Quadratic Chabauty over number fields VaNTAGe

Aashraya Jha

Boston University

April 8th, 2025

Joint with Jennifer Balakrishnan, L. Alexander Betts, Daniel Hast, and J. Steffen Müller

A classification problem

Elliptic Curves and Torsion

- Let K a number field, and E/K an elliptic curve.
- $E(K) \cong \mathbb{Z}^r \oplus E(K)_{tor}$ where $E(K)_{tor}$ is a finite abelian group.
- We will be interested in $E(K)_{tor}$ and $E(\overline{K})_{tor}$.
- Mazur (1975) provides a finite irredundant list classifying $E(\mathbb{Q})_{tor}$.
- Sufficient to determine \mathbb{Q} -points on *modular* curves $X_1(N)$ for all N, which parametrise elliptic curves with an N-torsion point.

Torsion and Galois representations

• The N-torsion $E[N](\overline{K})$ is a G_K -module. Get a representation

$$\rho_{E,N}: G_K \to \operatorname{Aut}(E[N]) \cong \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

- Let H_N be the image of $\rho_{E,N}$.
- Suppose $P \in E[N](K)$ of order N. Since $P^{\sigma} = P$ for any $\sigma \in G_K$, we get H_N is of the form

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$
.

Think $\Gamma_1(N)$.

Modular curves

- Let $H \leq \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We say E has H-level structure if there exists a twist E' of E such that $\rho_{E',N}(G_K) \leq H$ up to conjugation.
- Let X_H denote the compactified (coarse) moduli space of elliptic curves E with level structure H. Call it modular curve of level H.
- $X_1(N)$ is a special example of this phenomenon.
- Let X(N) denote moduli space of elliptic curves with full level structure, that is $H = \{ \mathrm{Id} \} \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Parametrises pairs (E,(P,Q)) along with isomorphism $\langle P,Q \rangle \cong (\mathbb{Z}/N\mathbb{Z})^2$.
- We note $X_H = X(N)/H$.

Open Image theorem

• Consider E[N] for all N, that is consider

$$E(\overline{K})_{tor} = \varprojlim_{N} E[N](\overline{K}).$$

Get a representation

$$\rho_E: G_K \to \mathsf{GL}_2(\hat{\mathbb{Z}}).$$

• If E does not have CM, Serre (1972) proved

$$ho_{\mathsf{E}}:\mathsf{G}_{\mathsf{K}} o\mathsf{GL}_2(\hat{\mathbb{Z}})\cong\prod_{\ell}\mathsf{GL}_2(\mathbb{Z}_\ell)$$

has open image. Equivalently the image is finite index.

Program B

Mazur asks the following question:

B. Given a number field K and a subgroup H of
$$\operatorname{GL}_2\widehat{\mathbf{z}} = \prod_p \operatorname{GL}_2 \mathbf{z}_p$$
 classify all elliptic curves $\operatorname{E}_{/K}$ whose associated Galois representation on torsion points maps $\operatorname{Gal}(\overline{K}/K)$ into $\operatorname{H} \subset \operatorname{GL}_2\widehat{\mathbf{z}}$.

Mazur - Rational points on modular curves (1977)

- This is hard!
- Consider "vertical" analogue, that is classify images in $\mathsf{GL}_2(\mathbb{Z}_\ell)$.

Theorem 1 also fits into a general program:

Classifying *ℓ*-adic images

- For E/\mathbb{Q} , Rouse and Zureick-Brown classify ℓ -adic images for $\ell=2$ (2015).
- The classification for $\ell=13,17$ has also been completed (2023).
- Rouse, Sutherland, Zureick-Brown compute ℓ -adic images for $\ell \leq 37$ and suggest a classification for all ℓ (2022).
- Conjectured to be surjective for ℓ > 37, strong evidence due to Furio–Lombardo (2023).
- Classification of these images is equivalent to finding rational points on modular curves of level ℓ^e .

