Quadratic Chabauty for elliptic curves over number fields

ANTS XVI

Aashraya Jha

Boston University

aashjha@bu.edu

July 18, 2024

Integral points of affine curves

K : A number field.
O_K : Ring of integers of K.
$\mathcal{U}/O_K$: Absolutely irreducible affine curve.
C/K : Compactification of the generic fibre of $\mathcal{U}$.

Theorem (Siegel's Theorem (partial), 1929)

If the genus of C is greater than equal to 1, $\mathcal{U}(O_K)$ is finite.

The main example we will look at are elliptic curves without the identity section.

Integral points on affine elliptic curves

Let $\mathcal{U}/O_K$ be an elliptic curve without the identity section, given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Figure: Google Gemini rendition of integral points on elliptic curve

State of the art algorithms

- Siegel's proof is ineffective, can not be used to determine the set $\mathcal{U}(O_K)$.
- Algorithms by Stroeker, Tszanakis ('94), Gebel, Pethö, Zimmer('94), Smart, Stephens ('97) to find integral points using *elliptic logarithms*.
- Zagier ('87), based on work of Lang ('78,'86), suggests use of elliptic logarithms.
- Hirata-Kohno, David ('91) give lower bounds for elliptic logarithms.
- Not implemented for imaginary quadratic fields on Sage/Magma/Pari GP/Oscar.

Quadratic Chabauty over $\mathbb{Z}$

Chabuaty–Coleman–Kim idea: Compute locally analytic p-adic map $\rho\colon \mathcal{U}(\mathbb{Q}_p) \to \mathbb{Q}_p$, and finite set $T \subset \mathbb{Q}_p$, such that $\rho(\mathcal{U}(\mathbb{Z})) \subseteq T$.
Locally analytic functions have finitely many roots, so the preimage $\rho^{-1}(T)$ is finite and contains $\mathcal{U}(\mathbb{Z})$.

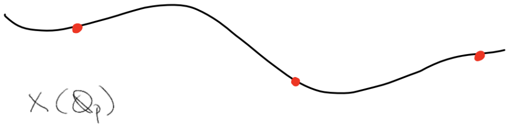

Figure: QC over $\mathbb{Q}$

Quadratic Chabauty over number fields

Use Weil restrictions, and consider $\mathcal{U}(K \otimes \mathbb{Q}_p)$. Need at least $[K : \mathbb{Q}]$ functions $\rho_i : \mathcal{U}(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ and finite sets $T_i \subseteq \mathbb{Q}_p$ such that $\rho_i(\mathcal{U}(O_K)) \subseteq T_i$. Consider

$$\bigcap \rho_i^{-1}(T_i).$$

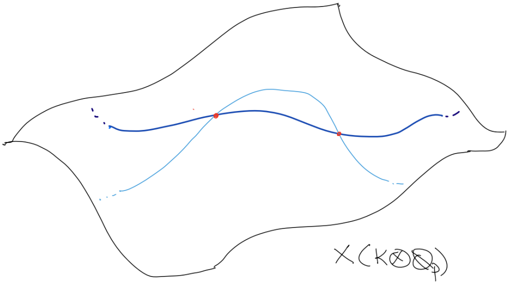

Figure: QC over quadratic K

A survey of Chabauty–Coleman–Kim over number fields

- Siksek ('13) introduced Chabauty over number fields K. Using abelian Coleman integrals, find functions that vanish on rational points of curves.
- Balakrishnan-Besser-Bianchi-Müller ('21) find quadratic Chabauty formulation of the same. Use Coleman-Gross heights. The reason this works is *Arakelov theory*.
- Bianchi ('20) finds $\mathbb{Z}[\zeta_3]$-points on the curve

$$y^2 = x^3 - 4.$$

- Gajović-Müller ('23) find $\mathbb{Z}[\sqrt{7}]$-points on non-base changed hyperelliptic curve.

All the examples need the rank of the Jacobian of the curve bounded suitably.

Warning!

Two locally analytic p-adic functions vanish in two variables can vanish on infinitely many points.
Consider $\mathbb{A}^2_{\mathbb{Q}_p} = \operatorname{Spec} \mathbb{Q}_p[x_1, x_2]$, and

$$f_1 = \log(1 - x_1) - \log(1 - x_2), \qquad f_2 = \log(x_1) - \log(x_2).$$

Both functions vanish on $x_1 = x_2$, so vanishing locus has infinitely many points!

Main theorem

- Let K be an imaginary quadratic field of class number 1, and E/K an elliptic curve of rank 2 (rank suitably bounded), which is not a base change.
- Let p be a prime that splits in K, such that E has good ordinary reduction at primes above p. Let $\mathcal{U} \subset \mathbb{A}^2_{O_K}$ be cut out by Weierstrass equation as before.

