Chabauty–Kim Theory: Retrospectives and prospects

12th July 2024, Mordell +100 conference

Alexander Betts, Harvard University

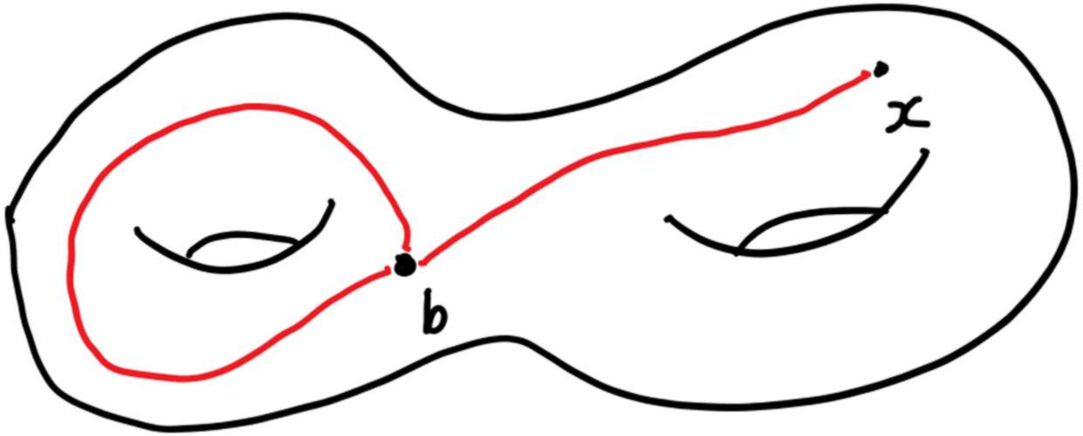
What is the Chabauty–Kim method?

A technique for studying rational points on curves using fundamental groups (Kim 2005)

What is the Chabauty–Kim method?

$X/\mathbb{Q}$ a smooth projective curve of genus ≥ 2, $b \in X(\mathbb{Q})$.

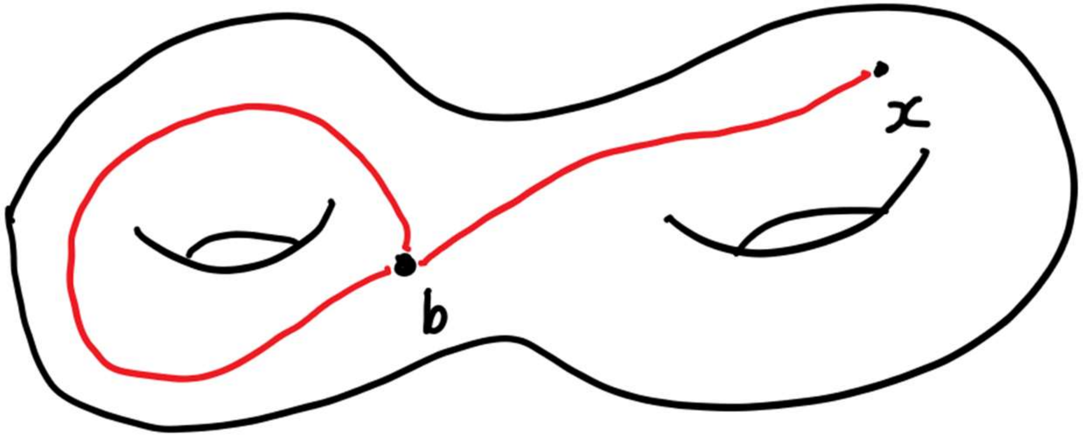
$G_{\mathbb{Q}}$ acts on $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)$, and $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b, x)$ for every $x \in X(\mathbb{Q})$.



What is the Chabauty–Kim method?

For $x \in X(\mathbb{Q}_p)$, G_p acts on $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}_p}; b, x)$.

