Rational points on modular curves and quadratic Chabauty

Jennifer Balakrishnan

Boston University

VaNTAGe
February 11, 2025

Rational points on higher genus curves

Gerd Faltings
MFO

Theorem (Faltings, 1983)

The set of rational points on a curve $X/\mathbf{Q}$ of genus 2 or more is always finite.

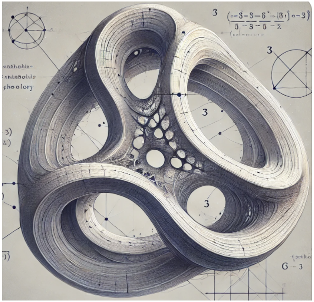
Faltings' theorem is **not** constructive.

Motivating problem:
Given a curve $X/\mathbf{Q}$ with genus $g \geqslant 2$, compute the set $X(\mathbf{Q})$.

Motivating problem:
Given a curve $X/\mathbf{Q}$ with genus $g \geqslant 2$, compute the set $X(\mathbf{Q})$.

What makes a curve difficult to compute with—or what might make a curve more amenable to computation?

Which curves are interesting to study?

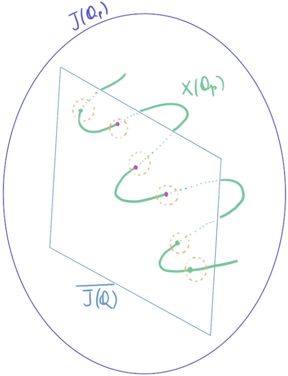


A curve, by DALL-E 3

What is known about computing $X(\mathbf{Q})$ when $g \geqslant 2$?

For *certain* curves X of genus at least 2, by associating other geometric objects to X, we can explicitly compute a slightly larger (but importantly, **finite**) set of points containing $X(\mathbf{Q})$, and then (hopefully) use this set to determine $X(\mathbf{Q})$.

- This program starts with the Chabauty–Coleman method, where one embeds the curve into its Jacobian J.
- This construction relies on the Mordell–Weil rank r of the Jacobian being less than the genus and uses analysis over $\mathbf{Q}_p$.
- What about $r \geqslant g$? (More soon!)



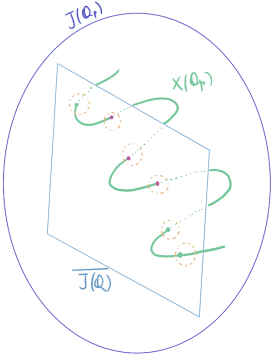
Chabauty's theorem

Theorem (Chabauty, '41)

Let X be a curve of genus $g \geqslant 2$ over $\mathbf{Q}$. Suppose the Mordell-Weil rank r of $J(\mathbf{Q})$ is less than g. Then $X(\mathbf{Q})$ is finite.

Coleman ('85) made Chabauty's theorem effective:

- He gave an upper bound on $\#(X(\mathbf{Q}_p) \cap \overline{J(\mathbf{Q})})$.
- Idea: construct functions (p-adic integrals of regular 1-forms) on $J(\mathbf{Q}_p)$ that vanish on $\overline{J(\mathbf{Q})}$ and restrict them to $X(\mathbf{Q}_p)$.
- Since $X(\mathbf{Q}) \subset X(\mathbf{Q}_p) \cap \overline{J(\mathbf{Q})}$, this gives an upper bound on $\#X(\mathbf{Q})$.



The method of Chabauty–Coleman

Let $p > 2$ be a prime of good reduction for X. Fix $b \in X(\mathbf{Q})$. Embed X into its Jacobian J via the Abel-Jacobi map $\iota : X \hookrightarrow J$, sending $P \mapsto [(P) - (b)]$.

The map $H^0(J_{\mathbf{Q}_p}, \Omega^1) \longrightarrow H^0(X_{\mathbf{Q}_p}, \Omega^1)$ induced by ι is an isomorphism of $\mathbf{Q}_p$-vector spaces. Suppose ω_J restricts to ω.

Robert Coleman
MFO

Then for $Q, Q' \in X(\mathbf{Q}_p)$, define the *Coleman integral*

$$\int_Q^{Q'} \omega := \int_0^{[(Q')-(Q)]} \omega_J.$$

Computing rational points via Chabauty–Coleman

If $r < g$, there exists an *annihilating differential* $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$ such that

$$\int_b^P \omega = 0$$

for all $P \in X(\mathbf{Q})$. Thus by studying the zeros of $\int \omega$, we can find a finite set of p-adic points containing the rational points of X.

We have

$$X(\mathbf{Q}) \subset X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0 \right\}$$

for a p-adic line integral $\int_b^* \omega$, with $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

By counting the number of zeros of such an integral, Coleman gave the bound

$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$

We would like to compute an annihilating differential ω and then calculate the finite set of p-adic points $X(\mathbf{Q}_p)_1$.

Example: Computing an annihilating differential

The curve $X_0(37)$, given as $y^2 = -x^6 - 9x^4 - 11x^2 + 37$ has $\operatorname{rk} J_0(37)(\mathbf{Q}) = 1$.