Non-split Cartan

- Let ℓ be an odd prime and \mathcal{O} be the degree 2 unramified extension of \mathbb{Z}_{ℓ} .
- Multiplication by $a \in \mathcal{O}^{\times}$ is a \mathbb{Z}_{ℓ} -linear map, induces injection

$$\mathcal{O}^{\times} \hookrightarrow \mathsf{GL}_2(\mathbb{Z}_{\ell}).$$

Induces map

$$(\mathcal{O}/\ell^e)^{\times} \hookrightarrow \mathsf{GL}_2(\mathbb{Z}_\ell/\ell^e\mathbb{Z}_\ell).$$

The image is $Ns(\ell^e)$, the non split Cartan group of level ℓ^e .

- Let ι be natural involution on \mathcal{O} . The extended non-split Cartan group, $Ns^+(\ell^e)$ is generated by $Ns(\ell^e)$, ι .
- The corresponding modular curve is denoted $X_{\rm ns}^+(\ell^e)$.

Mazur's proof crucially uses the fact that $Jac(X_0(N))$ has a rank 0 quotient. This is not true for $Jac(X_{ns}^+(N))$.

Geometric moduli interpretation of non-split Cartan

- Let h be the image of a generator of $\mathbb{F}_{\ell^2}^{\times}$ under $\mathbb{F}_{\ell^2}^{\times} \hookrightarrow \mathsf{GL}_2(\mathbb{F}_{\ell})$.
- For $0 \le i \le \ell$, let C_i denote the subgroups of $E[\ell](\overline{K})$ of cardinality ℓ . For any i, $h(C_i) = C_i$ for some j.
- A *h-oriented necklace* is an equivalence class of sequences $[C_0, \ldots C_\ell]$ with $h(C_i) = C_{i+1}$.



Figure: An h-oriented necklace

- If h' is another generator, bijection between sets of h-oriented necklace and h'-oriented necklace.
- A *necklace* is the orbit of an oriented necklace under the involution $w([C_0, C_1, \ldots, C_\ell]) = [C_\ell, \ldots, C_1, C_0].$

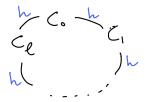


Figure: An h-oriented necklace

Theorem (Rebolledo, Wuthrich)

 $X_{ns}(\ell)$ parametrises elliptic curves E with an oriented necklace, and $X_{ns}^+(\ell)$ parametrises elliptic curves with a necklace.

$$X_{\rm ns}^+(27)$$

- After RSZB, the classification for $\ell=3$ was almost complete. Needed to to determine $X_{ns}^+(27)(\mathbb{Q})$.
- The curve $X_{ns}^+(27)$ has g=r=12. This is "large" for computational purposes.
- There are 8 known CM points.
- Known methods don't seem to work to determine $X_{ns}^+(27)(\mathbb{Q})$.

Main theorem

Theorem (Balakrishnan, Betts, Hast, J., Müller)

$$\#X_{ns}^{+}(27)(\mathbb{Q})=8.$$

Consequently if E/\mathbb{Q} is a non-CM elliptic curve, then $im \, \rho_{E,3^{\infty}}$ is one of 47 subgroups of $GL_2(\mathbb{Z}_3)$ of level at most 27 and index at most 72, as in RSZB Table 3.

- RSZB find a genus 3 quotient $X/\mathbb{Q}(\zeta_3)$. Jac(X) has rank 6 over $\mathbb{Q}(\zeta_3)$. There are 13 known points.
- Sufficient to compute $X(\mathbb{Q}(\zeta_3))$.

How do we determine $X(\mathbb{Q}(\zeta_3))$?

p-adic methods

Set Up

- Let K be a number field of degree d, and let X/K be a *nice* curve of genus $g \ge 2$.
- Assume there is a rational prime p that splits totally in K, such that for p|p, X has good reduction at p.
- For $1 \le i \le d$, we let $\psi_i \colon K \hookrightarrow \mathbb{Q}_p \cong K_{\mathfrak{p}_i}$ be embeddings of K in \mathbb{Q}_p .
- Let J be the Jacobian of X, and the rank of J(K) be r.
- Assume there is a rational point $b \in X(K)$, and embed $X \hookrightarrow J, x \mapsto [x-b]$ via the Abel-Jacobi map .

