Rational points on the cursed curve

Jennifer Balakrishnan
joint work with
Netan Dogra, Jan Steffen Müller,
Jan Tuitman, Jan Vonk

Boston University

JNT Biennial, Cetraro
July 24, 2019

Some motivation: a question about triangles

We say a *rational* triangle is one with sides of rational lengths.

Question

Does there exist a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area?

Some motivation: a question about triangles

We say a *rational* triangle is one with sides of rational lengths.

Question

Does there exist a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area?

This feels like a very classical question...perhaps studied by the ancient Greeks?

Some motivation: a question about triangles

This was the result of work by Y. Hirakawa and H. Matsumura (2019):

Journal of Number Theory 194 (2019) 297–302

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A unique pair of triangles ☆

Yoshinosuke Hirakawa, Hideki Matsumura *

Department of Science and Technology, Keio University, 14-1, Hiyoshi 3-chome, Kouhoku-ku, Yokohama-shi, Kanagawa-ken, Japan

The techniques used in their investigation are closely related to the tools used for studying the cursed curve.

A question about triangles

Assume that there exists such a pair of triangles (rational right triangle, rational isosceles triangle). By rescaling both of the given triangles, we may assume their lengths are

$$(k(1+t^2), k(1-t^2), 2kt) \quad \text{and} \quad ((1+u^2), (1+u^2), 4u),$$

respectively, for some rational numbers $0 < t, u < 1, k > 0$.

A question about triangles

Given side lengths of

$$(k(1+t^2), k(1-t^2), 2kt) \quad \text{and} \quad ((1+u^2), (1+u^2), 4u),$$

by comparing perimeters and areas, we have

$$k + kt = 1 + 2u + u^2 \qquad \text{and} \qquad k^2 t(1-t^2) = 2u(1-u^2).$$

By a change of coordinates, this is equivalent to studying rational points on the genus 2 curve given by

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^{\pm}$$

in $X(\mathbf{Q})$. We've found 10 points!

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^{\pm}$$

in $X(\mathbf{Q})$. We've found 10 points!

So we have provably determined $X(\mathbf{Q})$.

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^{\pm}$$

in $X(\mathbf{Q})$. We've found 10 points!
So we have provably determined $X(\mathbf{Q})$.

And $(12/11, 868/11^3)$ gives rise to a pair of triangles.

A question about triangles: answer

Theorem (Hirakawa–Matsumura, 2018)

Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with sides of lengths $(377, 135, 352)$ *and the isosceles triangle with sides of lengths* $(366, 366, 132)$.

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:
- Crucial hypothesis: satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:
- Crucial hypothesis: satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$
- Theorem: work of Chabauty and Coleman

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:
- Crucial hypothesis: satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$
- Theorem: work of Chabauty and Coleman
- ...and a bit of luck!

Challenges in studying rational points on curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus at least 2. The set $X(\mathbf{Q})$ is finite.

Challenges in studying rational points on curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus at least 2. The set $X(\mathbf{Q})$ is finite.

How do we find $X(\mathbf{Q})$?

- Faltings' proof is **not** constructive.
- There is another proof of finiteness due to Vojta, but it also is not constructive.
- Recent work of Lawrence–Venkatesh gives another proof of finiteness.
- Method of Chabauty–Coleman can explicitly compute $X(\mathbf{Q})$ in some cases.

Challenges in studying rational points on curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus at least 2. The set $X(\mathbf{Q})$ is finite.

How do we find $X(\mathbf{Q})$?

- Faltings' proof is **not** constructive.
- There is another proof of finiteness due to Vojta, but it also is not constructive.
- Recent work of Lawrence–Venkatesh gives another proof of finiteness.
- Method of Chabauty–Coleman can explicitly compute $X(\mathbf{Q})$ in some cases.

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

Example: Can we compute $X(\mathbf{Q})$?

Consider X:

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

Example: Can we compute $X(\mathbf{Q})$?

Consider X:

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

This is a model for the "split Cartan" modular curve $X_s(13)$.

Example: Can we compute $X(\mathbf{Q})$?

Consider X:

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

This is a model for the "split Cartan" modular curve $X_s(13)$.

The set $X(\mathbf{Q})$ contains 7 rational points (Galbraith):

$$(0:1:0),(0:0:1),(-1:0:1),$$

$$(1:0:0),(1:1:0),(0:3:2),(1:0:1).$$

Example: Can we compute $X(\mathbf{Q})$?

Consider X:

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

This is a model for the "split Cartan" modular curve $X_s(13)$.