We see $\{(\pm 1, \pm 4)\} \subset X(\mathbf{Q})$, and we set $b = (-1, 4) \in X(\mathbf{Q})$ as our basepoint.

- We have $H^0(X_{\mathbf{Q}_p}, \Omega^1) = \langle \frac{dx}{y}, \frac{x\,dx}{y} \rangle$.
- Since $r = 1 < 2 = g$, we can compute $X(\mathbf{Q}_p)_1$ as the zero set of a p-adic integral. Take $p = 3$.
- The point $P := [(1, -4) - (-1, 4)] \in J_0(37)(\mathbf{Q})$ is non-torsion, as can be seen by computing the 3-adic Coleman integral

$$\int_P \frac{x\,dx}{y} = 3^2 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^5 + 3^7 + O(3^9).$$

Moreover, $\int_P \frac{dx}{y} = O(3^9)$. Thus we may take $\frac{dx}{y}$ as our annihilating differential.

Example: from an annihilating differential to $X(\mathbf{Q}_p)_1$

The curve $X_0(37)$, given as

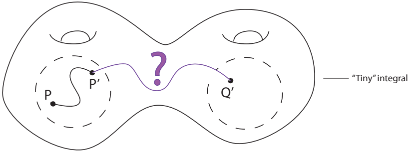
$$y^2 = -x^6 - 9x^4 - 11x^2 + 37$$

has $\mathrm{rk}\, J_0(37)(\mathbf{Q}) = 1$ and $\{(\pm 1, \pm 4)\} \subset X(\mathbf{Q})$.

- We compute the Chabauty–Coleman set $X(\mathbf{Q}_3)_1$ by solving the equation
$$\int_b^z \frac{dx}{y} = 0$$
for $z \in X(\mathbf{Q}_3)$.
- The set $X(\mathbf{Q}_3)_1 := \{z \in X(\mathbf{Q}_3) : \int_b^z \frac{dx}{y} = 0\}$ is finite, and $X(\mathbf{Q})$ is contained in this set.

p-adic integration

Coleman integrals are *p*-adic *line integrals*.



p-adic line integration is difficult – how do we construct the correct path?

- We can construct local ("tiny") integrals easily, but extending them to the entire space is challenging.
- Coleman's solution: *analytic continuation along Frobenius*, giving rise to a theory of *p*-adic line integration satisfying the usual nice properties: linearity, additivity, change of variables, fundamental theorem of calculus.
- Implementations in SageMath, Julia, and Magma.

Example: $X_0(37)(\mathbf{Q}_3)_1$

Consider $X_0(37)$, given as

$$y^2 = -x^6 - 9x^4 - 11x^2 + 37.$$

We want to compute $X(\mathbf{Q}_3)_1 := \{z \in X(\mathbf{Q}_3) : \int_b^z \frac{dx}{y} = 0\}$, which we do in each residue disk.

- Over $\mathbf{F}_3$, these are the rational points of $X_0(37)$: $\overline{(0,1)}, \overline{(0,2)}, \overline{(1,1)}, \overline{(1,2)}, \overline{(2,1)}, \overline{(2,2)}$, which correspond to the residue disks.
- We start in the residue disk of $\overline{(0,1)}$. We take

  $$S_0 = (0, 1 + 2 \cdot 3^2 + 3^4 + 2 \cdot 3^5 + 3^7 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10})),$$

  at which we compute our local coordinate, producing

  $$\begin{aligned} S_t = (t, &-3788 + O(3^{10}) + (2159 + O(3^{10}))t^2 - \\ &(15737 + O(3^{10}))t^4 - (23833 + O(3^{10}))t^6 + \\ &(746 \cdot 3^3 + O(3^{10}))t^8 + O(t^{10})) \\ =: &\ (x(t), y(t)). \end{aligned}$$

Example: $X_0(37)(\mathbf{Q}_3)_1$

- We compute the zeros of the power series $I(3T)$, where

$$I(T) = \int_{(-1,4)}^{S_0} \frac{dx}{y} + \int_{S_0}^{S_T} \frac{dx(t)\,dt}{y(t)}.$$

We find

$$\begin{aligned} I(3T) &= \left(3 + 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 3^6 + 3^7 + 2\cdot 3^8 + 3^9 + 3^{10} + O(3^{11})\right) T + \\ &= \left(3^2 + 2\cdot 3^4 + 2\cdot 3^5 + 3^7 + 2\cdot 3^8 + 2\cdot 3^9 + 3^{10} + O(3^{12})\right) T^3 + \\ &= \left(3^6 + 3^7 + 2\cdot 3^8 + 3^9 + 3^{10} + 3^{11} + 2\cdot 3^{13} + 2\cdot 3^{14} + O(3^{15})\right) T^5 + \\ &= \left(3^8 + 2\cdot 3^9 + 3^{10} + 2\cdot 3^{11} + 2\cdot 3^{12} + 2\cdot 3^{13} + 2\cdot 3^{15} + O(3^{17})\right) T^7 + \\ &= \left(3^7 + 2\cdot 3^8 + 2\cdot 3^{10} + 2\cdot 3^{11} + 3^{12} + 3^{14} + 2\cdot 3^{16} + O(3^{17})\right) T^9 + O(T^{10}), \end{aligned}$$

which has precisely one zero at $T = 0$, corresponding to S_0, which we can identify, after fixing a choice of $\sqrt{37} \in \mathbf{Q}_3$, as $(0, \sqrt{37})$.

