Geometric Quadratic Chabauty over number fields

joint with David Lilienfeldt, Luciena X. Xiao, Zijian Yao

Pavel Čoupek
Purdue University
MFF Number Theory Seminar,
15. 12. 2020

I. Motivation & Background

Classical algebraic geometry – affine

Fix a field K. Let $f_1, f_2, \ldots, f_m \in K[x_1, x_2, \ldots, x_n]$ be some polynomials.

- The *affine variety* $X = V(f_1, f_2, \ldots, f_m)$ "is"

$$X \equiv X(\overline{K}) = \{P \in \overline{K}^n : f_i(P) = 0 \ \ \forall i\} \subseteq \mathbb{A}^n(\overline{K}) = \overline{K}^n$$

  (together with *Zariski topology*: a subset $Z \subset X(\overline{K})$ is closed if $Z = V(g_1, \ldots, g_l)$ for some $g_1, g_2, \ldots g_l \in K[x_1, x_2, \ldots, x_n]$)

- In fact, for a field extension $K \hookrightarrow L$, denote by $X(L)$ the *set of L-points of X*,

$$X(L) = \{P \in L^n : f_i(P) = 0 \ \ \forall i\}.$$

- In particular, $X(K)$ is the *set of K-rational points* of X.
- Setting $A = K[\underline{x}]/(\underline{f})$, (or, better: $A' = K[\underline{x}]/\sqrt{(\underline{f})}$), there is a natural bijection

$$\mathrm{Alg}_K(A, L) \simeq X(L) \qquad (\text{ and also } \mathrm{Alg}_K(A', L) \simeq X(L) \text{ }).$$

  A' is called the *coordinate ring* of X.

Classical algebraic geometry – projective

Fix a field K. Let $f_1, f_2, \dots, f_m \in K[x_0, x_1, \dots, x_n]$ be some nonconstant *homogeneous* polynomials: $f_i(\lambda \underline{x}) = \lambda^{d_i} f_i(\underline{x})$ where $d_i = \deg f_i$.

- For a field embedding $K \hookrightarrow L$, set

$$\mathbb{P}^n(L) = (L^{n+1} \setminus \{0\})/\sim, \quad v \sim \lambda v \quad \forall \lambda \in L \; \forall v \in L^{n+1}.$$

- The *projective variety* $X = V_p(f_1, f_2, \dots, f_m)$ determines its sets of L-points,

$$X(L) = \{P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(L) : f_i(x_0, x_1, \dots, x_n) = 0 \;\; \forall i\} \subseteq \mathbb{P}^n(L).$$

- In particular, $X(K)$ is the *set of K-rational points* of X.
- We may again identify $X \equiv X(\overline{K})$ as a subset of $\mathbb{P}^n(\overline{K})$, and endow it with the Zariski topology, where closed subsets are ($\overline{K}$-points of) projective subvarieties.
- A *quasi-projective variety* is an open subset U of a projective variety. It comes with a ring of functions on U.

Diophantine equations and algebraic geometry (I)

Consider a system of diophantine equations

$$f_i(x_1, x_2, \ldots, x_n) = 0, \quad f_i \in \mathbb{Z}[x_1, x_2, \ldots, x_n], \ i = 1, 2, \ldots, m.$$

Suppose that f_i's are homogeneous. Then

$$\begin{aligned} \text{solutions in } \mathbb{Z}^n \quad &\leftrightarrows \quad \text{solutions in } \mathbb{Q}^n \\ \mathbb{Z} \cdot d\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}\right) &\hookleftarrow \left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}\right) \\ d = \operatorname{lcm}(b_1, b_2, \ldots, b_n). & \end{aligned}$$

$\Rightarrow$ Solutions correspond to rational points of the projective variety $X = V_p(f_1, f_2, \ldots, f_m)$

$\Rightarrow$ One can use geometry of X to describe the solutions.

Diophantine equations and algebraic geometry (I)

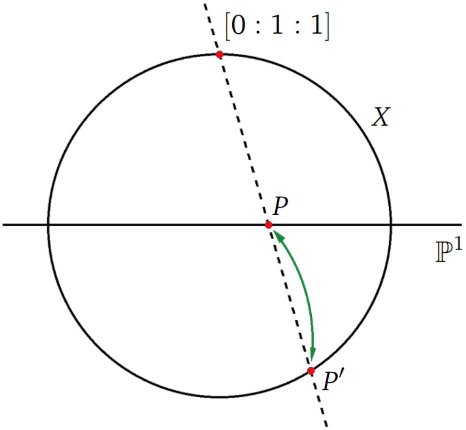
Example (Pythagorean triples)

$$x^2 + y^2 = z^2, \quad x, y, z \in \mathbb{Z}$$

Then $X = V(x^2 + y^2 - z^2)$ is isomorphic to $\mathbb{P}^1$:

$$\begin{aligned} \mathbb{P}^1 &\xrightarrow{\sim} X \\ [t : v] &\longmapsto [2tv : t^2 - v^2 : t^2 + v^2] \\ [x : z - y] &\longleftarrow [x : y : z] \end{aligned}$$

The map $\mathbb{P}^1 \to X$ parametrizes $X(\mathbb{Q})$ by $\mathbb{P}^1(\mathbb{Q})$.



Analytifications

Assume that X is a smooth variety over K.