Chabauty–Coleman over Q

- Idea : Consider $B := X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p)$. Note $B \supset X(\mathbb{Q})$. Chabauty shows $r < g \Rightarrow B$ finite.
- Let $\{\omega_i\}_{i=1}^g$ be holomorphic differentials. Using Coleman integrals, find g-functionals

$$f_i: J(\mathbb{Q}) \otimes \mathbb{Q}_p \to \mathbb{Q}_p, \ [P-b] \mapsto \int_b^P \omega_i.$$

Since r < g, find vanishing functional.

• Pull back vanishing functional to a non-zero locally analytic $\rho \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$. The zeros of ρ contain $X(\mathbb{Q})$.

(Skim) Quadratic Chabauty over Q

- Assume $J(\mathbb{Q}) \otimes \mathbb{Q}_p \cong H^0(X_{\mathbb{Q}_p}, \Omega^1)^* = H^0(X, \Omega^1)^* \otimes \mathbb{Q}_p$ (implies r = g), and there exists *nice* correspondence $Z \subseteq X \times X$.
- Balakrishnan and Dogra show that there is a computable non-constant locally analytic function obtained from a p-adic height

$$\rho_Z \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$$

and a fine set set $T \subset \mathbb{Q}_p$ such that $\rho_Z(X(\mathbb{Q})) \subseteq T$.

• The preimage $\rho_Z^{-1}(T)$ is finite and contains $X(\mathbb{Q})$.



Figure: QC over Q

Modular Curves and quadratic Chabauty

- For a modular curve X whose Jacobian J is \mathbb{Q} -simple, r is a multiple of g. This follows from $J(\mathbb{Q})$ being an $\operatorname{End}(J)$ -module, which has \mathbb{Z} -rank equal g.
- Thus in the case r ≠ 0, Chabauty–Coleman does not apply directly. Quadratic Chabauty often does!
- For modular curves, Hecke correspondences often provide the nice correspondence required in the method of Balakrishnan and Dogra.
- Quadratic Chabauty has been used to determine the rational points of several modular curves with $g \le 6$.

Chabauty-Coleman over number fields

 Siksek considers Chabauty–Coleman over number fields by considering functionals

$$f_{i,j} \colon J(K) \otimes \mathbb{Q}_p \to \mathbb{Q}_p$$

$$[x-b] \mapsto \int_{\psi_j(b)}^{\psi_j(x)} \psi_j^* \omega_i.$$

- Get dg functionals, which can be extended to $X(K \otimes \mathbb{Q}_p)$.
- Since $X(K \otimes \mathbb{Q}_p)$ is d-dimensional, need at least d functions ρ_i for $1 \leq i \leq d$ such that ρ_i vanish on K-points.
- Can expect this when $r \leq d(g-1)$, but not always true!
- Siksek computes points of a generalised Fermat equation (2,3,10) using this approach.

Quadratic Chabauty over number fields

- Assume $J(K) \otimes \mathbb{Q}_p \cong H^0(X, \Omega^1)^* \otimes \mathbb{Q}_p = \prod_{\mathfrak{p}|p} H^0(X_{K_{\mathfrak{p}}}, \Omega^1)^*$. Thus r = dg.
- Need d p-adic heights from which we obtain functions $\rho_i \colon X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ and finite sets $T_i \subseteq \mathbb{Q}_p$ such that $\rho_i(X(K)) \subseteq T_i$.
- Consider $B := \bigcap \rho_i^{-1}(T_i)$ and $X(K) \subseteq B$.



Figure: QC over quadratic K

Warning!

Two locally analytic *p*-adic functions in two variables could vanish simultaneously on infinitely many points.