When does this G_p-action look like the restriction of a $G_{\mathbb{Q}}$-action?



it does if $x \in X(\mathbb{Q})$

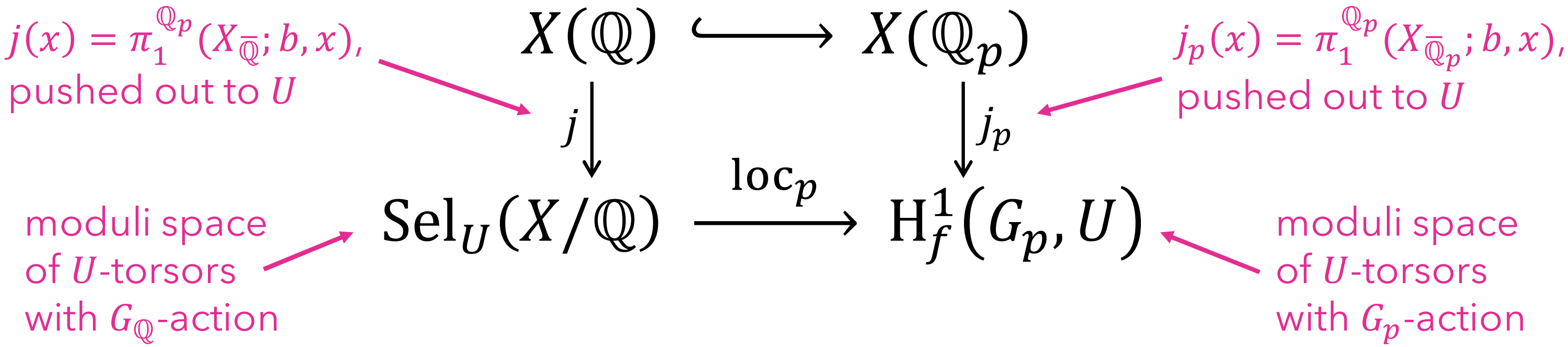
by studying when the action looks global, we hope to study $X(\mathbb{Q})$

Quotients of the fundamental group

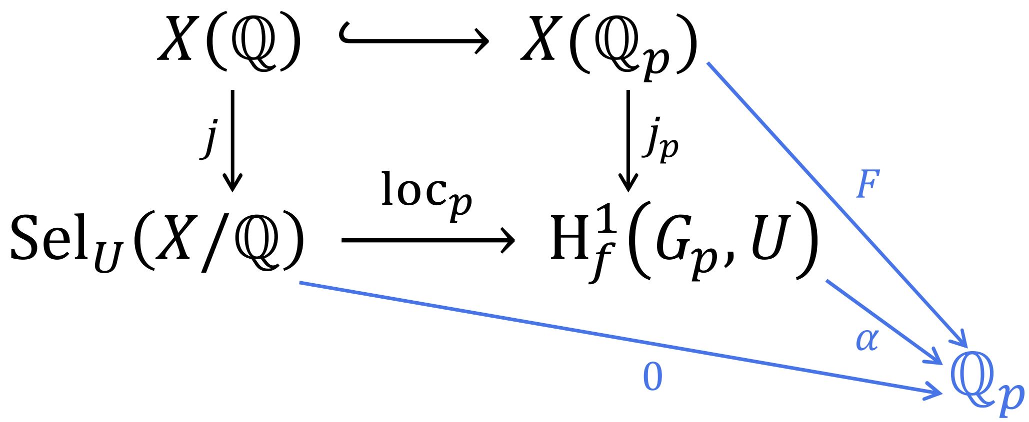
U a quotient of $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)$

- $U_1 = \pi_1^{\mathbb{Q}_p}\left(X_{\overline{\mathbb{Q}}}; b\right)^{\mathrm{ab}} = V_p J$
- $U_2 = \pi_1^{\mathbb{Q}_p}\left(X_{\overline{\mathbb{Q}}}; b\right)/\Gamma^3$ central extension of $V_p J$ by $\Lambda^2 V_p J / \mathbb{Q}_p(1)$
- $U_n = \pi_1^{\mathbb{Q}_p}\left(X_{\overline{\mathbb{Q}}}; b\right)/\Gamma^{n+1}$
- $\Lambda^2 V_p J$ contains $\rho = \mathrm{rk}(\mathrm{NS}(J)(\mathbb{Q}))$ copies of $\mathbb{Q}_p(1)$:
  push out U_2 to get U_{QC}, a central extension of $V_p J$ by $\mathbb{Q}_p(1)^{\rho-1}$

Chabauty–Kim functions



Chabauty–Kim functions



$F: X(\mathbb{Q}_p) \to \mathbb{Q}_p$ is an analytic function which vanishes on $X(\mathbb{Q})$.
We call F a *Chabauty–Kim function*.