- If $K \subseteq \mathbb{C}$, then $X(\mathbb{C})$ is naturally a complex manifold - locally, it is isomorphic to unit ball in $\mathbb{C}^m$ for some m.
- An analogue of this holds over other topological fields, such as

$$\mathbb{Q}_p = \left\{ \sum_{i=-n}^{\infty} a_i p^i \mid n \geq 0,\ a_i \in \{0, 1, 2, \ldots, p-1\} \right\},$$

  whose topology is dictated by the norm

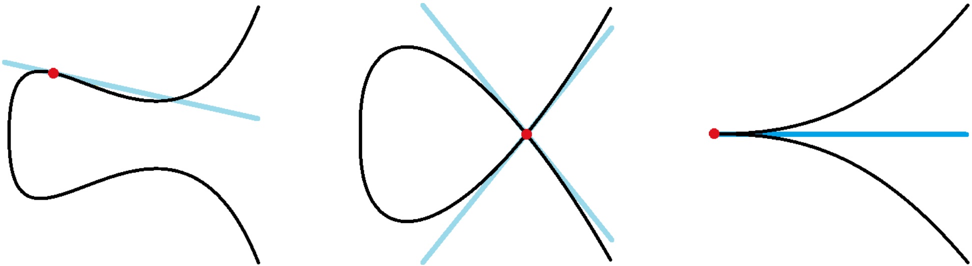
$$\left| \sum_{i=-n}^{\infty} a_i p^i \right| := p^{-k}, \quad k \text{ smallest such that } a_k \neq 0$$

  (more generally, may consider completion $K_{\mathfrak{p}}$ of a number field K at a prime $\mathfrak{p}$).
- If $K \subseteq \mathbb{Q}_p$, then $X(\mathbb{Q}_p)$ has a structure of a *p-adic analytic manifold*. Locally, it s isomorphic to $\mathbb{Z}_p^m$ for some m.

Smooth projective curves

- *Algebraic curves* are varieties of dimension 1.
- A curve is *smooth* if at every point, it has only one tangent line.

Example



Smooth curve, e.g. $y^2 = x^3 - x + 1$

Not smooth - node, e.g. $y^2 = x^3 + x^2$

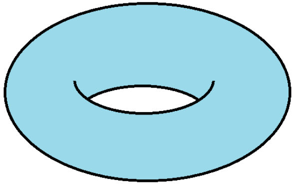
Not smooth - cusp, e.g. $y^2 = x^3$

Smooth projective curves

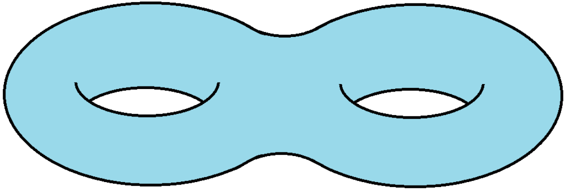
Projective smooth curves are categorized by their *genus*:

- C is a smooth projective curve over $K \subseteq \mathbb{C}$
  $\Rightarrow C(\mathbb{C})$ is a compact complex manifold of dim $= 1$ (*Riemann surface*)
  $\Rightarrow C(\mathbb{C})$ is a compact topological manifold of dim $= 2$.
- Classification theorem $\Rightarrow C(\mathbb{C})$ is a sphere with g handles attached.
- The genus of $C = g$:=the number of handles.

Example



Genus 1 curve



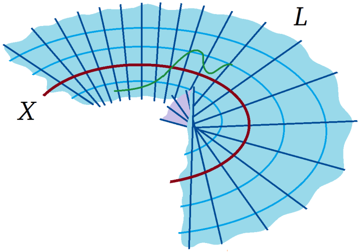
Genus 2 curve

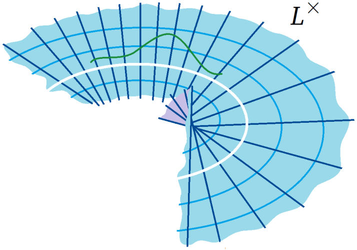
Line bundles and $\mathbb{G}_m$–torsors

- A *line bundle* on a variety X is a variety L together with a map $\pi : L \to X$ such that

$$\forall U \subseteq X \text{ small enough open: } (\pi^{-1}(L) \xrightarrow{\pi} U) \simeq (U \times \mathbb{A}^1 \xrightarrow{\mathrm{pr}_U} U)$$

  (+ compatibility condition on the iso's).
- Fibers of L over points of X are 1-dim. vector spaces, that "vary continuously".
- An isomorphic copy of X sits in L, as the 0-elements in each fiber.
- A $\mathbb{G}_m$-*torsor* $L^\times$ is obtained from L by removing X from L. It retains the action of nonzero scalars in fibres.

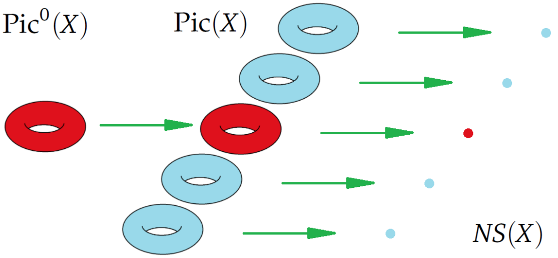




Picard variety

Assume that X is projective over K, $\operatorname{char} K = 0$.

- Line bundles on X form a commutative group, under $(L_1, L_2) \mapsto L_1 \otimes L_2$. The resulting group is $\mathrm{Pic}(X)$, the *Picard group of X*.
- $\mathrm{Pic}(X)$ itself has a geometric structure, and the connected component $\mathrm{Pic}^0(X)$ of the neutral element is called the *Picard variety of X*.
  $\mathrm{Pic}^0(X)$ is an *Abelian variety* = projective connected variety with group structure.
- $NS(X) := \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$ is the *Néron-Severi group*. It is a fin-gen Abelian group.



