 - 4.$$

Thus one may apply bielliptic quadratic Chabauty.

Outline

Sieving: bielliptic case

Let $X/\mathbb{Q}$ be a bielliptic genus 2 curve with

$$\mathrm{Jac}(X)(\mathbb{Q}) \sim E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$$

with $\mathrm{rk}(E_1(\mathbb{Q})) = \mathrm{rk}(E_2(\mathbb{Q})) = 1$.

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, "\varphi"] \arrow[d, "\mathrm{red}_p"] & E_1(\mathbb{Q}) \times E_2(\mathbb{Q}) \arrow[d, "\mathrm{red}_p"] & \mathbb{Z} \times \mathbb{Z} \arrow[l, "\eta"'] \arrow[dl, "\mu"] \\
X(\mathbb{F}_p) \arrow[r, "\varphi"] & E_1(\mathbb{F}_p) \times E_2(\mathbb{F}_p) &
\end{tikzcd}$$

Sieving: bielliptic case

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, "\varphi"] \arrow[d, "\mathrm{red}_p"] & E_1(\mathbb{Q}) \times E_2(\mathbb{Q}) \arrow[d, "\mathrm{red}_p"] & \mathbb{Z} \times \mathbb{Z} \arrow[l, "\eta"'] \arrow[dl, "\mu"] \\
X(\mathbb{F}_p) \arrow[r, "\varphi"] & E_1(\mathbb{F}_p) \times E_2(\mathbb{F}_p), &
\end{tikzcd}$$

where $\varphi = (\varphi_1, \varphi_2), \eta(m, n) = (mP_1, nP_2)$, where P_1, P_2 are generators for $E_1(\mathbb{Q}), E_2(\mathbb{Q})$ respectively, and $\mu = \mathrm{red}_p \circ \eta$.

Since

$$(\mathrm{red}_p \circ \varphi)(X(\mathbb{Q})) \subseteq \varphi(X(\mathbb{F}_p)) \cap \mu(\mathbb{Z} \times \mathbb{Z}),$$

to prove that $X(\mathbb{Q}) = \emptyset$, it is enough to show that $\varphi(X(\mathbb{F}_p)) \cap \mu(\mathbb{Z} \times \mathbb{Z}) = \emptyset$.

The Mordell–Weil Sieve: general case

Assume that one can compute generators for (a finite index subgroup of) $J(\mathbb{Q})$.

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

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/MJ(\mathbb{Q}) \arrow[d, "\alpha"] \\ \prod_{\ell \in S} X(\mathbb{F}_\ell) \arrow[r, "\beta"] & \prod_{\ell \in S} J(\mathbb{F}_\ell)/MJ(\mathbb{F}_\ell) \end{tikzcd}$$

Conjecturally, one can always choose an integer M and a set of primes S such that the Mordell-Weil sieve eliminates all p-adic points resulted from Chabauty methods which do not come from $\mathbb{Q}$-rational points.


VIELEN DANK
FÜR IHRE
AUFMERKSAMKEIT!
makeameme.org