- Parametrizing each residue disk by a local coordinate and computing the zeros of $I(3T)$ in each disk, we find that $X_0(37)(\mathbf{Q}_3)_1 = \{(0, \pm\sqrt{37}), (\pm 1, \pm 4)\}$. Thus $X_0(37)(\mathbf{Q}) = \{(\pm 1, \pm 4)\}$.

On luck

It was fairly lucky that

$$X_0(37)(\mathbf{Q}_3)_1 = \{(0, \pm\sqrt{37}), (\pm 1, \pm 4)\}:$$

- We can't always choose a small good prime p to run Chabauty–Coleman, and by the Weil bound, we know $\#X(\mathbf{F}_p)$ grows as p grows. (Counterpoint: one may also use a small bad prime! This is work of Katz–Zureick-Brown.)
- So if we'd used larger p, we'd expect more p-adic points in $X(\mathbf{Q}_p)_1$. This would then necessitate other tools, such as the Mordell–Weil sieve, to rule out points not in $X(\mathbf{Q})$.
- Relatedly, we were able to recognize the points in $X_0(37)(\mathbf{Q}_3)_1$ that weren't in $X(\mathbf{Q})_{\text{known}}$ as points in $X(\mathbf{Q}(\sqrt{37}))$.

Beyond Chabauty–Coleman

Do we have any hope of doing something like Chabauty–Coleman when $r \geqslant g$?

- Conjecturally, yes, via Kim's *nonabelian Chabauty* program.
- Instead of using the Jacobian of X and abelian integrals, use *nonabelian geometric objects* associated to X, which carry *iterated* Coleman integrals.
- These iterated integrals cut out Selmer varieties, which give a sequence of sets

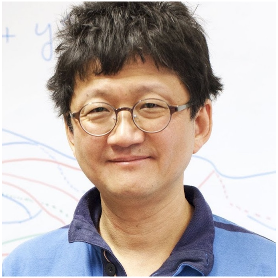
  $$X(\mathbf{Q}) \subset \cdots \subset X(\mathbf{Q}_p)_n \subset X(\mathbf{Q}_p)_{n-1} \subset \cdots \subset X(\mathbf{Q}_p)_2 \subset X(\mathbf{Q}_p)_1$$

  where the depth n set $X(\mathbf{Q}_p)_n$ is given by equations in terms of n-fold iterated Coleman integrals

  $$\int_b^P \omega_n \cdots \omega_1.$$

- Note that $X(\mathbf{Q}_p)_1$ is the classical Chabauty–Coleman set.

Nonabelian Chabauty



Conjecture (Kim, '12)

For $n \gg 0$, the set $X(\mathbf{Q}_p)_n$ is finite.

Questions:

- When can $X(\mathbf{Q}_p)_n$ be shown to be finite?
- For which classes of curves can nonabelian Chabauty be used to determine $X(\mathbf{Q})$?

We focus today on the case of $n = 2$, known as *quadratic Chabauty*.

Quadratic Chabauty: pre-history

JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 24, Number 1, January 2011, Pages 281–291
S 0894-0347(2010)00675-3
Article electronically published on August 2, 2010

APPENDIX AND ERRATUM TO "MASSEY PRODUCTS FOR ELLIPTIC CURVES OF RANK 1"

JENNIFER S. BALAKRISHNAN, KIRAN S. KEDLAYA, AND MINHYONG KIM

The paper [6] contains a few errors in the basic assumptions as well as in the formula of Corollary 0.2. First of all, it should have been made clear at the outset that the regular model $\mathcal{E}$ for the elliptic curve E must be the minimal regular model, and $\mathcal{X}$ the complement of the origin in the regular minimal model. Similarly, the tangential base-point b must be integral, in that it is a $\mathbb{Z}$-basis of the relative tangent space $e^*T_{\mathcal{E}/\mathbb{Z}}$. It could also be an integral two-torsion point for the arguments of the paper to hold verbatim.

The most significant error is in the contribution of the local terms at $l \neq p$, that is, Lemma 1.2. The problem is that a point that is integral on $\mathcal{X}$ may not be integral on a smooth model over a field of good reduction. As it stands, the lemma will only apply to points that are integral in this stronger sense.

However, to get immediate examples, one can replace the lemma by

Lemma 1.2′. *Suppose the Neron model of E has only one rational component for each prime. (Equivalently, the Tamagawa number is one at each prime.) Then the map*

$$\mathcal{X}(\mathbb{Z}_l) \to H^1(G_l, U_2)$$

is trivial for every $l \neq p$.