Consider $\mathbb{A}^2_{\mathbb{Q}_p} = \operatorname{\mathsf{Spec}} \mathbb{Q}_p[x_1, x_2]$, and

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

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

p-adic heights

There exists étale Abel–Jacobi map

$$X(K) \to J(K) \otimes \mathbb{Q}_p \cong H^0(X, \Omega^1)^* \otimes \mathbb{Q}_p.$$

Nekovář defines a family of bilinear height functions

$$h: (H^0(X,\Omega^1)^* \otimes \mathbb{Q}_p)^{\otimes 2} \to \mathbb{Q}_p,$$

which depend on a choice of

- 1. Idèle class character $\chi: \mathbb{A}_{\kappa}^{\times}/K^{\times} \to \mathbb{Q}_{p}$
- 2. Splittings of the Hodge filtration $H^0(X_{\mathfrak{p}},\Omega^1)\otimes \mathbb{Q}_p\hookrightarrow H^1_{dR}(X_{\mathfrak{p}})\otimes \mathbb{Q}_p$ for all $\mathfrak{p}|p$.
- h decomposes into local heights $h = \sum_{\nu} h_{\nu}$.

Heights to ρ

• Given Z, for each point $x \in X(K)$, Balakrishnan and Dogra construct an element

$$A(x) := A_{b,Z}(x) \in H^0(X,\Omega)^* \otimes H^0(X,\Omega)^*.$$

- A(x) corresponds to divisor [x b] and Chow–Heegner cycle $D_{Z,b}(x)$.
- Fix an idèle class character and splitting of Hodge filtration, and let h be the corresponding p-adic height. We let

$$\rho \colon X(K) \to \mathbb{Q}_p$$
$$x \mapsto h(A(x)) - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}}(A(x))$$

Can extend ρ analytically to $X(K \otimes \mathbb{Q}_p)$.

Quadratic Chabauty pair

 Balakrishnan and Dogra (based on work of Kim and Tamagawa) show the set

$$\mathcal{T} = \left\{ \sum_{v \nmid p} h_v(X(\mathcal{K}_v))
ight\}$$

is finite.

- For $v \nmid p$, h_v takes finitely many values on $X(K_v)$, and if X has potentially good reduction at $v \nmid p$, h_v is identically 0.
- Get $\rho(X(K)) \subseteq T$. We call (ρ, T) a quadratic Chabauty pair.
- If $K = \mathbb{Q}$, $\rho^{-1}(T)$ is finite and one can identify $X(\mathbb{Q}) \subseteq \rho^{-1}(T)$.

- In the case of number fields, for each Z, we obtain independent heights corresponding to linearly independent idèle class characters.
- If r_{NS} is rank of Néron–Severi of J/K, we obtain $r_{NS}-1$ linearly independent nice correspondences.
- If r_2 is the number of complex places, then we expect to have $r_2 + 1$ linearly independent idèle class characters.
- Thus we can obtain up to $(r_2 + 1)(r_{NS} 1)$ *p*-adic heights
- Will compute

$$B := \bigcap_{Z,\chi} \rho_{Z,\chi}^{-1}(T_{Z,\chi}).$$

Finiteness results

- Siksek observes if C/L is such that $r_L > d_L(g_L 1)$, then for any extension K/L, the Chabauty–Coleman locus for C_K will still be infinite even if the rank is suitably bounded.
- Dogra exhibits a curve C/K where $r_L \le d_L(g_L 1)$ for all subfields $L \subseteq K$, but the Chabauty–Coleman locus is infinite.
- Dogra shows if for all $i \neq j$

$$\mathsf{Hom}(J_{\overline{K},\psi_i},J_{\overline{K},\psi_i})=0,$$

and rank is suitable bounded by the genus, the Chabauty–Coleman locus and quadratic-Chabauty locus are finite.

See also the work of Hast and Triantafillou.

Computing with QCNF

- Balakrishnan, Besser, Bianchi and Müller compute integral points of hyperelliptic curves over number fields, and the rational points of bielliptic curves over number fields.
- Bianchi computes the $\mathbb{Z}(\zeta_3)$ -points of a base-changed elliptic curve.
- Extended by J. to non-base-changed elliptic curve over imaginary quadratic fields.
- Gajović and Müller compute the $\mathbb{Z}[\sqrt{7}]$ -points of a hyperelliptic curve.