The set $X(\mathbf{Q})$ contains 7 rational points (Galbraith):

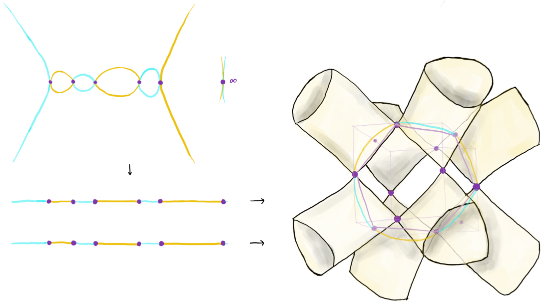
$$(0:1:0),(0:0:1),(-1:0:1),$$

$$(1:0:0),(1:1:0),(0:3:2),(1:0:1).$$

Question: Is this set of points above precisely $X(\mathbf{Q})$?

Working with higher genus curves

- For curves $X/\mathbf{Q}$ of genus at least 2, $X(\mathbf{Q})$ is just a set, so to study rational points, it helps to associate to X other objects that have more structure.
- Fix a basepoint $b \in X(\mathbf{Q})$. Embed X into its *Jacobian* J via the Abel-Jacobi map $\iota : X \hookrightarrow J$, sending $P \mapsto [(P) - (b)]$. The Mordell–Weil theorem tells us that $J(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$.
- The rank r is an important (but hard to compute) invariant.



A genus 2 curve and its Kummer surface
Sachi Hashimoto

Strategy for computing rational points on curves

Upshot: 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 story starts with the Chabauty–Coleman method.
- We will use a generalization of this (*nonabelian Chabauty*, a program initiated by Kim) to understand rational points on the cursed curve.

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 (1985) made Chabauty's theorem effective by re-interpreting this result in terms of p-adic line integrals of regular 1-forms.
- In fact, by counting the number of zeros of such an integral, Coleman gave the bound

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

Robert Coleman
MFO

The method of Chabauty–Coleman

Let $p > 2$ be a prime of good reduction for X. 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.

The method of Chabauty–Coleman

Let $p > 2$ be a prime of good reduction for X. 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.
Then for $Q, Q' \in X(\mathbf{Q}_p)$, define

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

The method of Chabauty–Coleman

Let $p > 2$ be a prime of good reduction for X. 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.
Then for $Q, Q' \in X(\mathbf{Q}_p)$, define

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

If $r < g$, there exists $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$ 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.

Recap of the method (+bonus observations)

Given a curve $X/\mathbf{Q}$ of genus $g \geqslant 2$, embed it inside its *Jacobian* J and consider the rank r of $J(\mathbf{Q})$.

- If $r < g$, we can use the Chabauty–Coleman method to compute a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.
- By studying the zeros of this integral, Coleman gave the bound
$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$
- This bound can be sharp in practice, as in the triangle example:
  - There $g = 2, r = 1$; taking $p = 5$ gave $\#X(\mathbf{F}_p) = 8$ and thus $\#X(\mathbf{Q}) \leqslant 10$.
- Regardless, the Coleman integral cuts out a finite set of p-adic points; this set contains $X(\mathbf{Q})$ as a subset.
- Even when the bound is not sharp, we can often combine Chabauty–Coleman data at multiple primes (Mordell–Weil sieve) to extract $X(\mathbf{Q})$.

Computing rational points via Chabauty–Coleman

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 $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

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: Chabauty–Coleman with $g = 2, r = 1$

Suppose we have a genus 2 curve $X/\mathbf{Q}$ with $\operatorname{rk} J(\mathbf{Q}) = 1$ and $X(\mathbf{Q}) \neq \emptyset$. Fix a basepoint $b \in X(\mathbf{Q})$.

- We know $H^0(X_{\mathbf{Q}_p}, \Omega^1) = \langle \omega_0, \omega_1 \rangle$.
- Since $r = 1 < 2 = g$, we can compute $X(\mathbf{Q}_p)_1$ as the zero set of a p-adic integral.
- If we know one more point $P \in X(\mathbf{Q})$, we can compute the constants $A, B \in \mathbf{Q}_p$:

  $$\int_b^P \omega_0 = A, \quad \int_b^P \omega_1 = B,$$

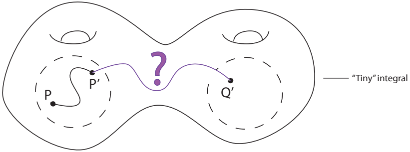
  then solve the equation

  $$f(z) := \int_b^z (B\omega_0 - A\omega_1) = 0$$

  for $z \in X(\mathbf{Q}_p)$.
- The set of such z 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.