Picard variety

Two important cases:

1. When $X = C$ is a smooth projective curve, $J := \mathrm{Pic}^0(C)$ is called the *Jacobian of* C.
   - $\dim J =$ genus of C.
   - Any "choice of origin" $b \in C(K)$ induces an embedding $j_b : C \hookrightarrow J$, called *Abel–Jacobi map*.
2. When $X = A$ is an Abelian variety, $A^\vee := \mathrm{Pic}^0(A)$ is called the *dual abelian variety of* A.
   - $A^{\vee\vee} = A$
   - There are always isogenies $A \to A^\vee, A^\vee \to A$.
   - If $A = J$ is a Jacobian of a curve, the isogenies may be chosen as isomorphisms.

Diophantine equations and algebraic geometry (II)

- Want to "attach geometry" to general systems of diophantine equations.
- Given such a system,

$$(*) \qquad f_i(\underline{x}) = 0, \;\; f_i(\underline{x}) \in \mathbb{Z}[x_1, x_2, \ldots, x_n],$$

upon setting $A = \mathbb{Z}[\underline{x}]/(\underline{f})$, one still has

$$\mathrm{Alg}_{\mathbb{Z}}(A, \mathbb{Z}) \overset{1\text{-}1}{\leftrightarrow} \text{ solutions of } (*).$$

$\rightsquigarrow$ need a geometric object for which A would be a "coordinate ring".

- Such an object is *the affine scheme* $X = \operatorname{Spec} A$:
  - As a topological space, $\operatorname{Spec} A = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ is a prime ideal}\}$, and closed sets are of the form $V(I) = \{\mathfrak{p} \mid I \subseteq \mathfrak{p}\}$ for any ideal $I \subseteq A$
  - Given another affine scheme $Y = \operatorname{Spec} B$, maps of schemes $Y \to X$ correspond precisely to

$$\mathrm{Alg}_{\mathbb{Z}}(A, B) =: X(B),$$

the "B-valued points of X".

Schemes (from bird's-eye view)

- General schemes are spaces that are locally modelled by affine schemes.
- Given a scheme S, one can consider *schemes over* S (S-*schemes*)= morphisms of schemes $X \to S$. Morphism of S-schemes is a morphism of schemes compatible with the structure maps to S.
- Any scheme is tautologically a scheme over $\operatorname{Spec}\mathbb{Z}$; given a field K, classical varieties over K naturally correspond to certain schemes over $\operatorname{Spec} K$.
- Given two S-schemes X, Y, the set of S-morphisms $Y \to X$ is sometimes denoted by $X(Y)$, and called the "set of Y-valued points of X".
- Points are functorial in X and Y:

a morphism of S-schemes $Y_1 \to Y_2$ ($X_1 \to X_2$, resp.) induces a map $X(Y_2) \to X(Y_1)$. ($X_1(Y) \to X_2(Y)$ resp.)

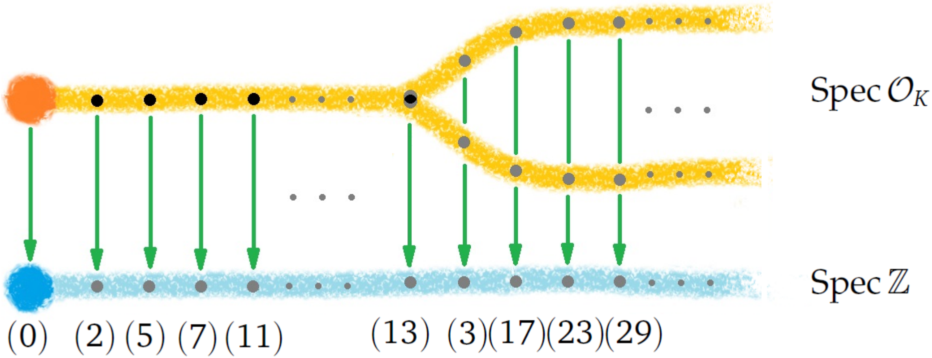
Schemes – examples

Example (Number fields)

$K/\mathbb{Q}$ finite extension ($K = \mathbb{Q}(\sqrt{13})$ on picture).

$\mathbb{Z} \subseteq \mathcal{O}_K$ induces a map $\operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbb{Z}$, which is a cover of "curves" of degree $[K : \mathbb{Q}]$.

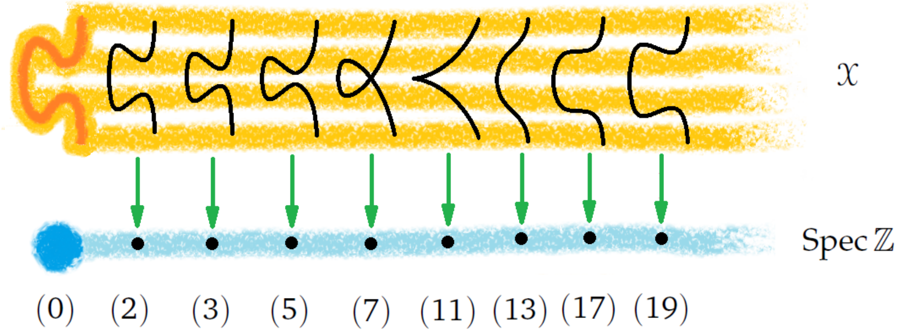
Fact: $\operatorname{Pic}(\operatorname{Spec} \mathcal{O}_K) = Cl(K)$.