Classifying 3-adic images

The genus 3 quotient

- Recall $X_{\rm ns}^+(27)$ has r=g=12, but too large for quadratic Chabauty over \mathbb{Q} .
- The curve $X_{\rm ns}^+(9)\cong \mathbb{P}^1$, so can't pull back points. RSZB there is notice no intermediate subgroup $N_{\rm ns}^+(9)\leq H\leq N_{\rm ns}^+(27)$. But exists H

$$N_{\mathsf{ns}}^+(27) \cap D \le H \le N_{\mathsf{ns}}^+(9) \cap D$$

where $D = \{g \in GL_2(27) : \det(g) \cong 1 \pmod{3}\}$

- $X = X_H$ has genus 3, and is naturally defined over $K = \mathbb{Q}(\zeta_3)$. It is a smooth plane quartic. Let $J = \operatorname{Jac}(X)$.
- Have $J(K) \otimes \mathbb{Q}_p \cong H^0(X, \Omega^1)^* \otimes \mathbb{Q}_p$.

Hence r = 2g! Can't use quadratic Chabauty directly :(

Quadratic Chabauty for X

• Nice correspondences are in bijection with $\operatorname{End}^+(J)^{\operatorname{tr}=0}$, the trace 0 Rosati-fixed endomorphisms of J.

$$\operatorname{End}^+(J) \cong \mathbb{Z}(\zeta_9)^+,$$

therefore exists a nice correspondence Z.

- X has bad reduction at the unique ramified prime q₃ of K.
- For K we have two idéle class characters, $\chi = \chi^{\rm cyc}, \chi^{\rm anti}$.
- Consider $\rho^{\chi}(x) = h^{\chi}(A(x)) \sum_{\mathfrak{p}|p} h^{\chi}_{\mathfrak{p}}(A(x))$, which take values in the finite sets $T^{\chi} = \{h^{\chi}_{\mathfrak{q}_3}(X(K_3))\}$.

Computing local heights over p

- The prime p = 13 satisfies the conditions required in the set up.
- There are algorithms to compute $h_{\mathfrak{p}}$ for curves C/\mathbb{Q} , first developed by Balakrishnan-Dogra-Müller-Tuitman-Vonk. These generalise to X/K. Requires iterated Coleman integration and computing action of Frobenius on the curve.
- We require the action of a nice correspondence Z on $H^1_{dR}(X)$ for the above algorithm. We use the Eichler-Shimura relation to calculate this action. For our choice of basis, one of the entries in the matrix had 48 decimal digits!

Need to compute T^{χ} !

Some digits

A.0.1 The matrix corresponding to nice correspondences

Let Z be the antisymmetric matrix in (3.28). We provide the entries Z_{ij} for $1 \le i < j \le 2g$, where g = 3.

$$\begin{split} Z_{12} &= 1/553587347843318347476850951021526443966596354944 \times \\ & (862120979734593693544241958365169183472558541867\zeta_3 - \\ & 709894138835979310068275485431537847366451682980) \\ Z_{13} &= 1/198091943042726842099239658448738045316928 \times \\ & (-5947643782312778539319798842170745533960566\zeta_3 - \\ & 5151106304577577853661504516396456634539397) \end{split}$$

Dual graphs of curves

Definition

The dual graph of a curve is a graph whose vertices are the irreducible components of the curve, and whose edges are singular points of the curve.

The last example below is due to Ossen.

Description of couve	Cove C	د_ًا
Smooth come		•
IP1 intersecting with IP1 in 2 pts)
Special Libre of minimal stable model of XK3	***	

Computing local height at q_3

We want to determine the set T^{χ} . It is sufficient to compute $h_{\mathfrak{q}_3}(X(K_3))$. We use the following theorem.

Theorem (Betts-Dogra)

Let Γ_X be the dual graph of the special fibre of a regular semistable model of X. The local height at $v \nmid p$

$$h_v \colon X(K_v) \to \mathbb{Q}_p$$

factors through the map red : $X(K_v) \rightarrow \Gamma_X$. Also, $h_v(b) = 0$.

Height at q₃ strategy

- Our ultimate aim is to show red : X(K₃) → Γ_X is constant. It
 is sufficient to show Γ_X has precisely one G_{K₃}-invariant vertex.
- Ossen computes the minimal regular model of X. We determine the G_{K_3} -action on the dual graph of this model.
- Ossen computes a stable model of X by finding a field extension L/K_3 and a model \mathcal{Y}/O_L for \mathbb{P}^1_L , and considers its normalisation \mathcal{X}' in the function field $K(X_L)$.
- To compute *Y*, Ossen computes a degree 9 polynomial
 φ ∈ K₃[x] and defines an associated valuation v_φ. Uses model
 corresponding to this valuation.
 - Observation: G_{K_3} transitively permutes roots of ϕ .