For which curves X do we want to compute $X(\mathbf{Q})$?

There are a number of fundamental questions in number theory that come from moduli problems, in particular, understanding rational points on *modular curves*, e.g.:

Theorem (Mazur, 1977)

If $E/\mathbf{Q}$ is an elliptic curve, and $P \in E(\mathbf{Q})$ has finite order N, then $N \in \{1, \ldots, 10, 12\}$.

Idea: Find the rational points on the modular curve $X_1(N)$.

- Non-cuspidal points in $X_1(N)(\mathbf{Q})$ correspond to elliptic curves $E/\mathbf{Q}$ with a point $P \in E(\mathbf{Q})$ of order N.
- So Mazur's theorem is equivalent to the assertion that $X_1(N)(\mathbf{Q})$ consists only of cusps if $N = 11$ or $N \geqslant 13$.

Residual Galois representations

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

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

Residual Galois representations

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, 1972)

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

Residual Galois representations

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, 1972)

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 $\ell > \ell_0$?

Folklore: $\ell_0 = 37$ 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 $\mathrm{im}(\bar{\rho}_{E,\ell}) \subset G$.

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 ✓(Mazur)
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 $\mathrm{im}(\bar{\rho}_{E,\ell}) \subset G$.

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 ✓(Mazur)
2. Exceptional subgroups ✓(Serre)
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 $\mathrm{im}(\bar{\rho}_{E,\ell}) \subset G$.

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 ✓(Mazur)
2. Exceptional subgroups ✓(Serre)
3. Normalizers of split Cartan subgroups ✓(Bilu–Parent–Rebolledo)
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 $\mathrm{im}(\bar{\rho}_{E,\ell}) \subset G$.

Serre's Uniformity Problem

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

1. Borel subgroups ✓(Mazur)
2. Exceptional subgroups ✓(Serre)
3. Normalizers of split Cartan subgroups ✓(Bilu–Parent–Rebolledo)
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 $\text{im}(\bar{\rho}_{E,\ell}) \subset G$.

The cursed modular curve

All normalizers of split Cartan $G \subset \mathbf{GL}_2(\mathbf{F}_\ell)$ are conjugate, so all corresponding $X_G = X(\ell)/G$ are isomorphic. Denote $X_s(\ell) = X_G$.

Theorem (Bilu-Parent 2011, Bilu-Parent-Rebolledo 2013)

We have $X_s(\ell)(\mathbf{Q}) = \{$cusps, CM-points$\}$ for $\ell \geqslant 11$, $\ell \neq 13$.

The cursed modular curve

All normalizers of split Cartan $G \subset \mathbf{GL}_2(\mathbf{F}_\ell)$ are conjugate, so all corresponding $X_G = X(\ell)/G$ are isomorphic. Denote $X_s(\ell) = X_G$.

Theorem (Bilu-Parent 2011, Bilu-Parent-Rebolledo 2013)
We have $X_s(\ell)(\mathbf{Q}) = \{$*cusps, CM-points*$\}$ *for* $\ell \geqslant 11$, $\ell \neq 13$.

What goes wrong at $\ell = 13$? Bilu-Parent-Rebolledo refer to $\ell = 13$ as the “cursed” level; crucial to their method is Mazur’s method for integrality of non-cuspidal rational points, using the following:

$$\mathrm{Jac}(X_s(\ell)) \sim \mathrm{Jac}(X_0^+(\ell^2)) \sim J_0(\ell) \times \mathrm{Jac}(X_{ns}(\ell))$$

Curses of the cursed curve

We have

$$\mathrm{Jac}(X_{\mathrm{s}}(\ell)) \sim \mathrm{Jac}(X_0^+(\ell^2)) \sim J_0(\ell) \times \mathrm{Jac}(X_{\mathrm{ns}}(\ell))$$

- Mazur's method applies whenever $J_0(\ell) \neq 0$, which is the case for $\ell = 11$ and $\ell \geqslant 17$.

Curses of the cursed curve

We have

$$\mathrm{Jac}(X_{\mathrm{s}}(\ell)) \sim \mathrm{Jac}(X_0^+(\ell^2)) \sim J_0(\ell) \times \mathrm{Jac}(X_{\mathrm{ns}}(\ell))$$

- Mazur's method applies whenever $J_0(\ell) \neq 0$, which is the case for $\ell = 11$ and $\ell \geqslant 17$.
- But for $\ell = 13$, we have $J_0(13) = 0$.