Theorem (Jha, ANTS XVI)

There exists an algorithm that computes a quadratic Chabauty set $\mathcal{U}(\mathbb{Z}_p)_2$ such that

$$\mathcal{U}(O_K) \subseteq \mathcal{U}(\mathbb{Z}_p)_2 \subseteq \mathcal{U}(O_K \otimes \mathbb{Z}_p)$$

Ideas of proof

Let K, p as before.

- Want at least 2 non-zero locally analytic p-adic functions

$$\rho_1, \rho_2 : \mathcal{U}(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p.$$

- Compute finite sets $T_i \subset \mathbb{Q}_p$ such that $\rho_i(\mathcal{U}(O_K)) \subseteq T_i$.

Mazur–Stein–Tate p-adic heights ('06) satisfy all these conditions!

p-adic heights

Given an idèle class character $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p$, one can associate a bilinear form $h := h^\chi : E(K) \otimes E(K) \to \mathbb{Q}_p$.

- h decomposes as $h = \sum_{v \in M_K} h_v$. Let

$$\rho := h - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}}.$$

  There exists $T \subset \mathbb{Q}_p$ such that $\rho(\mathcal{U}(O_K)) \subset T$. The set T can be computed using intersection numbers (Silverman ('88), Cremona, Pricket, Siksek ('06)).
- One can extend h and $h_{\mathfrak{p}}$ for $\mathfrak{p}|p$ to $E(K \otimes \mathbb{Q}_p)$ using Coleman integrals.
- Imaginary quadratic K have two such χ, the cyclotomic and anticyclotomic character.

Inputs for heights

- One can attach a *p-adic sigma function* (Mazur-Tate,'91) to elliptic curves over finite extensions of $\mathbb{Q}_p$. Fast implementation due to David Harvey ('08).
- Let P be a point of $E(K)$ so we can find a *denominator* d such that

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right).$$

- There exists $E^\bullet(K) \subseteq E(K)$ of finite index such that if $P \in E^\bullet(K)$.

$$\log d(nP) = n^2 \log d(P) + \log f_n(P),$$
$$\log \sigma(nP) = n^2 \log \sigma(P) + \log f_n(P)$$

Formulas for heights

Let $\psi_1, \psi_2 : K \hookrightarrow \mathbb{Q}_p$ be embeddings. Let σ_1, σ_2 be the associated p-adic sigma functions to curves basec There exists finite index $E^\circ(K) \subseteq E(K)$ such that if $P \in E^\circ(K)$,

$$h^{\mathrm{cyc}}(P) = \log\left(\frac{\sigma_1(P)}{\psi_1(d)}\right) + \log\left(\frac{\sigma_2(P)}{\psi_2(d)}\right)$$
$$h^{\mathrm{anti}}(P) = \log\left(\frac{\sigma_1(P)}{\psi_1(d)}\right) - \log\left(\frac{\sigma_2(P)}{\psi_2(d)}\right)$$

We can extend this formula to all of $E(K)$ via

$$h(P) = \frac{h(nP)}{n^2}.$$

Quadratic Chabauty algorithm

Let E/K be an elliptic curve of rank 2 and $\mathcal{U}$ as described before. Also fix p as before.

Algorithm

Input: Given generators P, Q *of* $E(K)/E(K)_{tors}$.

1. *Compute heights* $h^{\chi}(P,P), h^{\chi}(Q,Q), h^{\chi}(P,Q)$. *Solve for constants* α_{ij}^{χ} *such that*

$$h^{\chi}(P_i, P_j) = \alpha_{11}^{\chi} f_1^2 + \alpha_{12}^{\chi} f_1 f_2 + \alpha_{22}^{\chi} f_2^2$$

   where $f_n = \int \psi_n^* \omega$ *for* $n = 1, 2$ *for* $P_i, P_j \in \{P, Q\}$.
2. *Compute sets* T^{χ} *such that* $\rho^{\chi}(\mathcal{U}(O_K)) \subseteq T^{\chi}$.
3. *Compute* $A_p = \{\mathcal{R} \in \mathcal{U}(K \otimes \mathbb{Q}_p) : \rho^{cyc}(\mathcal{R}) \in T^{cyc}, \rho^{anti}(\mathcal{R}) \in T^{anti}\}$.