Therefore, for the function

$$\mathcal{X}(\mathbb{Z}_p) \xrightarrow{j_{2,loc}^{et}} H^1_f(G_p, U_2) \xrightarrow{\psi^p} H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

constructed via the refined Massey product, we get

Theorem 0.1′. *Suppose the Neron model of E has only one rational component for each prime. Then the map*

$$\psi^p \circ j_{2,loc}^{et}$$

vanishes on the global points $\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)$.

The first quadratic Chabauty formula, for integral points on punctured rank 1 elliptic curves:

Corollary 0.2′. *In addition to the assumptions of the theorem, suppose there is a point y of infinite order in $\mathcal{E}(\mathbb{Z})$. Then*

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{E}(\mathbb{Z}_p)$$

is in the zero set of

$$(\log_\alpha(y))^2 D_2(z) - (\log_\alpha(z))^2 D_2(y).$$

The proof of Theorem 0.1′ is identical to that of Theorem 0.1, once we have replaced Lemma 1.2 by Lemma 1.2′.

Shortly after we had finished this, Minhyong Kim generously shared another insight about this formula: *the double integral D_2 is "essentially the log of Mazur and Tate's sigma function."*

What are p-adic heights?

Let p be an odd prime and let A be an abelian variety over a number field K with good reduction at p.

- A (global) p-adic height pairing is a symmetric bilinear pairing
$$(\quad , \quad) : A(K) \times A^{\vee}(K) \to \mathbf{Q}_p.$$
- p-adic height pairings were
  - First defined for abelian varieties by Schneider ('82), Mazur-Tate ('83),
  - extended to motives by Nekovář ('93), and
  - also defined, in the case of Jacobians of curves, by Coleman and Gross ('89).
  - This third definition is known to be equivalent to the previous ones (Besser, '04).
- A global height pairing h can be written as a sum of local height pairings $h = \sum_v h_v$.

Quadratic Chabauty (roughly)

Given a global p-adic height h, we study it on rational points:

$$\underbrace{h}_{\substack{\text{bilinear form, rewrite in terms}\\ \text{of locally analytic function}\\ \text{using known rational points}}} = \underbrace{h_p}_{\substack{\text{locally analytic function}\\ \text{via } p\text{-adic differential equation}}} + \underbrace{\sum_{v \neq p} h_v}_{\substack{\text{takes on finite}\\ \text{number of values}\\ \text{on rational points}\\ \text{(best case: all trivial)}}}$$

Quadratic Chabauty (roughly)

$$\underbrace{h}_{\substack{\text{quadratic form, rewrite as a} \\ p\text{-adic analytic function} \\ \text{using Coleman integrals}}} = \underbrace{h_p}_{\substack{p\text{-adic analytic function} \\ \text{via double Coleman integral}}} + \underbrace{\sum_{v \neq p} h_v}_{\substack{\text{takes on finite} \\ \text{number of values} \\ \text{(controlled in some way)}}}$$

$$\underbrace{h_p}_{\substack{p\text{-adic analytic function} \\ \text{via double Coleman integral}}} - \underbrace{h}_{\substack{\text{quadratic form, rewrite as a} \\ p\text{-adic analytic function} \\ \text{using Coleman integrals}}} = - \underbrace{\sum_{v \neq p} h_v}_{\substack{\text{takes on finite} \\ \text{number of values} \\ \text{(controlled in some way)}}}$$

Quadratic Chabauty for integral points

Theorem (B–Besser–Müller '16)

Let $X/\mathbf{Q}$ be a hyperelliptic curve. If $r = g \geqslant 2$ and $f_i(x) := \int_b^x \omega_i$ for $\omega_i \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$ are linearly independent, then there is an explicitly computable finite set $S \subset \mathbf{Q}_p$ and explicitly computable constants $\alpha_{ij} \in \mathbf{Q}_p$ such that

$$\theta(P) - \sum_{0 \leqslant i \leqslant j \leqslant g-1} \alpha_{ij} f_i f_j(P),$$

takes values in S on integral points, where $\theta(P) = \sum_{i=0}^{g-1} \int_b^P \omega_i \bar{\omega}_i$.

Quadratic Chabauty for *rational points*

Theorem (B–Dogra '18)

For $X/\mathbf{Q}$ with $g \geqslant 2$ and $r < g + \operatorname{rk} NS(J_{\mathbf{Q}}) - 1$, the set $X(\mathbf{Q}_p)_2$ is finite.

We also gave a quadratic Chabauty formula for bielliptic curves with $g = r = 2$ and, with Müller, used it to determine $X_0(37)(\mathbf{Q}(i))$.

Together with Dogra, Müller, Tuitman, and Vonk, we sought to generalize these quadratic Chabauty techniques to curves beyond hyperelliptic ones.

- The main application that we had in mind was a certain genus 3 non-hyperelliptic *modular curve*, coming from Serre's uniformity problem.

Serre's uniformity problem

Let $E/\mathbf{Q}$ be an elliptic curve, ℓ a prime number.

