

Quadratic Chabauty over number fields and 3-adic Galois representations

Steffen Müller (Rijksuniversiteit Groningen)

joint work with

J.S. Balakrishnan, A. Betts, D.R. Hast, A. Jha

Rational Points 2025

Schloss Schney

July 29, 2025

Part I

ℓ -adic Galois representations and modular curves

Residual Galois representations

Let E/\mathbb{Q} be an elliptic curve and $N \geq 1$. Define

$$E[N] := \{P \in E(\bar{\mathbb{Q}}) : NP = 0\} \simeq (\mathbb{Z}/N\mathbb{Z})^2.$$

For $E[N] \subset E(K)$ and K/\mathbb{Q} Galois, $\text{Gal}(K/\mathbb{Q})$ acts on $E[N]$ via

$$(x, y)^\sigma := (\sigma(x), \sigma(y))$$

\rightsquigarrow mod N -Galois representation

$$\bar{\rho}_{E,N} : G_{\mathbb{Q}} := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[N]) \simeq \text{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

ℓ -adic Galois representations and modular curves

Let ℓ be prime, $n \geq 1$.

The $\bar{\rho}_{E,\ell^n}$ fit together to give the ℓ -adic Galois representation

$$\bar{\rho}_{E,\ell^\infty} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Goal (Mazur 1977). Classify all ℓ -adic Galois representations of elliptic curves E/\mathbb{Q} for all primes ℓ .

$G \leq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \rightsquigarrow$ modular curve $X_G \simeq X(\ell^n)/G$ such that

$$E/\mathbb{Q} \text{ with } \mathrm{im}(\bar{\rho}_{E,\ell^n}) \subset G \rightsquigarrow \text{non-cuspidal } P \in X_G(\mathbb{Q}).$$

Goal. Compute $X_G(\mathbb{Q})$ for all $G \leq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Done for $\ell = 2$ (Rouse – Zureick-Brown, 2015) and $\ell \in \{13, 17, 3\}$.

Non-split Cartan

Usually hardest case: $G = N_{\text{ns}}(\ell^n) \leq \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ normalizer of non-split Cartan subgroup $C_{\text{ns}}(\ell^n) \leq \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Write

$$X_{\text{ns}}^+(\ell^n) := X_{N_{\text{ns}}(\ell^n)}.$$

Example. Prime level ℓ . Then $\mathbb{F}_{\ell^2}^*$ acts on $\mathbb{F}_{\ell} \times \mathbb{F}_{\ell} \simeq \mathbb{F}_{\ell^2}$

$$\rightsquigarrow C_{\text{ns}}(\ell) = \text{im}(\mathbb{F}_{\ell^2}^* \rightarrow \text{GL}_2(\mathbb{F}_{\ell})) \leq N_{\text{ns}}(\ell).$$

$X_{\text{ns}}^+(\ell)(\mathbb{Q})$ is known only for

- $\ell \in 2, 3, 5, 7, 11$: genus 0,1
- $\ell = 13, 17$ (Balakrishnan-Dogra-M.-Tuitman-Vonk, '19, '23)

We also computed $X_{S_4}(13)(\mathbb{Q})$. This completed the classification of ℓ -adic Galois representations for $\ell = 13, 17$.

$X_{\text{ns}}^+(27)$ and a quotient

Rouse–Sutherland–Zureick–Brown, 2022. Finished computation of $X_G(\mathbb{Q})$ for all $G \leq \text{GL}_2(\mathbb{Z}/3^n\mathbb{Z})$ except for $X_{\text{ns}}^+(27)$.

- $N_{\text{ns}}(27) = \left\langle \begin{pmatrix} 20 & 14 \\ 7 & 20 \end{pmatrix}, \begin{pmatrix} 2 & 9 \\ 9 & 25 \end{pmatrix} \right\rangle \leq \text{GL}_2(\mathbb{Z}/27\mathbb{Z})$.
- <https://beta.lmfdb.org/ModularCurve/Q/27.243.12.a.1/>
- genus = 12 = Mordell–Weil rank :-)

RSZB construct a genus 3 quotient X'_H of $X_{\text{ns}}^+(27)$ over $\mathbb{Q}(\zeta_3)$.

So computing $X'_H(\mathbb{Q}(\zeta_3))$ suffices to finish case $\ell = 3$:-)

Existing methods to do so are not applicable or feasible :-)

This talk. Extending quadratic Chabauty to number fields and applying it to $X'_H/\mathbb{Q}(\zeta_3)$.