Schemes – examples

Example (integral models)

For a variety $X/\mathbb{Q}$, one can consider various schemes $\mathcal{X}$ over $\mathbb{Z}$ such that $\mathcal{X}(R) = X(R)$ for every $\mathbb{Q}$-algebra R.
Upshot: Can consider points $\mathcal{X}(R)$ for R not necessarily over $\mathbb{Q}$ - e.g. $\mathcal{X}(\mathbb{F}_p)$ or $\mathcal{X}(\overline{\mathbb{F}_p})$.



Two key finiteness results

Theorem (Mordell–Weil Theorem; ’22, ’29)

Let A be an Abelian variety over a number field K. Then $A(K)$ is a finitely generated group.

Theorem (Mordell’s conjecture; Faltings ’83)

Let C be a smooth, projective, geometrically connected curve of genus $g \geq 2$ over a number field K. Then $C(K)$ is a finite set.

Questions of *effectivity* and *explicit methods*:

- How to algorithmically compute $C(K)$?
- How to produce sharp bound?
- How to make optimal bounds in families?
- ...

II. Chabauty–Coleman & Beyond

Chabauty–Coleman

Let J denote the Jacobian of C. Denote $r = \mathrm{rank}_{\mathbb{Z}} J(K)$ its Mordell-Weil rank.

Theorem (Chabauty '41)

If $r \leq g - 1$ then $|C(K)|$ is finite.

- first proof of special case of Mordell's conjecture

Theorem (Coleman '85)

Under the same assumption, fix an unramified prime $\mathfrak{p}|p$ of good reduction such that $p > 2g$. Then

$$|C(K)| \leq N(\mathfrak{p}) + 2g(\sqrt{N(\mathfrak{p})} + 1) - 1.$$

- "good" bound on the size of $|C(K)|$
- Further improvements by Stoll (2006), Katz–Zurieck-Brown (2013), Katz–Rabinoff–Zurieck-Brown (2016), . . .
- Siksek (2013): explicit Chabauty over number fields, method of Weil restriction

Chabauty–Coleman

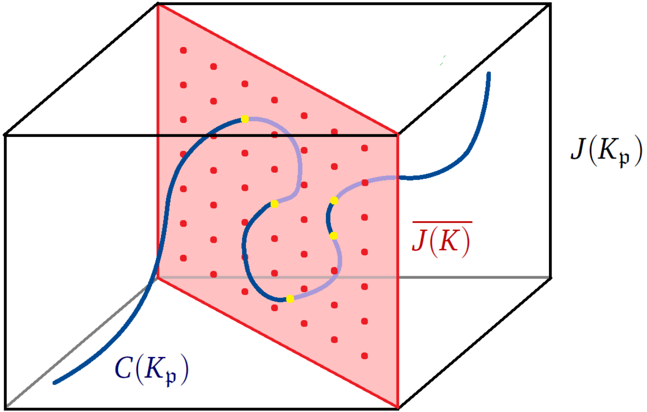
Strategy:
Let $b \in C(K)$ be a point, and $j_b : C \hookrightarrow J$ the Abel–Jacobi map.

$$\begin{array}{ccccc}
C(K) & & \hookrightarrow & & C(K_{\mathfrak{p}}) \\
\downarrow j_b & & & \swarrow\!\!\!\nearrow & \downarrow j_b \\
J(K) & \hookrightarrow & \overline{J(K)} & \longrightarrow & J(K_{\mathfrak{p}})
\end{array}$$

Then $C(K) \subseteq C(K_{\mathfrak{p}}) \cap \overline{J(K)}$.

$C(K_{\mathfrak{p}}), \overline{J(K)}$ are $\mathfrak{p}$-adic/p-adic manifolds of dimensions 1 and $r' \leq r$, resp., in the $\mathfrak{p}$-adic manifold $J(K_{\mathfrak{p}})$ of dimension $g > r'$.

Chabauty–Coleman



Chabauty–Coleman

Strategy:

$$\begin{array}{ccccccc}
C(K) & \hookrightarrow & & & C(K_{\mathfrak{p}}) & & \\
\downarrow {\scriptstyle j_b} & & & \swarrow\!\!\nearrow & \downarrow {\scriptstyle j_b} & \overset{\int}{\searrow} & \\
J(K) & \hookrightarrow & \overline{J(K)} & \longrightarrow & J(K_{\mathfrak{p}}) & \xrightarrow{\log} & H^0(J, \Omega^1_{J_{K_{\mathfrak{p}}}/K_{\mathfrak{p}}})^\vee
\end{array}$$

log, $\int$ are given by $x \mapsto \int_b^x (\bullet)$, the *Coleman integral*. Let

$$V = \{\omega \in H^0(J, \Omega^1_{J_{K_{\mathfrak{p}}}/K_{\mathfrak{p}}}) \mid \int_b^x \omega = 0 \ \ \forall x \in \overline{J(K)}\}.$$

Then

$$C(K_{\mathfrak{p}}) \cap \overline{J(K)} \subseteq \{x \in C(K_{\mathfrak{p}}) \mid \int_b^x j_b^* \omega = 0 \ \ \forall \omega \in V\} =: C(K_{\mathfrak{p}})_1.$$

If $r' < g$, then $V \neq 0$ and it can be shown that $C(K_{\mathfrak{p}})_1$ is finite.