Curses of the cursed curve

We have

$$\mathrm{Jac}(X_{\mathrm{s}}(\ell)) \sim \mathrm{Jac}(X_0^+(\ell^2)) \sim J_0(\ell) \times \mathrm{Jac}(X_{\mathrm{ns}}(\ell))$$

- Mazur's method applies whenever $J_0(\ell) \neq 0$, which is the case for $\ell = 11$ and $\ell \geqslant 17$.
- But for $\ell = 13$, we have $J_0(13) = 0$.
- Curse #1: We thus have $\mathrm{Jac}(X_{\mathrm{s}}(13)) \sim \mathrm{Jac}(X_{\mathrm{ns}}(13))$ and $\mathrm{Jac}(X_{\mathrm{s}}(13))$ is absolutely simple.

Curses of the cursed curve, continued

Curse #2: Baran found an explicit smooth plane quartic model and showed

$$X_{\mathrm{s}}(13) \simeq_{\mathbf{Q}} X_{\mathrm{ns}}(13),$$

its non-split analogue. (No modular explanation for this!)

Curses of the cursed curve, continued

Curse #2: Baran found an explicit smooth plane quartic model and showed

$$X_{\mathrm{s}}(13) \simeq_{\mathbf{Q}} X_{\mathrm{ns}}(13),$$

its non-split analogue. (No modular explanation for this!)

Baran's model for $X_{\mathrm{s}}(13)$:

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

Visualizations of the cursed curve

JB and Sachi Hashimoto

Curses of the cursed curve, continued

Curse #2: Baran found an explicit smooth plane quartic model and showed

$$X_{\mathrm{s}}(13) \simeq_{\mathbf{Q}} X_{\mathrm{ns}}(13),$$

its non-split analogue. (No modular explanation for this!)

Baran's model for $X_{\mathrm{s}}(13)$:

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

Visualizations of the cursed curve
JB and Sachi Hashimoto

Question: Can we use Chabauty–Coleman to compute $X(\mathbf{Q})$?

Curses of the cursed curve, continued

Curse #2: Baran found an explicit smooth plane quartic model and showed

$$X_s(13) \simeq_{\mathbf{Q}} X_{ns}(13),$$

its non-split analogue. (No modular explanation for this!)

Baran's model for $X_s(13)$:

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

Visualizations of the cursed curve
JB and Sachi Hashimoto

Question: Can we use Chabauty–Coleman to compute $X(\mathbf{Q})$?

Curse #3: $r = \operatorname{rk} J(\mathbf{Q}) \geqslant 3 = g$. ☹

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.

Nonabelian Chabauty

Conjecture (Kim, '12)

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

This is implied by the Bloch-Kato conjectures.

Nonabelian Chabauty

Conjecture (Kim, ’12)

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

This is implied by the Bloch-Kato conjectures.

Questions:

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

Finiteness of $X(\mathbf{Q}_p)_n$

Theorem (Coates–Kim '10)

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

Theorem (Ellenberg–Hast '17)

Can extend the above to give a new proof of Faltings' theorem for curves $X/\mathbf{Q}$ that are solvable Galois covers of $\mathbf{P}^1$.

Theorem (B.–Dogra '16)

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.

Finiteness of $X(\mathbf{Q}_p)_n$

Theorem (Coates–Kim '10)

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

Theorem (Ellenberg–Hast '17)

Can extend the above to give a new proof of Faltings' theorem for curves $X/\mathbf{Q}$ that are solvable Galois covers of $\mathbf{P}^1$.

Theorem (B.–Dogra '16)

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.

So when can we explicitly compute $X(\mathbf{Q}_p)_2$? We call this *quadratic Chabauty*.

Quadratic Chabauty: $\mathbf{Q}$-points and p-adic heights

Want to use "quadratic Chabauty" to compute $X(\mathbf{Q}_p)_2$, a finite set of p-adic points that contains all rational points on X for certain curves that have $r = g$

- We know that $X(\mathbf{Q}_p)_2$ is finite when $r = g$ and $\operatorname{rk} NS(J) > 1$. The difficulty is in making this effective.
- The functions cutting out p-adic points can be expressed in terms of p-adic heights pairings; the key is to move from linear relations (as in Chabauty–Coleman) to bilinear relations.
- These p-adic heights have a natural interpretation in terms of p-adic differential equations, with relevant constants computed in terms of known rational points.