Results

$$X'_H: x^4 + (\zeta_3 - 1)x^3y + (3\zeta_3 + 2)x^3 - 3x^2 + (2\zeta_3 + 2)xy^3 - 3\zeta_3xy^2 \\ + 3\zeta_3xy - 2\zeta_3x - \zeta_3y^3 + 3\zeta_3y^2 + (-\zeta_3 + 1)y + (\zeta_3 + 1) = 0.$$

Theorem. (Balakrishnan-Betts-Hast-Jha-M., 2025)

$$X'_H(\mathbb{Q}(\zeta_3)) = \left\{ (0, -\zeta_3 - 1), (1, -\zeta_3 - 1), (\zeta_3 + 1, -\zeta_3 - 1), (0, -\zeta_3), (\zeta_3 + 1, 0), (2\zeta_3 + 2, \zeta_3), (\zeta_3, 1), \right. \\ \left. \left(\frac{\zeta_3 - 3}{2}, \frac{\zeta_3 + 2}{2} \right), \left(\frac{-\zeta_3 - 2}{3}, \frac{\zeta_3 + 2}{3} \right), \left(\frac{-\zeta_3}{2}, \frac{-1}{2} \right), \left(\frac{5\zeta_3 + 4}{7}, -1 \right), (1 : 0 : 0), (1 : \zeta_3 + 1 : 0) \right\}.$$

Corollary. We have $\#X_{\text{ns}}^+(27)(\mathbb{Q}) = 8$; all points are CM, with discriminants $-4, -7, -16, -19, -28, -43, -67, -163$.

Corollary. If E/\mathbb{Q} is non-CM, then $\text{im } \bar{\rho}_{E,3^\infty}$ is one of 47 subgroups of $\text{GL}_2(\mathbb{Z}_3)$ of level at most 27 and index at most 72 listed by RSZB.

Part II

Chabauty methods over \mathbb{Q}

Chabauty methods: idea

Quadratic Chabauty is a p -adic analytic method to **compute** $C(\mathbb{Q})$ for certain nice¹ curves C/\mathbb{Q} of genus ≥ 2 , extending linear Chabauty.

Idea of Chabauty-type methods over \mathbb{Q}

Step 1. Construct a nontrivial **locally analytic** function

$$F: C(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p \quad \text{such that } F(C(\mathbb{Q})) = 0.$$

Step 2. Compute the (finitely many!) zeros of F and find $C(\mathbb{Q})$ among them.

Theorem. (Chabauty, 1941, Coleman, 1985)

Let $J := \text{Jac}_C$. If $\text{rk } J(\mathbb{Q}) < g$, then there is an effectively computable F as in Step 1.

¹smooth, projective, geometrically integral

Linear Chabauty over \mathbb{Q}

Fix $b \in C(\mathbb{Q})$ and $\iota = \iota_b: C \hookrightarrow J; \quad x \mapsto [x - b]$.

Commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) \\ \iota \downarrow & & \downarrow \iota \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) \end{array}$$

Analytic homomorphism:

$$\log: J(\mathbb{Q}_p) \xrightarrow{\sim} T_0 J(\mathbb{Q}_p) \xrightarrow{\sim} H^0(J_{\mathbb{Q}_p}, \Omega^1)^\vee \xrightarrow{\sim} H^0(C_{\mathbb{Q}_p}, \Omega^1)^\vee =: T_p$$

Chabauty–Coleman

$$\begin{array}{ccccc}
 C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) & & \\
 \downarrow \iota & & \downarrow \iota & \searrow & \\
 J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & T_p
 \end{array}$$

If $\text{rk } J(\mathbb{Q}) < g$, there is an $\omega_C \in H^0(C_{\mathbb{Q}_p}, \Omega^1) \setminus \{0\}$ with
 $(\log D)(\omega_C) = 0$ for all $D \in J(\mathbb{Q})$.

Hence

$$F: C(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p; \quad x \mapsto (\log \iota(x))(\omega_C)$$

satisfies $F(C(\mathbb{Q})) = 0$.