- $G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the ℓ-torsion points $E[\ell]$.
- Fixing a basis of $E[\ell] \cong (\mathbf{Z}/\ell\mathbf{Z})^2$, get a Galois representation

$$\bar{\rho}_{E,\ell} : G_{\mathbf{Q}} \to \mathrm{Aut}(E[\ell]) \cong \mathbf{GL}_2(\mathbf{F}_\ell)$$

Theorem (Serre, '72)

If E does not have complex multiplication, then $\bar{\rho}_{E,\ell}$ is surjective for $\ell \gg 0$.

Serre's uniformity problem: Does there exist an absolute constant ℓ_0 such that $\bar{\rho}_{E,\ell}$ is surjective for every non-CM elliptic curve $E/\mathbf{Q}$ and every prime $\ell > \ell_0$?

Conjecture: $\ell_0 = 37$ should work.

Serre's Uniformity Problem

Idea: To show that $\bar{\rho}_{E,\ell}$ is surjective, show that $\mathrm{im}(\bar{\rho}_{E,\ell})$ is not contained in a maximal subgroup of $\mathbf{GL}_2(\mathbf{F}_\ell)$. These are

1. Borel subgroups
2. Exceptional subgroups
3. Normalizers of split Cartan subgroups
4. Normalizers of non-split Cartan subgroups

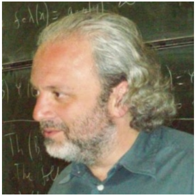
Idea: For a maximal $G \subset \mathbf{GL}_2(\mathbf{F}_\ell)$, there is a modular curve $X_G/\mathbf{Q}$ such that non-cuspidal points in $X_G(\mathbf{Q})$ correspond to elliptic curves $E/\mathbf{Q}$ with $\mathrm{im}(\bar{\rho}_{E,\ell}) \subset G$.

The "cursed" modular curve

Bilu, Parent, and Rebolledo proved a spectacular result about essentially all split Cartan modular curves:

Theorem (Bilu–Parent '11, Bilu–Parent–Rebolledo '13)
We have $X_s^+(\ell)(\mathbf{Q}) = \{\textit{cusps, CM-points}\}$ *for* $\ell \geqslant 11$, $\ell \neq 13$.

....yes, except for one: the one at "cursed" level 13.


Bilu


Parent


Rebolledo

Quadratic Chabauty and the cursed curve

The split Cartan modular curve $X_s^+(13)$, given as

$$-x^3y+2x^2y^2-xy^3-x^3z+x^2yz+xy^2z-2xyz^2+2y^2z^2+xz^3-3yz^3=0$$

was referred to as “cursed” (Bilu–Parent–Rebolledo), after their classification of rational points on *essentially all other* split Cartan modular curves.

This is a genus $g=3$ curve that was known to have larger Jacobian rank ($r \geqslant g$; it turned out $r=g$). Our goal was to apply quadratic Chabauty to determine its rational points.

Abel–Jacobi with basepoint

Let AJ_b be the map

$$X(\mathbf{Q}_p) \xrightarrow{AJ_b} H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$$
$$x \mapsto (\omega \mapsto \int_b^x \omega).$$

Quadratic Chabauty function

A quadratic Chabauty function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ has these properties:

1. On each residue disk, the map $(AJ_b, \theta) : X(\mathbf{Q}_p) \to H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \times \mathbf{Q}_p$ is locally analytic.
2. There exist
   - an endomorphism E of $H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$,
   - a functional $c \in H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$, and
   - a bilinear form

   $$B : H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \to \mathbf{Q}_p$$

   such that for all $x \in X(\mathbf{Q})$,

   $$\theta(x) - B(AJ_b(x), E(AJ_b(x)) + c) = 0.$$

Quadratic Chabauty functions for rational points

When $r = g$ and $\operatorname{rk} NS(J) > 1$, we construct a quadratic Chabauty function by associating to points of X certain p-adic Galois representations, and then take Nekovář p-adic heights.

- Idea is to construct a representation $A_Z(x)$ for every $x \in X(\mathbf{Q})$. This depends on a choice of "nice" correspondence Z on X, given by nontrivial elements of $\ker(NS(J) \to NS(X) \simeq \mathbf{Z})$. Such a correspondence exists when $\operatorname{rk} NS(J) > 1$.
- Compute p-adic height of $A_Z(x)$ via p-adic Hodge theory.
- It turns out that for many interesting curves, for all $v \neq p$, local heights $h_v(A_Z(x))$ are trivial (e.g., if X has potential good reduction at v).

Quadratic Chabauty for rational points

Using Nekovář's p-adic height h, there is a local decomposition

$$h(A_Z(x)) = h_p(A_Z(x)) + \sum_{v \neq p} h_v(A_Z(x))$$

where

- $x \mapsto h_p(A_Z(x))$ extends to a locally analytic function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ by Nekovář's construction.

This gives a quadratic Chabauty function whose pairing is h and whose endomorphism is induced by Z.

