Low degree points on modular curves and their quotients

Nikola Adžaga

University of Zagreb

Modular curves and Galois representations

21st September, 2023

Hrvatska zaklada za znanost

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 $[K:\mathbb{Q}] \leqslant 7$.

- Open problem: Computation of $X_0(p)(K)$ for all p and <u>all</u> 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

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

Consider the quotients

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

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.)

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 (QC)

- 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):

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

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

QC: assumptions and input

Input:

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

On low genus $X_0^+(N)$ for prime levels N

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.

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 $4 - 6$

(If not hyperelliptic:)

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

(Each our) genus 5 curve is a complete intersection of 3 quadrics in $\mathbb{P}^4$.

(Each our) genus 6 curve is an intersection of 6 quadrics in $\mathbb{P}^5$.

From canonical models to plane models I

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

Goal: a suitable plane model.

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

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

is a birational map onto its image.

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
$x_1 = Z, x_2 = Y,\ y_1 = 42Z, y_2 = W + X + 2Y + Z,$
$\tau_x = [x_1 : x_2], \tau_y = [y_1 : y_2]$.

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

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 (A.-Arul-Beneish-Chen-Chidambaram-Keller-Wen)

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 $X_0(N)^*$

All Hyperelliptic Quotients

Theorem (Hasegawa, 1997)

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

There are 7 values of N for which $X_0(N)^*$ is hyperelliptic with genus $g \geqslant 3$ (, 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-Dogra-Müller-Tuitman-Vonk 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 ANTS paper (joint with Chidambaram, Keller, Padurariu).

Classical Chabauty

Theorem (Stoll, 2006)

Let C be a nice curve of genus $g \geqslant 2$. Let $r = \operatorname{rk} J_C(\mathbb{Q})$ and p a prime of good reduction for C. If $r < g$ and $p > 2r + 2$, then

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

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 $X_0(N)^*(\mathbb{Q})$

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 (A.-Chidambaram-Keller-Padurariu, 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.

On exceptional isomorphisms

(WIP:) Padurariu and Voight are classifying exceptional isomorphisms. They show that there are only finitely many squarefree levels $N_1 \neq N_2$ with existing Atkin-Lehner subgroups W_1 and W_2 so that

$$X_0(N_1)/W_1 \cong X_0(N_2)/W_2$$

and are working on giving a complete list of such isomorphisms.

Computing quadratic points on $X_0(N)$

Motivation

Quadratic isogenies conjecture: There exists a constant C such that if K is a quadratic field and $N > C$ is an integer, then any $P \in X_0(N)(K)$ is either a cusp or a CM-point.

C does not depend on K.

The Modular Approach to Diophantine equations requires knowledge of quadratic points (Freitas–Siksek, Khawaja–Jarvis, Michaud-Jacobs).

Previous results

A pair of quadratic points gives rise to a rational point on the symmetric square of $X_0(N)$, i. e. an effective degree 2 divisor $Q + Q^\sigma$.

Abramovich–Harris: A smooth projective curve $X/\mathbb{Q}$ of genus $\geqslant 2$ has infinitely many quadratic points if and only if it is hyperelliptic over $\mathbb{Q}$ or if it is bielliptic with a degree 2 morphism $X \to E$ where $E/\mathbb{Q}$ is an elliptic curve of positive rank over $\mathbb{Q}$.

Previous results II

All quadratic points have been determined in the following cases.

1. Bruin–Najman: the hyperelliptic $X_0(N)$ with $\operatorname{rk} J_0(N)(\mathbb{Q}) = 0$.
2. Ozman–Siksek: The non-hyperelliptic $X_0(N)$ with $g(X_0(N)) \leqslant 5$ and $\operatorname{rk} J_0(N)(\mathbb{Q}) = 0$.
3. Box: The $X_0(N)$ with $g(X_0(N)) \leqslant 5$ and $\operatorname{rk} J_0(N)(\mathbb{Q}) > 0$.
4. Najman–Vukorepa: The bielliptic $X_0(N)$ which have not been already dealt with in (1.)–(3.).

Previous results III

Two broad methods were used.

- Mordell–Weil sieve with different variations
- going-down method ($X_0(dM) \to X_0(M)$)

Our improvements on these methods

In a joint work with Keller, Michaud-Jacobs, Najman, Ozman and Vukorepa we extend these methods with new techniques:

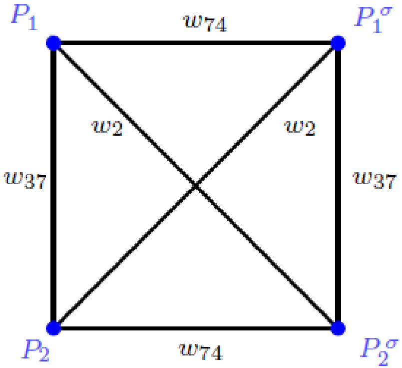
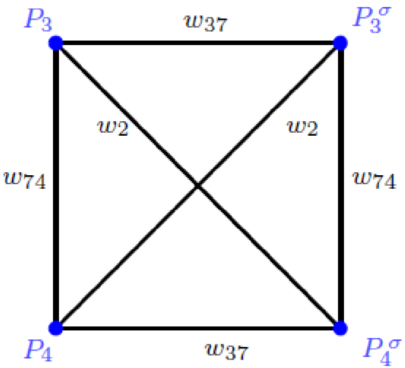
- simultaneously diagonalized models of $X_0(N)$
- faster computation of the equations for the j-map by improving on the known (Sturm) bound
- fast method for verifying nonsingularity at a given prime.