Dictionary between classical and quadratic Chabauty

technique	classical Chabauty	quadratic Chabauty
hypotheses	$r < g$	$r = g$ and $\operatorname{rk} NS(J_{\mathbf{Q}}) \geqslant 2$
geometry	Jacobian	Selmer variety
p-adic analysis	line integrals	iterated path integrals
algebra	linear algebra	bilinear algebra (heights)

From classical Chabauty to quadratic Chabauty

Recap: we can think of classical Chabauty as using linear relations among $\int_b^x \omega$ for $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$, when $r < g$, i.e., understanding

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

The simplest generalization of Chabauty–Coleman comes from considering bilinear relations on $H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$ when $r = g$. This motivates the notion of a *quadratic Chabauty function*.

Quadratic Chabauty function

Definition

A quadratic Chabauty function θ is a function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ such that:

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 given by a power series.
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

Lemma

A quadratic Chabauty function induces a function $F : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ *such that* $F(X(\mathbf{Q})) = 0$ *and* F *has finitely many zeros.*

Quadratic Chabauty functions

Lemma

A quadratic Chabauty function induces a function $F : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ *such that* $F(X(\mathbf{Q})) = 0$ *and* F *has finitely many zeros.*

- The goal is to make this explicit: need a quadratic Chabauty function: need an $E, c,$ and need to solve for B.
- Solving for B is very similar to solving for linear relations in Chabauty–Coleman.

Quadratic Chabauty functions

Lemma

A quadratic Chabauty function induces a function $F : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ *such that* $F(X(\mathbf{Q})) = 0$ *and* F *has finitely many zeros.*

- The goal is to make this explicit: need a quadratic Chabauty function: need an E, c, and need to solve for B.
- Solving for B is very similar to solving for linear relations in Chabauty–Coleman.

We find quadratic Chabauty functions using p-adic height functions. As a warm-up, we'll use p-adic heights to find integral points on affine hyperelliptic curves when $r = g$.

p-adic heights on Jacobians of curves (Coleman-Gross)

The Coleman-Gross p-adic height pairing is a (symmetric) bilinear pairing

$$h : \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \to \mathbf{Q}_p,$$

with $h = \sum_v h_v$

- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.
- The global height decomposes as a finite sum of local heights $h = \sum_v h_v$ over *finite* primes v
- Construction of local height h_v depends on whether $v = p$ or $v \neq p$.
  - $v \neq p$: intersection theory
  - $v = p$: normalized differentials (with respect to a splitting of the Hodge filtration on $H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$), Coleman integration

Quadratic Chabauty (roughly)

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

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

For example, using the Coleman-Gross p-adic height, the statement of quadratic Chabauty for integral points has, as its main ideas, (1) *computing the local height h_p as a double Coleman integral* and (2) *controlling* the finite number of values

$$\sum_{v \neq p} h_v(z - b, z - b)$$

takes on integral points z.

Note: to determine the local height h_p, need to compute Frobenius structure on the relevant p-adic differential equation.

Quadratic Chabauty for integral points

We use these double and single Coleman integrals to rewrite the global p-adic height pairing h and to study it on integral points:

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

Quadratic Chabauty for integral points

We use these double and single Coleman integrals to rewrite the global p-adic height pairing h and to study it on integral points:

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

Quadratic Chabauty for integral points

Theorem (B.-Besser-Müller)

Let $X/\mathbf{Q}$ be a hyperelliptic curve. If $r = g \geqslant 1$ 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 $\theta(P) = \sum_{i=0}^{g-1} \int_b^P \omega_i \bar{\omega}_i$.

This gives a quadratic Chabauty function θ and a finite set of values S (giving a *quadratic Chabauty pair*).

How can we use these ideas to study rational points?

Constructing quadratic Chabauty functions

Main problem generalizing this to rational points: we can't control $h_v(x)$ for $v \neq p$ when x is rational but not integral.

Constructing quadratic Chabauty functions

Main problem generalizing this to rational points: we can't control $h_v(x)$ for $v \neq p$ when x is rational but not integral.

Workaround for rational points:

- 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 $A(x)$ for every $x \in X(\mathbf{Q})$. Depends on a choice of "nice" correspondence Z on X. Such a correspondence exists when $\operatorname{rk} NS(J) > 1$.
- Restrict to case of X with everywhere potential good reduction, then for all $v \neq p$, local heights $h_v(A(x))$ are trivial.
- Compute p-adic height of $A(x)$ via explicit description of $D_{cris}(A(x))$ as a filtered ϕ-module.