Quadratic Chabauty (with Dogra, Müller, Tuitman, Vonk)

Suppose $X/\mathbf{Q}$ satisfies

- $r = g$,
- $\operatorname{rk} NS(J_{\mathbf{Q}}) > 1$,
- p-adic closure $\overline{J(\mathbf{Q})}$ has finite index in $J(\mathbf{Q}_p)$,
- X has everywhere potential good reduction (or otherwise some control of local heights away from p),
- and that we know enough rational points $P_i \in X(\mathbf{Q})$ to "fit" the global height pairing in terms of a basis of bilinear forms.

If we can solve the following problems, we have an algorithm for computing a finite subset of $X(\mathbf{Q}_p)$ containing $X(\mathbf{Q})$:

1. Expand the function $x \mapsto h_p(A_Z(x))$ into a p-adic power series on every residue disk.
2. Evaluate $h(A_Z(P_i))$ for the known rational points $P_i \in X(\mathbf{Q})$.

Applying quadratic Chabauty to the cursed curve

- We showed that $X_s^+(13)$ has $r = 3$.
- Since $\operatorname{rk} NS(J_{\mathbf{Q}}) = 3$, we had two independent nontrivial nice correspondences Z_1, Z_2 on X; we computed equations for 17-adic heights h^{Z_1}, h^{Z_2} on X.
- Checked the simultaneous solutions of the above two equations...are they precisely on the 7 known rational points?!

Quadratic Chabauty for rational points on $X_s^+(13)$

Theorem (B–Dogra–Müller–Tuitman–Vonk '19)
We have $|X_s^+(13)(\mathbf{Q})| = 7$.

This completes the classification of rational points on split Cartan curves by Bilu–Parent–Rebolledo.

Baran showed that $X_{\mathrm{s}}^+(13)$ is isomorphic to $X_{\mathrm{ns}}^+(13)$ over $\mathbf{Q}$, so we also get (for free) that $|X_{\mathrm{ns}}^+(13)(\mathbf{Q})| = 7$.

Two *new* formulations of quadratic Chabauty

Edixhoven–Lido (2019): Geometric quadratic Chabauty

J. Inst. Math. Jussieu (2023), **22**(1), 279–333
doi:10.1017/S1474748021000244 279

GEOMETRIC QUADRATIC CHABAUTY

BAS EDIXHOVEN AND GUIDO LIDO

Mathematisch Instituut Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
(edix@math.leidenuniv.nl, guidomaria.lido@gmail.com)

(Received 22 August 2020; revised 10 May 2021; accepted 11 May 2021; first published online 17 June 2021)

Abstract Since Faltings proved Mordell's conjecture in [16] in 1983, we have known that the sets of rational points on curves of genus at least 2 are finite. Determining these sets in individual cases is still an unsolved problem. Chabauty's method (1941) [10] is to intersect, for a prime number p, in the p-adic Lie group of p-adic points of the Jacobian, the closure of the Mordell–Weil group with the p-adic points of the curve. Under the condition that the Mordell–Weil rank is less than the genus, Chabauty's method, in combination with other methods such as the Mordell–Weil sieve, has been applied successfully to determine all rational points in many cases.

Minhyong Kim's nonabelian Chabauty programme aims to remove the condition on the rank. The simplest case, called quadratic Chabauty, was developed by Balakrishnan, Besser, Dogra, Müller, Tuitman and Vonk, and applied in a tour de force to the so-called cursed curve (rank and genus both 3).

This article aims to make the quadratic Chabauty method *small* and *geometric* again, by describing it in terms of only 'simple algebraic geometry' (line bundles over the Jacobian and models over the integers).

Besser–Müller–Srinivasan (2021): p-adic Arakelov theoretic quadratic Chabauty

p-ADIC ADELIC METRICS AND QUADRATIC CHABAUTY I

AMNON BESSER, J. STEFFEN MÜLLER, AND PADMAVATHI SRINIVASAN

Abstract. We give a new construction of p-adic heights on varieties over number fields using p-adic Arakelov theory. In analogy with Zhang's construction of real-valued heights in terms of adelic metrics, these heights are given in terms of p-adic adelic metrics on line bundles. In particular, we describe a construction of canonical p-adic heights on abelian varieties and we show that we recover the canonical Mazur–Tate height and, for Jacobians, the height constructed by Coleman and Gross. Our main application is a new and simplified approach to the Quadratic Chabauty method for the computation of rational points on certain curves over the rationals, by pulling back the canonical height on the Jacobian with respect to a carefully chosen line bundle. We show that our construction allows us to reprove, without using p-adic Hodge theory or arithmetic fundamental groups, several results due to Balakrishnan and Dogra. Our method also extends to primes p of bad reduction. One consequence of our work is that for any canonical height (p-adic or $\mathbb{R}$-valued) on an abelian variety (and hence on pull-backs to other varieties), the local contribution at a finite prime q can be constructed using q-analytic methods.

The modular curves $X_0^+(p)$

The modular curves $X_0^+(p) := X_0(p)/\langle w_p \rangle$ for prime level p provide an interesting testing ground for quadratic Chabauty.