Chabauty–Coleman

Example (Hirakawa–Matsumura 2019)

Q: *Can a rational right triangle and a rational isosceles triangle have the same area and perimeter?*

Upon setting up parameters for lengths of sides appropriately and simplifying, this leads to the task of finding $C(\mathbb{Q})$ for

$$C : y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

A list of 10 points is

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

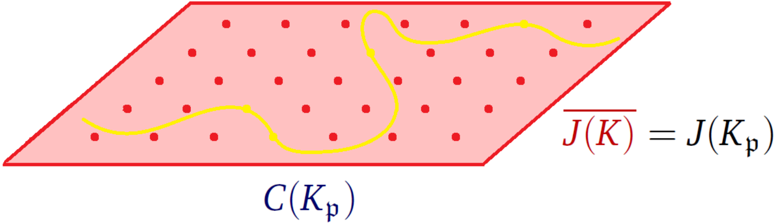
Only P^+ corresponds to a pair of triangles.

Chabauty–Coleman bound $\Rightarrow |C(\mathbb{Q})| \leq 10 \Rightarrow$ the list is complete.

The unique pair of triangles has sides $(377, 135, 352)$ and $(366, 366, 132)$, up to scaling.

Chabauty–Coleman

Problem when $r' = g$:



$\rightsquigarrow$ need to "extend the method beyond Jacobian".

Chabauty-Kim program

Kim (2005, 2009)
Goal: Extend the method beyond the $r < g$ case

$$\begin{array}{ccccc}
C(K) & \hookrightarrow & C(K_{\mathfrak{p}}) & & \\
\downarrow j_n & & \downarrow j_{n,p} & \searrow^{\int} & \\
\mathrm{Sel}(U_n) & \xrightarrow{loc_p} & H^1_f(K_{\mathfrak{p}}, U_n) & \xrightarrow{\log_n} & \pi_1^{dR}(C_{K_{\mathfrak{p}}})_n/\mathrm{Fil}^0
\end{array}$$

$U_n =$ certain unipotent quotients of $\pi_1^{et}(C_{\overline{K}})$

$$C(K_{\mathfrak{p}})_n = j_{n,p}^{-1}(loc_p(\mathrm{Sel}(U_n)))$$

Conjecture (Kim)

For $n >> 0$, $C(K_{\mathfrak{p}})_n$ is finite and coincides with $C(K)$.

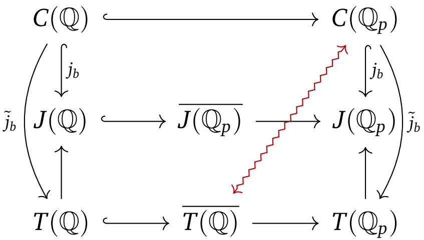
Quadratic Chabauty

- Case $n = 2$ of Kim's program
- uses double Coleman integrals
- Balakrishnan-Dogra (2016, 2017) - quadratic Chabauty over $\mathbb{Q}$
- Balakrishnan-Dogra-Müller-Tuitman-Vonk (2017)
  - determined rational points of $X_s(13)$, "cursed curve"
  - application to Serre's uniformity problem
- Balakrishnan-Besser-Bianchi-Müller (2019)
  - explicit quadratic Chabauty for hyperelliptic curves over number fields

II. Geometric quadratic Chabauty

Geometric quadratic Chabauty over $\mathbb{Q}$

Edixhoven–Lido (2019)
Goal: Formulate quadratic Chabauty in terms of "simple" geometry

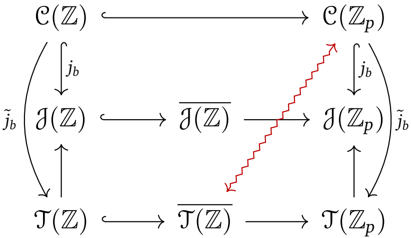


T is a certain $\mathbb{G}_m^{\rho-1}$-torsor on J, $\qquad \rho = \operatorname{rank} NS(J)$

Problem: $T(\mathbb{Q})$ has too many points ($\mathbb{Q}^{\times,\rho-1}$ in fibers)

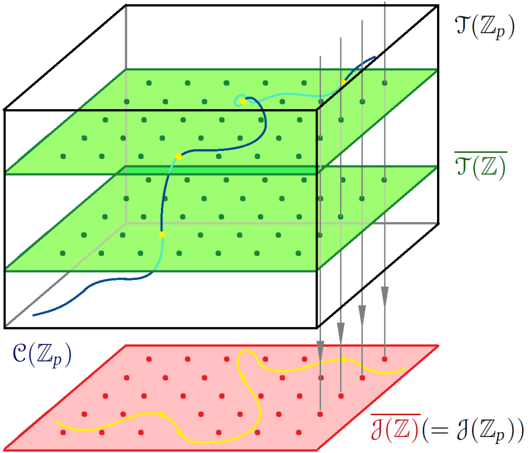
Geometric quadratic Chabauty over $\mathbb{Q}$

Edixhoven–Lido (2019)
Goal: Formulate quadratic Chabauty in terms of ″simple″ geometry



$\mathcal{T}$ is a certain $\mathbb{G}_m^{\rho-1}$-torsor on $\mathcal{J}$,
$\mathcal{J}$ is the Néron model of J,
$\mathcal{C}$ is the smooth locus in a regular proper model of C.