Output: Obtain a set $A_p \subseteq \mathcal{U}(K \otimes \mathbb{Q}_p)$ *which contains* $\mathcal{U}(O_K)$. *Output error if this set is infinite.*

An example

Set $K = \mathbb{Q}(\zeta_6)$. Consider the scheme $\mathcal{U} \subseteq \mathbb{A}^2_K$ given by the equation

$$y^2 + (\zeta_6 + 1)y = x^3 + (-\zeta_6 - 1)x^2 + \zeta_6 x. \qquad (1)$$

- The corresponding elliptic curve E has rank 2, and trivial K-torsion. Generators are $P = (1, 0)$, $Q = (\zeta_6, 0)$
- LMFDB label: 134689.3-CMa1
- Primes $p = 7$ and $q = 13$ split in K, and E has good, ordinary reduction at primes above p, q.
- $T^{\mathrm{cyc}} = T^{\mathrm{anti}} = \{0\}$.

Integral points from QC set

- Using the Quadratic Chabauty algorithm, we can compute the sets A_p, A_q. We get $\#A_p = 216, \#A_q = 120$. This took about 10 minutes on my laptop.
- A search yields 12 small O_K-points. Let B_p, B_q be the complement of the known O_K-points in A_p, A_q.

Do B_p, B_q have any O_K-points?

A sieve for elliptic curves

Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the primes above p, $\mathfrak{q}_1, \mathfrak{q}_2$ be the primes above q. One checks that

- $E_{\mathbb{F}_{\mathfrak{p}_1}}(\mathbb{F}_p) \cong E_{\mathbb{F}_{\mathfrak{p}_2}}(\mathbb{F}_p) \cong \mathbb{Z}/13\mathbb{Z}$
- $E_{\mathbb{F}_{\mathfrak{q}_1}}(\mathbb{F}_q) \cong \mathbb{Z}/7\mathbb{Z}$ and $E_{\mathbb{F}_{\mathfrak{q}_2}}(\mathbb{F}_q) \cong \mathbb{Z}/19\mathbb{Z}$.

Idea: Log and reduction restriction

- If $(R_1, R_2) \in A_p$ comes from $\mathcal{U}(O_K)$, then it is the image of $R = aP + bQ$ for $a, b \in \mathbb{Z}$.
- Restrict (a, b) with structure of group of reductions at p, q and Coleman integrals.

Sieve example

Let

$$(R_1, R_2) = ((3 + 6 \cdot 7 + .., 6 + 6 \cdot 7..), (2 + 7 + .., 2 + 2 \cdot 7 + ..)) \in B_p$$

- Solving the system

$$\overline{R_1} = a\overline{P_1} + b\overline{Q_1} \text{ in } E_{\mathbb{F}_{\mathfrak{p}_1}}(\mathbb{F}_p)$$
$$\overline{R_2} = a\overline{P_2} + b\overline{Q_2} \text{ in } E_{\mathbb{F}_{\mathfrak{p}_2}}(\mathbb{F}_p)$$

  yields restrictions on $(a, b) = (7, 0) \mod 13$.

- Also have

$$f_1(R_1) = af_1(P) + bf_1(Q) \text{ in } \mathbb{Q}_p$$
$$f_2(R_2) = af_2(P) + bf_2(Q) \text{ in } \mathbb{Q}_p$$

  giving constraints $(a, b) = (6, 5) \mod 7$.

- To $(R_1, R_2) =: \mathcal{R}$ we have associated log and reduction information:

$$\log_{\mathcal{R}} \subseteq \mathbb{F}_p^2, \qquad \text{red}_{\mathcal{R}} \subseteq \mathbb{F}_q^2.$$

- For each $\mathcal{R} \in A_p$ and $\mathcal{S} \in A_q$ compute log and reduction information.
- Compute

$$\bigcup_{\mathcal{R} \in A_p} (\log_{\mathcal{R}} \times \text{red}_{\mathcal{R}}) \bigcap \bigcup_{\mathcal{S} \in A_q} (\text{red}_{\mathcal{S}} \times \log_{\mathcal{S}})$$

- Hope this intersection is empty.
- For the curve in Equation (1), it is empty!
- $\#\mathcal{U}(O_K) = 12.$

Future work

- Good methods to solve systems of multivariate power series.
- Use method for rank 1 elliptic curves.
- Find a better sieve for elliptic curves.
- Use method for higher genus curves.

Summary

Let K be an imaginary quadratic field K with class number 1. Let E be an elliptic curve of rank at most 2. Let $\mathcal{U}/O_K$ be given by a minimal Weierstrass equation of E.

Theorem

There exists a prime p and an algorithm such that we can compute a quadratic Chabauty set $\mathcal{U}(\mathbb{Z}_p)_2$ with

$$\mathcal{U}(O_K) \subseteq \mathcal{U}(\mathbb{Z}_p)_2 \subseteq \mathcal{U}(O_K \otimes \mathbb{Z}_p).$$

Thank You!!