- Moduli perspective: non-cuspidal points classify unordered pairs $\{E_1, E_2\}$ of elliptic curves admitting a p-isogeny between them.
- Rational points are cusps, CM points, or "exceptional" (neither cusps nor CM points).
- Elkies (1998), Galbraith (2002): Computed models, searched for rational points, and asked if for all large primes p, only rational points are cusps or CM points.

The modular curves $X_0^+(p)$

- By work of Ogg, the modular curve $X_0^+(p)$ has genus 3 if and only if

$$p \in \{97, 109, 113, 127, 139, 149, 151, 179, 239\}.$$

- For all of these curves, $\operatorname{rk} J_0^+(p)(\mathbf{Q}) = 3$.

Using models of these (smooth plane quartic) curves computed by Elkies, we can apply quadratic Chabauty to show the following:

Theorem (B.–Dogra–Müller–Tuitman–Vonk ’23)

There are no exceptional rational points on the genus 3 modular curves $X_0^+(p)$.

The modular curves $X_0^+(p)$

The curve $X_0^+(p)$ has genus 4 iff

$$p \in \{137, 173, 199, 251, 311\},$$

genus 5 iff

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

and genus 6 iff

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

Nikola Adžaga, Vishal Arul, Lea Beneish, Mingjie Chen, Shiva Chidambaram, Timo Keller, Boya Wen started looking at the $X_0^+(p)$ of genus 4, 5, and 6 at the 2020 Arizona Winter School.

They used quadratic Chabauty to determine rational points on all such curves and proved the following:

Theorem (AABCCKW '22)

The only exceptional rational points on the genus 4, 5, and 6 curves $X_0^+(p)$ occur at level $p = 137$ or 311.

Quadratic Chabauty and Galbraith's conjecture

$X_0^+(N)$ with $2 \leqslant g(X_0^+(N)) \leqslant 6$, with N prime

- B.–Best–Bianchi–Lawrence–Müller–Triantafillou–Vonk ($g = 2$: $N = 67, 73, 103$)
- B.–Dogra–Müller–Tuitman–Vonk ($g = 2, 3$, $N = 107, 167, 191; 97, 109, 113, 127, 139, 149, 151, 179, 239$)
- Adžaga–Arul–Beneish–Chen–Chidambaram–Keller–Wen ($g = 4, 5, 6$: $N = 137, 173, 199, 251, 311; 157, 181, 227, 263; 163, 197, 211, 223, 269, 271, 359$)

$X_0^+(N)$, with N composite

- $N = 91$: B.–Besser–Bianchi–Müller
- $N = 125$: Arul–Müller
- $N = 169$: B.–Dogra–Müller–Tuitman–Vonk

Collectively, these results, plus work of Momose, Galbraith, and Arai–Momose settle a 2002 conjecture of Galbraith: that if $2 \leqslant g(X_0^+(N)) \leqslant 5$, then $X_0^+(N)(\mathbf{Q})$ contains exceptional rational points if and only if $N \in \{73, 91, 103, 125, 137, 191, 311\}$.

Quadratic Chabauty for modular curves

- With Dogra, Müller, Tuitman, and Vonk, we generalized our techniques and developed quadratic Chabauty algorithms for further modular curves over $\mathbf{Q}$.
- In addition to the Atkin–Lehner quotient curves, we computed rational points on curves motivated by the problem of classifying ℓ-adic images of Galois attached to elliptic curves (a suggestion of Rouse, Sutherland, and Zureick-Brown).

Theorem (BDMTV '23)

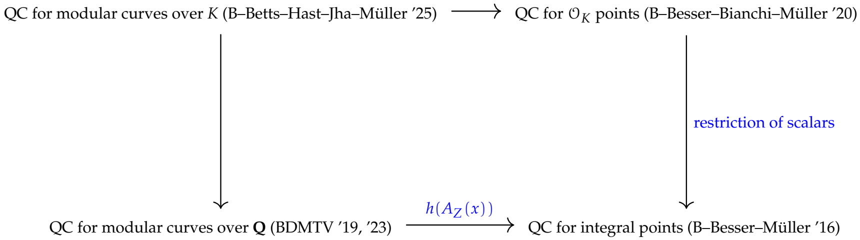
We have $\#X_{S_4}(13)(\mathbf{Q}) = 4$ *and* $\#X_{\mathrm{ns}}^{+}(17)(\mathbf{Q}) = 7$.

These computations finished the classification of 13-adic and 17-adic images.

A Magma package is available on GitHub.

Our most recent quadratic Chabauty roadmap

Idea: for *certain* (modular) curves X over number fields K of genus at least 2, we can explicitly compute a slightly larger (but importantly, **finite**) set of points containing $X(K)$, and then (hopefully) from this set, extract $X(K)$.



Nonabelian Chabauty over number fields?

- Dogra ('19) and Hast ('20): finiteness theorems over number fields.
- In work with Besser, Bianchi, and Müller ('20), we gave explicit quadratic Chabauty methods for integral points on hyperelliptic curves over number fields (and K-rational points on genus 2 bielliptic curves), using multiple p-adic heights and restriction of scalars.