Analysing Γ_Y

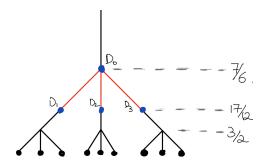
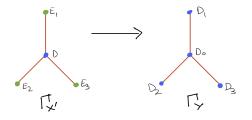


Figure: Skeleton due to Ossen

 G_{K_3} permutes D_1, D_2, D_3 , and fixes D_0 .

$$\Gamma_{X'} \to \Gamma_Y$$

- By construction $E_i \mapsto D_i$ for i = 1, 2, 3 and $D \mapsto D_0$.
- The map $\Gamma_{X'} \to \Gamma_Y$ is G_{K_3} -equivariant, and therefore $\Gamma_{X'}$ has only one G_{K_3} -invariant vertex.



Therefore, for this curve $T^{\chi} = \{0\}$ for any χ .

Identifying rational points

- Actually get two nice linearly independent correspondences Z_1, Z_2 . Essential to extend h(A(x)) from X(K) to $X(K \otimes \mathbb{Q}_p)$.
- Use a multivariate Hensel lifting to compute

$$B = \bigcap_{1 \le i \le 2} \rho_{Z_1, \chi_i}^{-1}(T^{\chi_i}).$$

• The set B contains points not in X(K), but we confirm that ρ_{Z_2,χ_i} don't vanish on these spurious points.

Main Theorem

Theorem (Balakrishnan, Betts, Hast, J., Müller)

The curve $X_{ns}^+(27)$ has exactly 8 \mathbb{Q} -points, all of which correspond to CM elliptic curves.

Proof.

```
Hence the set of K-rational points on the Curve over K defined by (2*u+2)*X1^3*Y1+(u-1)*X1*Y1^3+Y1^4-u*X1^3*Z1-3*u*X1^2*Y1*Z1+(3*u+2)*Y1^3*Z1+3*u*X1^2*Z1^2+3*u*X1*Y1*Z1^2-3*Y1^2*Z1^2+(-u+1)*X1*Z1^3-2*u*Y1*Z1^3+(u+1)*Z1^4 is [(1:0:0), (-u:1:0), (0:-u-1:1), (1:-u-1:1), (u+1:-u-1:1), (0:-u:1), (u+1:0:1), (2*u+2:u:1), (u:1:1), (1/2*u-3):1/2*(u+2):1), (1/3*(-u-2):1/3*(u+2):1), (-1/2*u:-1/2:1), (1/7*(5*u+4):-1:1)], where K is the Cyclotomic Field of order 3 and degree 2.This is the time taken 8441.2108458.660
```

Future Work

- Determine quotients of other modular curves over quadratic number fields; determine all points.
- Find sufficient criteria for finiteness of

$$\bigcap_{i} \rho_{i}^{-1}(T_{i}).$$

Dogra's hypothesis on geometric isogeny factors are violated by X_H .

Summary

- For quadratic fields K, exists a method to compute locally analytic functions $\rho \colon X(K \otimes \mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$ and finite sets $T \subset \mathbb{Q}_p$, such that $\rho(X(K)) \subseteq T$.
- $\#X_{ns}^+(27)(\mathbb{Q})=8$, which correspond to CM elliptic curves

Thank You!

Bounds

 For a curve X/K, we expect restriction of scalars Chabauty to work if

$$r \leq d(g-1)$$
.

 Le r_{NS} be the Néron- Severi rank of X, r₂ be the number of complex places od K, and r_K be the rank of the unit group of O_K. We expect quadratic Chabauty over number fields to work if

$$r \leq (r_{\mathsf{NS}} - 1)(r_2 + 1) + d(g - 1).$$

If we just use one nice correspondence, this reduces to

$$r+r_K\leq dg$$
.