Upshot

Chabauty–Kim theory takes as input a quotient U of $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)$ and defines a class of *Chabauty–Kim functions*, which are analytic functions

$$F: X(\mathbb{Q}_p) \to \mathbb{Q}_p$$

vanishing on $X(\mathbb{Q})$.

We study $X(\mathbb{Q})$ using Chabauty–Kim functions.

Theme 1:
Cases of Siegel–Faltings

Non-zero analytic functions have only finitely many zeroes.

$\Rightarrow$ As soon as we have a non-zero Chabauty–Kim function, we know that $X(\mathbb{Q})$ is finite.

Finiteness via Chabauty–Kim

Theorem: If
$$\dim \mathrm{Sel}_U(X/\mathbb{Q}) < \dim \mathrm{H}^1_f(G_p, U),$$
then $X(\mathbb{Q})$ is finite.

Finiteness via Chabauty–Kim

Theorem: If

$$\dim \mathrm{Sel}_U(X/\mathbb{Q}) < \dim \mathrm{H}^1_f(G_p, U),$$

then $X(\mathbb{Q})$ is finite.

Example: $U = U_1 = V_p J$:

- $\mathrm{Sel}_1(X/\mathbb{Q}_p) = \mathbb{Q}_p \otimes J(\mathbb{Q})$ has dimension $r = \mathrm{rk}(J(\mathbb{Q}))$
- $\mathrm{H}^1_f(G_p, U_1) = \mathrm{Lie}(J_{\mathbb{Q}_p})$ has dimension g
- $\Rightarrow$ if $r < g$, then $X(\mathbb{Q})$ is finite (Chabauty 1941)

Finiteness via Chabauty–Kim

Theorem: If
$$\dim \mathrm{Sel}_U(X/\mathbb{Q}) < \dim \mathrm{H}^1_f(G_p, U),$$
then $X(\mathbb{Q})$ is finite.

Example: $U = U_{\mathrm{QC}}$:

- $\mathrm{Sel}_{\mathrm{QC}}(X/\mathbb{Q}_p)$ has dimension r again
- $\mathrm{H}^1_f(G_p, U_{\mathrm{QC}})$ has dimension $g + \rho - 1$
- $\Rightarrow$ if $r < g + \rho - 1$, then $X(\mathbb{Q})$ is finite (Balakrishnan–Dogra 2018, Dogra–Le Fourn 2020)

More curves?

Need to use U_n for $n \gg 0$.

Main difficulty: computing $\dim \mathrm{Sel}_U(X/\mathbb{Q})$ is hard.

More curves?

- $X = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0,1,\infty\}$ (Kim 2005)
- $X = E \setminus \{\infty\}$ for E a CM elliptic curve (Kim 2010)
- X whose Jacobian is a product of CM abelian varieties (Coates–Kim 2010)
- X a solvable ramified cover of $\mathbb{P}^1_{\mathbb{Q}}$ (Ellenberg–Hast 2021)
- Assuming Fontaine–Mazur, any X (Kim 2009)

dimension bound on $\mathrm{Sel}_U(X/\mathbb{Z}_S)$ from Soulé

dimension bound on $\mathrm{Sel}_U(X/\mathbb{Q})$ from Iwasawa theory

bootstrap from Coates–Kim

Theme 2:
Computing rational points

In many cases, Chabauty–Kim functions can be computed explicitly.

Procedure:

1. Determine the ``shape'' of $F = \sum_{i=1}^{m} \lambda_i F_i$.
2. Use the fact that F must vanish on some known rational points to determine the λ_i.
3. For each $\mathbb{Q}_p$-point where F vanishes, either recognise it as rational, or show it is irrational by sieving.

Example: Chabauty–Coleman

$U = U_1 = V_p J,\ r < g$

1. $F(x) = \int_b^x \omega = \sum_{i=1}^{g} \lambda_i \int_b^x \omega_i$, with (ω_i) a basis of $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega_X^1)$.
2. Have $\int_D \omega = 0$ for all $D \in J(\mathbb{Q})$, so can determine λ_i.
3. Compute zero set of F, sieve out irrational points using Mordell–Weil sieve.