More on p-adic heights

For curves X/K, unlike the $\mathbf{R}$-valued canonical height, there may be *many* canonical p-adic valued heights associated to the curve's Jacobian for a given number field K.

- Up to nontrivial scalar multiple:

  $$\{\text{canonical } p\text{-adic height pairings}\} \stackrel{1:1}{\longleftrightarrow} \{\mathbf{Z}_p\text{-extensions } L/K\},$$

  where L has finitely many ramified primes and these primes are primes of ordinary reduction for J.
- So over K real quadratic, the situation is essentially the same as it was over $\mathbf{Q}$: just the cyclotomic p-adic height h^{cyc}
- Over K imaginary quadratic, have cyclotomic h^{cyc} and anticyclotomic h^{anti} p-adic heights.

Remarks

- For $V = \mathrm{Res}_{K/\mathbf{Q}} X$ and $A = \mathrm{Res}_{K/\mathbf{Q}} J$, one can check finiteness of the intersection

$$V(\mathbf{Q}_p) \cap \overline{A(\mathbf{Q})}$$

  for a given example by computing Coleman integrals.

  Difficult to prove finiteness in general. 🤔
- Siksek asked whether a sufficient condition for finiteness of the Chabauty–Coleman set $X(K_{\mathfrak{p}})_1$ is that $r \leqslant [K : \mathbf{Q}](g-1)$ with X not defined over any proper subfield of K.
- Dogra ('19) showed that this question has a negative answer.
- Triantafillou ('20) gave applications of restrictions of scalars Chabauty to study solutions to the S-unit equation.

Quadratic Chabauty over number fields

Suppose X/K, where $[K:\mathbf{Q}] = d = r_1 + 2r_2$.

- Siksek's restriction of scalars method generically works for $\operatorname{rk} J(K) + d \leqslant dg$.

In work with Besser, Bianchi, and Müller, extended quadratic Chabauty to approximate the $\mathcal{O}_K$-points on hyperelliptic X:

- There are at least $r_2 + 1$ independent p-adic heights.
- Generically, this approach works for

$$\operatorname{rk} J(K) + (d - (r_2 + 1)) \leqslant dg$$
$$\operatorname{rk}(J(K)) + \operatorname{rk}(\mathcal{O}_K^\times) \leqslant dg.$$

More on Mazur's Program B

Rouse–Sutherland–Zureick-Brown ('21) describe the classification of possible images of ℓ-adic Galois representations attached to elliptic curves E over $\mathbf{Q}$ (Mazur's "Program B").

- The case of $\ell = 2$ was completed by Rouse–Zureick-Brown and $\ell = 13, 17$ was finished by work of [BDMTV23].
- The work of [RSZB21] focuses on $\ell = 3, 5, 7, 11$: they classify rational points on almost all maximal ℓ-power level modular curves, aside from those dominating two modular curves of level 49 and genus 9 and the non-split Cartan curves of level 27, 25, 49, 121, and prime level greater than 17.
- The case of $X_{\text{ns}}^{+}(27)$ is particularly interesting: it would finish the classification of 3-adic images of Galois.

$X_{ns}^{+}(27)$ and quadratic Chabauty over number fields

The curve $X := X_{ns}^{+}(27)$ has genus 12 and rank 12 and satisfies the hypotheses of the [BDMTV23] algorithm.

- And yet it seems to be computationally infeasible to work directly with this curve using [BDMTV23]!

[RSZB21] identify a *smooth plane quartic* curve X'_H over $K = \mathbf{Q}(\zeta_3)$ together with a degree 3 morphism $X \to X'_H$ defined over K, and so every K-point of X maps to a K-point of X'_H.

- The restriction of scalars $\mathrm{Res}_{K/\mathbf{Q}} J(X'_H)$ is isogenous to the $\mathbf{Q}$-simple abelian variety associated to `729.2.a.c` with **rank 6**.

Quadratic Chabauty for curves over number fields

By combining quadratic Chabauty for modular curves with restriction of scalars, it should be possible to study $X'_H(K)$, even though it is a genus $g = 3$ curve with Jacobian rank $r = 6$ since

$$\begin{aligned} r &\leqslant [K : \mathbf{Q}](g-1) + (r_2+1)(r_{NS}-1), \\ &= \quad 2 \cdot (3-1) + (1+1)(3-1) = 8, \end{aligned}$$

where r_2 is the number of pairs of complex embeddings of K.

Computing $X'_H(\mathbf{Q}(\zeta_3))$ and 3-adic images of Galois

Together with Alexander Betts, Daniel Hast, Aashraya Jha, and Steffen Müller, we have combined quadratic Chabauty with restriction of scalars for this curve X'_H over $K = \mathbf{Q}(\zeta_3)$.

Theorem (BBHJM '25)

We have $\#X'_H(\mathbf{Q}(\zeta_3)) = 13$.

This yields

Theorem (BBHJM '25)

$\#X^+_{\mathrm{ns}}(27)(\mathbf{Q}) = 8$.

and completes the classification of 3-adic images of Galois, after the work of Rouse–Sutherland–Zureick-Brown.