Geometric quadratic Chabauty over $\mathbb{Q}$



Poincaré biextension

Let $P \to J \times J^\vee$ be the *Poincaré line bundle*:

- $P|_{J\times\{x\}} = L_x$, the line bundle corresponding to $x \in J^\vee$
- $P|_{J\times\{0\}}, P|_{\{0\}\times J^\vee}$ are trivial line bundles on $J, J^\vee$, resp.

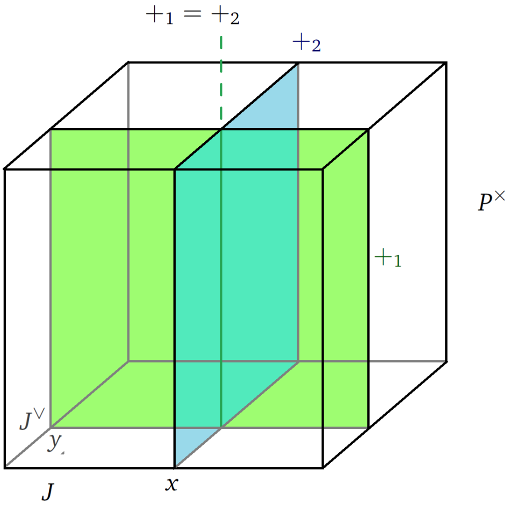
Let $P^\times$ be the associated $\mathbb{G}_m$-torsor on $J \times J^\vee$.
It has the structure of a $\mathbb{G}_m$*-biextension*:

- There are partial operations
  - $+_1$ on all points over a point of the form $(*, y) \in J \times J^\vee$, making it a commutative group,
  - $+_2$ on all points over a point of the form $(x, *) \in J \times J^\vee$, making it a commutative group,
  - compatibility of the two operations:

$$(a +_1 b) +_2 (c +_1 d) = (a +_2 c) +_1 (b +_2 d)$$

whenever the above makes sense.

Poincaré biextension



Constructing T

From now on, assume that $\rho = \operatorname{rank} NS(J) = 2$**.** We need a non-trivial $\mathbb{G}_m$–torsor T such that C lifts to T – equivalently, such that $T|_C$ is a trivial torsor over C.

$$\begin{array}{ccccccccc}
 & & & & \operatorname{Ker} j_b^* & \xrightarrow{\simeq} & \operatorname{Ker} \overline{j_b^*} & & \\
 & & & & \big\downarrow & & \big\downarrow & & \\
0 & \longrightarrow & J^\vee & \longrightarrow & \operatorname{Pic}(J) & \longrightarrow & NS(J) & \longrightarrow & 0 \\
 & & \big\downarrow \simeq & & \big\downarrow j_b^* & & \big\downarrow \overline{j_b^*} & & \\
0 & \longrightarrow & J & \longrightarrow & \operatorname{Pic}(C) & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Then $\operatorname{rank} \operatorname{Ker} j_b^* = \rho - 1 = 1$, so there is essentialy unique $\mathbb{G}_m$-torsor on J that is trivial over $C \hookrightarrow J$. Moreover, it is of the form

$$T' = (\mathrm{id}_J, \mathrm{t}_c \circ f)^* P^\times, \; f \in \operatorname{Hom}(J, J^\vee)^+, \; c \in J^\vee(\mathbb{Q}).$$

That is, T' is obtained by restricting the Poincaré torsor to a copy of J, embeded into $J \times J^\vee$ via $(\mathrm{id}_J, \mathrm{t}_c \circ f) : J \to J \times J^\vee$. For technical reasons we take $T = (\mathrm{id}_J, m \cdot \circ \mathrm{t}_c \circ f)^* P^\times$.

Constructing $\mathcal{T}$

The $\mathbb{G}_m$–torsor $\mathcal{T}$ on $\mathcal{J}$ is then given by

$$\mathcal{T} = (\mathrm{id}_{\mathcal{J}}, m \cdot \circ \mathrm{t}_c \circ f)^* \mathcal{P}^{\times}$$

for the analogous embedding $(\mathrm{id}_{\mathcal{J}}, m \cdot \circ \mathrm{t}_c \circ f) : \mathcal{J} \to \mathcal{J} \times \mathcal{J}^{\vee \circ}$, where:

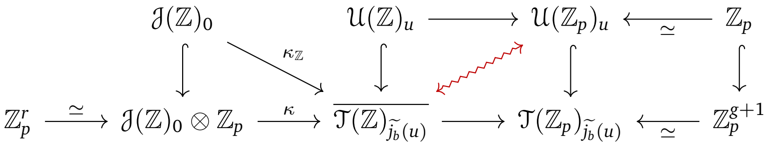
- $\mathcal{J}^{\vee,\circ}$ is a fiberwise connected component of $\mathcal{J}^{\vee}$,
- $\mathcal{P}^{\times}$ is an integral model of $P^{\times}$ as a $\mathbb{G}_m$-biextension,
- m is an integer large enough to annihilate $\mathcal{J}^{\vee}/\mathcal{J}^{\vee \circ}$.

The lift $\tilde{j}_b : \mathcal{C} \to \mathcal{T}$ does not exist globally anymore, but exists on certain open subschemes $\mathcal{U} \subseteq \mathcal{C}$ that are "big enough" to jointly contain all $\mathbb{Z}$-points.