Coleman:

$$F(x) = \int_b^x \omega_C$$

Quadratic Chabauty over \mathbb{Q}

Kim (2006, 2009): conjectural extension of linear Chabauty to all C/\mathbb{Q} using unipotent arithmetic fundamental groups \rightsquigarrow

$$C(\mathbb{Q}) \subseteq \cdots \subseteq C(\mathbb{Q}_p)_n \subseteq C(\mathbb{Q}_p)_{n-1} \subseteq \cdots \subseteq C(\mathbb{Q}_p)_1 \subseteq C(\mathbb{Q}_p).$$

Conjecture (Kim, 2009). $C(\mathbb{Q}_p)_n$ is finite for $n \gg 0$.

Quadratic Chabauty (Balakrishnan–Dogra, 2016): $F: C(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ under certain restrictions, vanishing on $C(\mathbb{Q})$

Algorithm and Magma-implementation:
Balakrishnan–Dogra–M.–Tuitman–Vonk (2019)

Alternative approaches:

- Edixhoven–Lido: via Poincaré torsors
- Besser–M.–Srinivasan: via p -adic Arakelov theory

Comparison over \mathbb{Q}

Method	Linear Chabauty	Quadratic Chabauty
cuts out:	$C(\mathbb{Q}_p)_1$	$C(\mathbb{Q}_p)_2$
condition:	$\mathrm{rk} J(\mathbb{Q}) < g$	$\mathrm{rk} J(\mathbb{Q}) < g - 1 + \mathrm{rk} \mathrm{NS}(J)$
integrals in $F(x)$:	$\int_b^x \omega$	$\int_b^x \omega_1, (\int_b^x \omega_1) \cdot (\int_b^x \omega_2), \int_b^x \eta_1$ $\int_b^x \eta_2 \eta_1 := \int_b^x (\eta_2(y) \int_b^y \eta_1)$
differentials:	ω regular	ω_i regular, η_i log-differentials
source:	Linear relations in $\log(J(\mathbb{Q}) \otimes \mathbb{Q}_p) \subseteq T_p$	Quadratic relations in $\log(J(\mathbb{Q}) \otimes \mathbb{Q}_p) \subseteq T_p$
extensions & variants	Flynn, Bruin; Siksek; Stoll	Balakrishnan–Dogra; Gajović–M. Dogra–Le Fourn; Dogra, Berry Balakrishnan–Besser–M.

Part III

Chabauty methods over number fields

Chabauty over number fields: idea

For simplicity:

- $K = \mathbb{Q}(\zeta_3)$.
- C/K : nice curve of genus $g \geq 2$,
- $b \in C(K) \neq \emptyset$ base point, $\iota = \iota_b$.
- p : good reduction prime for C such that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ is split.

Idea (Wetherell, Siksek). Use both \mathfrak{p} and \mathfrak{p}' .

Step 1. Construct ≥ 2 nontrivial locally analytic functions

$$F: C(K \otimes \mathbb{Q}_p) \simeq C(K_{\mathfrak{p}}) \oplus C(K_{\mathfrak{p}'}) \longrightarrow \mathbb{Q}_p \quad \text{such that } F(C(K)) = 0.$$

Step 2. Compute the (hopefully finitely many!) common zeros and find $C(K)$ among them.

Linear Chabauty over number fields

$$\begin{array}{ccccc}
 C(K) & \longrightarrow & C(K \otimes \mathbb{Q}_p) & & \\
 \downarrow \iota & & \downarrow \iota & \searrow & \\
 J(K) & \longrightarrow & J(K \otimes \mathbb{Q}_p) & \xrightarrow{\log} & H^0(C_p, \Omega^1)^\vee \oplus H^0(C_{p'}, \Omega^1)^\vee =: T_p
 \end{array}$$

Explicitly, for $(D_1, D_2) \in J(K_p) \oplus J(K_{p'}) \cong J(K \otimes \mathbb{Q}_p)$:

$$\log(D_1, D_2)(\omega_1, \omega_2) = \left(\int^{D_1} \omega_1, \int^{D_2} \omega_2 \right)$$

Siksek: If $\text{rk } J(K) \leq 2(g-1)$, get 2 locally analytic functions $F: C(K \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ that vanish on $C(K)$.

Finiteness of common zero set is often satisfied but hard to predict (Siksek, Triantafillou, Hast, Dogra). **Not an issue in practice.**

$(p\text{-adic})$ heights

Relations behind quadratic Chabauty come from \mathbb{Q}_p -valued heights.

More generally:

- L : local field, $\text{char}(L) = 0$.
- $\chi: \mathbb{A}_K^*/K^* \rightarrow L$ continuous nontrivial idèle class character

Get symmetric L -bilinear height pairing

$$\langle \cdot, \cdot \rangle^\chi: (J(K) \otimes L) \times (J(K) \otimes L) \rightarrow L.$$

Idea. Construct local height pairings and use χ to globalize.