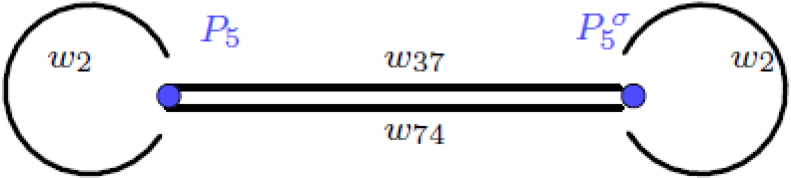
Our results

We provably find all the quadratic points on $X_0(N)$ of genus up to 8, and genus up to 10 with N prime.

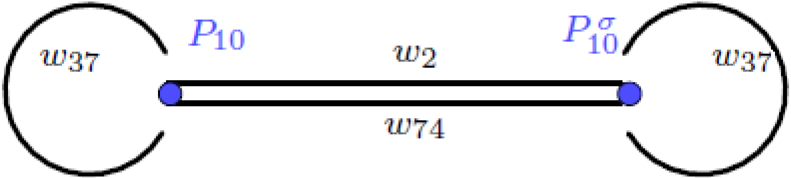
$$J_0(74)(\mathbb{Q}) \cong \mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/171\mathbb{Z}$$

Point	Field	j-invariant	CM
P_1	$\mathbb{Q}(\sqrt{-7})$	-3375	-7
P_2	$\mathbb{Q}(\sqrt{-7})$	-3375	-7
P_3	$\mathbb{Q}(\sqrt{-7})$	-3375	-7
P_4	$\mathbb{Q}(\sqrt{-7})$	16581375	-28
P_5	$\mathbb{Q}(\sqrt{-1})$	1728	-4
P_6	$\mathbb{Q}(\sqrt{-1})$	1728	-4
P_7	$\mathbb{Q}(\sqrt{-1})$	287496	-16
P_8	$\mathbb{Q}(\sqrt{-3})$	54000	-12
P_9	$\mathbb{Q}(\sqrt{-3})$	0	-3
P_{10}	$\mathbb{Q}(\sqrt{37})$	$-3260047059360000\sqrt{37} + 19830091900536000$	-148

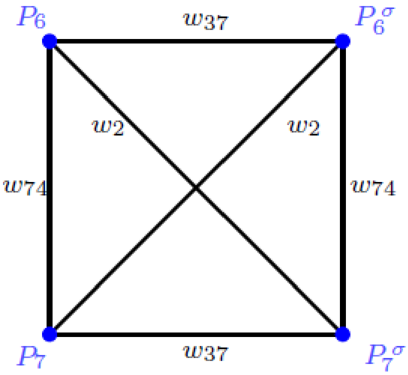

P_1
w_{74}
P_1^σ
w_2
w_2
w_{37}
w_{37}
P_2
w_{74}
P_2^σ

P_3
w_{37}
P_3^σ
w_2
w_2
w_{74}
w_{74}
P_4
w_{37}
P_4^σ

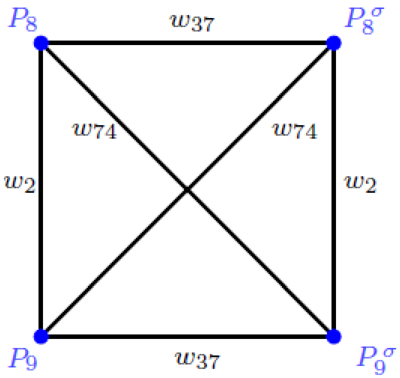


P_5
P_5^σ
$w2$
$w37$
$w74$
$w2$



P_{10}
P_{10}^σ
$w37$
$w2$
$w74$
$w37$


P_6
w_{37}
P_6^σ
w_2
w_2
w_{74}
w_{74}
P_7
w_{37}
P_7^σ


P_8
w_{37}
P_8^σ
w_{74}
w_{74}
w_2
w_2
P_9
w_{37}
P_9^σ

Higher-degree points

Box, Gajović and Goodman find all the cubic points on $X_0(N)$ for $N \in \{53, 57, 61, 65, 67, 73\}$, and all the quartic points on $X_0(65)$.

Possible future work:

- classifying points on hyperelliptic $X_0(N)^*$ for non-squarefree N
- higher genus $X_0(N)^*$ or
- $X_0(N)$

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, Compositio mathematica 159-6, 1111–1152, 2023
- 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