Parametrization of $\overline{\mathcal{T}(\mathbb{Z})}$

- Work on *residue disks*:

$$\mathcal{X}(\mathbb{Z}_p)_x = \text{ set of all } \widetilde{x} \in \mathcal{X}(\mathbb{Z}_p) \text{ reducing to a given } x \in \mathcal{X}(\mathbb{F}_p),$$
$$\mathcal{X}(\mathbb{Z})_x = \mathcal{X}(\mathbb{Z}_p)_x \cap \mathcal{X}(\mathbb{Z}).$$



- $\kappa_{\mathbb{Z}}$ is constructed using $+_1$ and $+_2$ of $\mathcal{P}^{\times}$
- $\kappa : \mathbb{Z}_p^r \to \mathbb{Z}_p^{g+1}$ can be expressed in terms of p-adically convergent power series.

Parametrization of $\overline{\mathcal{T}(\mathbb{Z})}$

As a consequence, the maps $\mathcal{U}(\mathbb{Z}_p)_u \xrightarrow{\widetilde{j_b}} \mathcal{T}(\mathbb{Z}_p)_{\widetilde{j_b}(u)} \xleftarrow{\kappa} \mathcal{J}(\mathbb{Z})_0 \otimes \mathbb{Z}_p$ induce maps of rings of p-adically convergent power series

$$\mathbb{Z}_p\langle X_1\rangle \xleftarrow[\widetilde{j_b}^*]{} \mathbb{Z}_p\langle X_1, \ldots, X_{g+1}\rangle \xrightarrow{\kappa^*} \mathbb{Z}_p\langle Y_1, \ldots, Y_r\rangle,$$

and upon setting $\quad A = \mathbb{Z}_p\langle Y_1, \ldots, Y_r\rangle / I, \quad I = (\kappa^*(\operatorname{Ker} \widetilde{j_b}^*)),$
$\kappa^{-1}\left(\overline{\mathcal{T}(\mathbb{Z}_p)}_{\widetilde{j_b}(u)} \cap \mathcal{U}(\mathbb{Z}_p)_u\right)$ corresponds to $\operatorname{Hom}(A, \mathbb{Z}_p)$.

Theorem (Edixhoven–Lido)

Assuming that $\overline{A} = A \otimes \mathbb{F}_p$ is finite, one has

$$|\mathcal{U}(\mathbb{Z})_u| \leq \dim_{\mathbb{F}_p} \overline{A}.$$

Example (Edixhoven–Lido)

[EL] use the method to explicitly determine $C(\mathbb{Q})$ for a curve C with $g = 2, r = 2, \rho = 2$.
$C =$ certain quotient of the modular curve $X_0(129)$; $\quad |C(\mathbb{Q})| = 14$.

Geometric quadratic Chabauty over number fields

Let $K/\mathbb{Q}$ be a number field, $[K:\mathbb{Q}] = d = r_1 + 2r_2$.

Main obstacles in the number field case:

1. The class group $Cl(K) = \mathrm{Pic}(\mathcal{O}_K)$ may prevent lifting $\mathcal{O}_K$-points and curves:

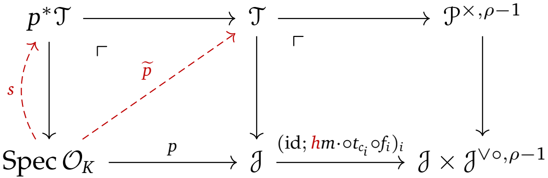
$$\begin{array}{ccc} p^*\mathcal{T} & \longrightarrow & \mathcal{T} \\ {\scriptstyle ?}\,\uparrow\downarrow & \lrcorner\;\nearrow^{?} & \downarrow \\ \operatorname{Spec}\mathcal{O}_K & \xrightarrow[p]{} & \mathcal{J} \end{array} \qquad \begin{array}{ccc} j_b^*\mathcal{T} & \longrightarrow & \mathcal{T} \\ {\scriptstyle ?}\,\uparrow\downarrow & \lrcorner\;\nearrow^{?} & \downarrow \\ \mathcal{U} & \xrightarrow[j_b]{} & \mathcal{J} \end{array}$$

   $\mathrm{Pic}(\mathcal{U}) \to \mathrm{Pic}(C)$ has an h-torsion kernel, $h = |\mathrm{Pic}(\mathcal{O}_K)|$

2. $\mathcal{T}(\mathcal{O}_K) \to \mathcal{J}(\mathcal{O}_K)$ has still too many points, namely $\mathcal{O}_K^{\times,\rho-1} \simeq (\text{torsion}) \times \mathbb{Z}^{\delta(\rho-1)}$, $\delta = r_1 + r_2 - 1$ in (trivial) fibres

Geometric quadratic Chabauty over number fields

Solution to 1 (for $\rho = 2$):



Let $\mathcal{T}' = (\mathrm{id},\, m\cdot \circ t_{c_i} \circ f_i)_i^* \mathcal{P}^{\times}$.

Then by the biextension law, one can show that

$$\mathcal{T} = (\mathrm{id},\, hm\cdot \circ t_{c_i} \circ f_i)_i^* \mathcal{P}^{\times} = (\mathcal{T}')^{\otimes h},$$
$$p^*\mathcal{T} = (p^*\mathcal{T}')^{\otimes h}$$

$\Rightarrow p^*\mathcal{T}$ is an h-th power of a torsor on Spec $\mathcal{O}_K$, therefore trivial, i.e. s exists.