Example. $L = \mathbb{R}$, χ idèle norm \rightsquigarrow canonical (Néron–Tate) height.

We use $L = \mathbb{Q}_p$ and choose $2 = r_2(K) + 1$ independent χ, χ' . E.g.

- $\chi_p = \log_p$ and $\chi_{p'} = 0$
- $\chi'_{p'} = \log_p$ and $\chi'_p = 0$,

where $\log_p: \mathbb{Q}_p^\times \rightarrow \mathbb{Q}_p$ and $\log_p(p) = 0$.

Assumptions

Assume $\mathrm{rk} \mathrm{NS}(J) > 1$ and choose nonzero $Z \in \ker(\mathrm{NS} J \rightarrow \mathrm{NS} C)$.

Define $h_Z: C(K) \rightarrow \mathbb{Q}_p$ by

$$h_Z(x) := \langle \iota(x), Z(\iota(x)) + c_Z \rangle^x,$$

where $c_Z \in J(K)$ is the Chow–Heegner point wrt. Z .

Also assume that

$$\log: J(K) \otimes \mathbb{Q}_p \rightarrow J(K \otimes \mathbb{Q}_p) \rightarrow T_p$$

is an **isomorphism**.

- In particular $\mathrm{rk} J(K) = 2g = [K : \mathbb{Q}]g$.
- Can generalise to C, K such that

$$\mathrm{rk} J(K) \leq [K : \mathbb{Q}](g - 1) + (\mathrm{rk} \mathrm{NS}(J) - 1)(r_2(K) + 1).$$

Quadratic Chabauty over number fields: Theory

$$h_Z: C(K) \rightarrow \mathbb{Q}_p, \quad h_Z(x) := \langle \iota(x), Z(\iota(x)) + c_Z \rangle^x$$

Theorem. (Balakrishnan-Betts-Hast-Jha-M., 2025)

For all $\mathfrak{q} \subset \mathcal{O}_K$ prime there is a function

$$h_{\mathfrak{q}}: C(K_{\mathfrak{q}}) \rightarrow \mathbb{Q}_p \quad \text{such that:}$$

(1) For $\mathfrak{q} \nmid p$: $h_{\mathfrak{q}}$ has finite image. For good $\mathfrak{q} \nmid p$: $h_{\mathfrak{q}} = 0$.

(2) For $x \in C(K)$:

$$\sum_{\mathfrak{q}} h_{\mathfrak{q}}(x) = h_Z(x).$$

(3) h_p and $h_{p'}$ are locally analytic.

(4) h_Z extends to locally analytic $h_Z: C(K \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$.

(5) $F := h_Z - h_p - h_{p'}: C(K \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ is non-constant.

Quadratic Chabauty over number fields: algorithm

$$F := h_Z - h_p - h_{p'}: C(K \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$$

Corollary.

$$F(x) = \sum_{\text{all } q} h_q(x) - h_p(x) - h_{p'}(x) = \sum_{q \nmid p} h_q(x) \text{ for all } x \in C(K).$$

In particular, if $h_q \equiv 0$ for all $q \nmid p$, then $F(C(K)) = 0$.

“Algorithm” to compute $C(K)$.

- (a) Show $h_q \equiv 0$ for all $q \nmid p$ (if that holds);
- (b) expand h_p and $h_{p'}$ locally into power series on $C(K_p)$;
- (c) expand h_Z on $C(K \otimes \mathbb{Q}_p)$;
- (d) do all of this for χ' rather than χ ($\rightsquigarrow h'_Z, h'_q, F'$);
- (e) solve for set of common zeros of $F, F': C(K \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ using multivariate Hensel and hope it's finite;
- (f) find $C(K)$ in this set.

Global heights

(c) Expand h_Z into locally analytic function on $C(K \otimes \mathbb{Q}_p)$.

By assumption

$$\log: J(K) \otimes \mathbb{Q}_p \xrightarrow{\simeq} H^0(C_p, \Omega^1)^\vee \oplus H^0(C_{p'}, \Omega^1)^\vee =: T_p,$$

and we get

$$h_Z(x) = \langle \iota(x), Z(\iota(x)) + c_Z \rangle^\chi = [\log \iota(x), \log(Z(\iota(x)) + c_Z)]^\chi$$

for a locally analytic symmetric bilinear pairing

$$[\cdot, \cdot]^\chi: T_p \times T_p \rightarrow \mathbb{Q}_p.$$

We solve for $[\cdot, \cdot]^\chi$ (and hence h_Z) in terms of a **basis of such pairings** by evaluating in enough points.