Quadratic Chabauty for rational points

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

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

where

1. $x \mapsto h_p(A(x))$ extends to a locally analytic function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ by Nekovář's construction and
2. For $v \neq p$ the local heights $h_v(A(x))$ are trivial since by assumption, all primes $v \neq p$ are of potential good reduction

This gives a QCF whose pairing is h and whose endomorphism is induced by Z.

Quadratic Chabauty

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
- and that we know enough rational points $P_i \in X(\mathbf{Q})$.

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

Quadratic Chabauty

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
- and that we know enough rational points $P_i \in X(\mathbf{Q})$.

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

Note that since we are assuming we have everywhere potentially good reduction, we have

$$h(A(x)) = h_p(A(x)),$$

i.e., the second problem is subsumed by the first.

High-level strategy: QC for the cursed curve

Practical matters:

- Show that $X_s(13)$ has $r = 3$.
- Make a small change of coordinates to work with the following curve X:

  $$Q(x,y) = y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$$

  so that we have enough (5 of the known) rational points in each of two affine patches.
- Since $\operatorname{rk} NS(J_{\mathbf{Q}}) = 3$, we have two independent nontrivial nice correspondences Z_1, Z_2 on X; we compute equations for 17-adic heights h^{Z_1}, h^{Z_2} on X
- Check the simultaneous solutions of the above two equations...are they precisely on the 7 known rational points?!

Rational points on $X_s(13)$

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

We have $|X_s(13)(\mathbf{Q})| = 7$.

Rational points on $X_{\mathrm{s}}(13)$

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

We have $|X_s(13)(\mathbf{Q})| = 7$.

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

Rational points on $X_s(13)$

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

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

By the work of Baran, we know $X_s(13)$ is isomorphic to $X_{ns}(13)$ over $\mathbf{Q}$, so we also get (for free) that $|X_{ns}(13)(\mathbf{Q})| = 7$.

Does the curse continue?

Does the curse continue?

Consider the following smooth plane quartic:

$$X_{S_4}(13) : 4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

- Via Mazur's Program B: the last remaining modular curve of level 13^n whose rational points have not been determined.

Does the curse continue?

Consider the following smooth plane quartic:

$$X_{S_4}(13) : 4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

- Via Mazur's Program B: the last remaining modular curve of level 13^n whose rational points have not been determined.
- There are 4 known rational points computed by Banwait and Cremona: $(1 : 3 : -2), (0 : 0 : 1), (0 : 1 : 0), (1 : 0 : 0)$.

Does the curse continue?

Consider the following smooth plane quartic:

$$X_{S_4}(13) : 4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

- Via Mazur's Program B: the last remaining modular curve of level 13^n whose rational points have not been determined.
- There are 4 known rational points computed by Banwait and Cremona: $(1:3:-2), (0:0:1), (0:1:0), (1:0:0)$.
- The rank of the Jacobian is 3 since its Jacobian is isogenous to $X_s(13)$.

Does the curse continue?

Consider the following smooth plane quartic:

$$X_{S_4}(13) : 4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

- Via Mazur's Program B: the last remaining modular curve of level 13^n whose rational points have not been determined.
- There are 4 known rational points computed by Banwait and Cremona: $(1:3:-2), (0:0:1), (0:1:0), (1:0:0)$.
- The rank of the Jacobian is 3 since its Jacobian is isogenous to $X_s(13)$.
- We have potential good reduction at $p = 13$.

Does the curse continue?

Consider the following smooth plane quartic:

$$X_{S_4}(13) : 4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

- Via Mazur's Program B: the last remaining modular curve of level 13^n whose rational points have not been determined.
- There are 4 known rational points computed by Banwait and Cremona: $(1:3:-2), (0:0:1), (0:1:0), (1:0:0)$.
- The rank of the Jacobian is 3 since its Jacobian is isogenous to $X_s(13)$.
- We have potential good reduction at $p = 13$.

Does the curse continue?

Consider the following smooth plane quartic:

$$X_{S_4}(13) : 4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

- Via Mazur's Program B: the last remaining modular curve of level 13^n whose rational points have not been determined.
- There are 4 known rational points computed by Banwait and Cremona: $(1:3:-2), (0:0:1), (0:1:0), (1:0:0)$.
- The rank of the Jacobian is 3 since its Jacobian is isogenous to $X_s(13)$.
- We have potential good reduction at $p = 13$.

Theorem (BDMTV)

$X_{S_4}(13)(\mathbf{Q}) = \{(1:3:-2), (0:0:1), (0:1:0), (1:0:0)\}$.