Geometric quadratic Chabauty over number fields

Solution to 2:

$$\begin{array}{ccc} \mathcal{J}(\mathcal{O}_K)_0 \times \mathcal{O}_{K,\mathrm{tf}}^{\times,\rho-1} & & \mathcal{U}(\mathcal{O}_K)_u \\ \big\downarrow & \overset{\kappa_{\mathbb{Z}}}{\searrow} & \big\downarrow \\ (\mathcal{J}(\mathcal{O}_K)_0 \times \mathcal{O}_{K,\mathrm{tf}}^{\times,\rho-1}) \otimes \mathbb{Z}_p & \xrightarrow{\kappa} & \overline{\mathcal{T}(\mathcal{O}_K)_{\widetilde{j_b}(u)}} \end{array}$$

Parametrization includes action on fibers by a torsion-free part of $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$, $\mathcal{O}_{K,\mathrm{tf}}^{\times,\rho-1} \simeq \mathbb{Z}^{\delta(\rho-1)}$.

Key fact: The $\mathbb{G}_m^{\rho-1}$-action on $\mathcal{P}^{\times,\rho-1}$ is expressible in terms of $+_1, +_2 \Rightarrow \kappa_{\mathbb{Z}}$ is still expressible in terms of $+_1, +_2$, and p-adic interpolation still works.

Summary over number fields

- Fix integral models $\mathcal{C}, \mathcal{J}, \mathcal{P}^\times, \mathcal{U}, \ldots,$ analogously
- Fix a rational prime p of good reduction, $e(\mathfrak{p}_i/p) < p - 1 \;\; \forall \mathfrak{p}_i | p$, and work on "multiresidue disks": fibers of

$$\mathcal{X}(\mathcal{O}_K) \subseteq \mathcal{X}(\prod_i \mathcal{O}_{K,\mathfrak{p}_i}) \to \mathcal{X}(\prod_i \mathbb{F}_{\mathfrak{p}_i})$$

$$=$$

$$\mathcal{X}(\mathcal{O}_K) \subseteq \prod_i \mathcal{X}(\mathcal{O}_{K,\mathfrak{p}_i}) \to \prod_i \mathcal{X}(\mathbb{F}_{\mathfrak{p}_i})$$

Summary over number fields

- Parametrization of a "multiresidue" disk now takes the form:

$$
\begin{array}{ccccccccc}
 & & \mathcal{J}(\mathcal{O}_K)_0 \times \mathcal{O}_{K,\mathrm{tf}}^{\times,\rho-1} & \overset{\kappa_{\mathbb{Z}}}{\searrow} & \mathcal{U}(\mathcal{O}_K)_u & \longrightarrow & \mathcal{U}(\mathcal{O}_{K,p})_u & \xleftarrow{\simeq} & \mathcal{O}_{K,p} \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}_p^{r+\delta(\rho-1)} & \xrightarrow{\simeq} & (\mathcal{J}(\mathbb{Z})_0 \times \mathcal{O}_{K,\mathrm{tf}}^{\times,\rho-1}) \otimes \mathbb{Z}_p & \xrightarrow{\kappa} & \overline{\mathcal{T}(\mathcal{O}_K)_{\widetilde{j_b}(u)}} & \to & \mathcal{T}(\mathcal{O}_{K,p})_{\widetilde{j_b}(u)} & \xleftarrow{\simeq} & \mathcal{O}_{K,p}^{g+\rho-1}
\end{array}
$$

- $\mathcal{O}_{K,p} = \prod_i \mathcal{O}_{K,\mathfrak{p}_i}$; by a restriction of scalars procedure, or when p splits completely, may view $\mathcal{O}_{K,p} \simeq \mathbb{Z}_p^d$, then κ becomes

$$\kappa : \mathbb{Z}_p^{r+\delta(\rho-1)} \longrightarrow \mathbb{Z}_p^{d(g+\rho-1)}$$

Main result, Chabauty condition

Theorem (Č., Lilienfeldt, Xiao, Yao)

Given a choice of "multiresidue" disks, there is an explicitely computable $\mathbb{F}_p$-algebra $\overline{A}$ such that, assuming $\overline{A}$ is finite,

$$|\mathcal{U}(\mathcal{O}_K)_u| \leq \dim_{\mathbb{F}_p} \overline{A}.$$

- Method expected to work when $r + \delta(\rho - 1) \leq d(g + \rho - 2)$, equivalently

$$r \leq (g-1)d + (\rho - 1)(r_2 + 1)$$

- agrees with [BBBM] (quadratic Chabauty $/K$, hyperelliptic curves) when $\rho = 2$
- Over $\mathbb{Q}$, this gives $r \leq g + \rho - 2$ - same as [EL], [BD]
- Siksek (linear Chabauty $/K$): condition $r \leq (g-1)d$

Todo list (work in progress)

Question

What is a reasonable sufficient condition for the intersection $\overline{\mathcal{T}(\mathcal{O}_K)} \cap \mathcal{U}(\mathcal{O}_{K,p})$ to be finite?

- in the $K = \mathbb{Q}$ case, assuming the quadratic Chabauty condition $r \leq g + \rho - 2$ is enough (Edixhoven–Lido 2020)
- not expected to hold over K

Question

Assuming that $\overline{\mathcal{T}(\mathcal{O}_K)} \cap \mathcal{U}(\mathcal{O}_{K,p})$ is finite, does a suitable choice of a prime p lead to all the rings $\overline{A}$ being finite?

- **Examples!**
  - reprove some already done examples, e.g. [BBBM]
  - Bring's curve:

$$\begin{aligned} v + w + x + y + z &= 0, \\ v^2 + w^2 + x^2 + y^2 + z^2 &= 0, \\ v^3 + w^3 + x^3 + y^3 + z^3 &= 0 \end{aligned}$$

Thank you!