Local heights away from p

(a) Find $h_q(C(K_q))$ for all $q \nmid p$.

Theorem. (Betts–Dogra, 2019) For $q \nmid p$, h_q factors through the **irreducible components** of the special fiber \mathcal{C}_s of a semistable regular model \mathcal{C} of C_q .

Corollary. If all points in $C(K_q)$ **reduce to the same component** of \mathcal{C}_s , then $h_q \equiv 0$.

Example. If C has potentially good reduction at q , then $h_q \equiv 0$.

What if $h_q \not\equiv 0$? Betts, Duque-Rosero, Hashimoto and Spelier (2024) describe a complete algorithm to compute (all values of) h_q for hyperelliptic C whose idea generalises.

Local heights above p

(b) Expand h_p on $C(K_p)$.

$K_p \cong \mathbb{Q}_p \Rightarrow$ can compute h_p using algorithm of Balakrishnan-Dogra-M.-Tuitman-Vonk.

Both h_p and Coleman integrals can be described in terms of unipotent overconvergent isocrystals (Nekovář, Besser).

Hence can compute $h_p(x)$ using p -adic Hodge theory in terms of:

- ~> Hodge filtration and Frobenius action of a certain mixed extension of filtered ϕ -modules with graded pieces $\mathbb{Q}_p, H_{\text{dR}}^1(C_{\mathbb{Q}_p})^\vee, D_{\text{cris}}(\mathbb{Q}_p(1));$
- ~> reduction in rigid cohomology, differentials and p -adic linear algebra (Tuitman).

Application to $C = X'_H$, $K = \mathbb{Q}(\zeta_3)$

- Magma-implementation + precision analysis
- $C = X'_H$ has $\text{rk } J(K) = 6 = 2g$ via Kolyvagin–Logachev.
- Use $p = 13 = \text{pp}'$.
- $\text{rk NS}(J) = 3$: RM by $\mathbb{Q}(\zeta_9)^+$
- Compute independent $Z, Z' \in \ker(\text{NS } J \rightarrow \text{NS } C)$ ² using Eichler–Shimura.
- All $h_q = 0$ for $q \nmid 13$ (and both χ and χ'), using a semistable model of $C_{K(1-\zeta_3)}$ constructed by Ossen.
- Get $4 = 2 \cdot 2$ locally analytic functions

$$F: C(K \otimes \mathbb{Q}_{13}) \simeq C(K_p) \times C(K_{p'}) \rightarrow \mathbb{Q}_{13},$$

whose common zero set is precisely $C(K)$. Done!

²actually their action on $H_{\text{dR}}^1(C_{K_p})$ – just what our algorithms really need.

What's next?

Chabauty–Kim.

- Dogra, Berry: Quadratic Chabauty without condition on NS J using map from Bloch–Kato Selmer group to a certain étale algebra and 2-adic Coleman integrals \rightsquigarrow make more explicit and implement in suitable generality
- Equationless (linear or quadratic) Chabauty
- Beyond quadratic Chabauty?
- Higher-dimensional Chabauty? (see Wednesday!)

Open modular curves.

- $X_{\text{ns}}^+(5^2)$: $g = 14$
- X_H , where H has RSZB-label 49.147.9.1 or 49.147.9.1: $g = 9$.
- ~~$X_{\text{ns}}^+(7^2)$, $g = 69$!~~ Recently done by Furio–Lombardo (see Thursday!)
- $X_{\text{ns}}^+(11^2)$: $g = 511$
- $X_{\text{ns}}^+(\ell)$, $\ell > 17$ prime

Correctness

We implemented (almost) all our algorithms in Magma, which is powerful, but partially closed source.

Kevin Buzzard asks³: “Is this science?”

In our defense:

- Careful precision analysis to guarantee correctness of p -adic approximations
- In most quadratic Chabauty computations so far: more equations $F = 0$ than necessary to cut out finite set \rightsquigarrow sanity checks
- Independent verification for $X_{\text{ns}}^+(13)$ in Sage.

Formalization??

³about the computation for $X_{\text{ns}}^+(13)$