Example: modular curves

Mazur's Program B: classify all possible mod ℓ Galois images of non-CM elliptic curves.

$\Leftrightarrow$ which modular curves have non-cuspidal, non-CM rational points?

Example: modular curves

If the image is not all of $\mathrm{GL}_2(\mathbb{F}_\ell)$, then it is contained in either:

- the Borel subgroup
  only for $\ell = 2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163$ (Mazur 1978)
- the normaliser of a split Cartan subgroup
  only for $\ell = 2, 3, 5, 7$ and maybe 13 (Bilu–Parent–Rebolledo 2013)
- the normaliser of a non-split Cartan subgroup
  very mysterious!
- an exceptional group $\mathbb{F}_\ell^\times \rtimes S_4$, $\mathbb{F}_\ell^\times \rtimes A_4$, $\mathbb{F}_\ell^\times \rtimes A_5$
  only for $\ell = 5, 13$ (Serre 1972)

Example: modular curves

Theorem (Balakrishnan–Dogra–Müller–Tuitman–Vonk 2019):

There is no non-CM elliptic curve over $\mathbb{Q}$ whose mod 13 Galois image is contained in the normaliser of a split Cartan subgroup, or of a non-split Cartan subgroup.

$X_s(13)(\mathbb{Q}) \cong X_{ns}(13)(\mathbb{Q})$ consists only of cusps and CM points.

$X_{ns}(17)(\mathbb{Q})$ was computed by the same authors in 2023.

Example: Atkin–Lehner quotients

$X_0^+(N) = X_0(N)/\langle w_N \rangle$ parametrises pairs of elliptic curves with a cyclic N-isogeny.

Galbraith's Conjecture: the only values of N with $2 \leq g_0^+(N) \leq 5$ for which $X_0^+(N)$ has a non-cuspidal, non-CM rational point are

$$N = 73, 91, 103, 125, 137, 191, 311.$$

Example: Atkin–Lehner quotients

Galbraith, Momose, Arai–Momose showed this for all N except

$$67, 73^*, 91^*, 103^*, 107, 125^*, 167, 191^*$$
$$97, 109, 113, 127, 169$$
$$137^*, 173, 199, 251, 311^*$$
$$157, 181, 227, 263$$

- Balakrishnan–Dogra–Müller–Tuitman–Vonk 2019
- Balakrishnan–Besser–Bianchi–Müller 2021
- Balakrishan–Best–Bianchi–Lawrence–Müller–Triantafillou–Vonk 2021
- Balakrishnan–Dogra–Müller–Tuitman–Vonk 2023
- Adžaga–Arul–Beneish–Chen–Chidambaram–Keller–Wen 2023
- Arul–Müller 2023

$\Rightarrow$ Galbraith's Conjecture is true

Other examples

- All rank 2 genus 2 bielliptic curves in the LMFDB (Bianchi–Padurariu, 2024)
- Maximal Atkin–Lehner quotients $X_0^*(N) = X_0(N)/\langle (w_d)_{d|N} \rangle$ which are hyperelliptic (Bars–González–Xarles 2021, Adžaga–Chidambaram–Keller–Padurariu 2022)
- All Atkin–Lehner quotients of geometrically hyperelliptic Shimura curves (Padurariu–Schembri, 2023)
- $\mathbb{Z}_S$-integral points on $\mathbb{P}^1 \setminus \{0,1,\infty\}$ for $S = \{2\}$ (Dan-Cohen–Wewers 2015), $S = \{3\}$ (Dan-Cohen–Corwin), $S = \{2, q\}$ (Best–B.–McAndrew–Kumpitsch–Lüdtke–Qian–Studnia–Xu)

Theme 3:
Applications to uniformity

Knowing the shape of a Chabauty–Kim function F can allow one to bound the number of zeroes, and hence $\#X(\mathbb{Q})$, even without determining F directly.

The Coleman bound

Theorem (Coleman 1985):

Suppose that $r < g$. Let $p > 2g$ be a prime of good reduction for X. Then

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

$2r$ (Stoll 2002)

For $r \leq g - 3$, the bound can be made completely uniform (Stoll 2013, Katz–Rabinoff–Zureick-Brown 2016)

$$\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28$$

Bounds from quadratic Chabauty

Theorem (Balakrishnan–Dogra 2019):

Suppose that $r = g$, $\rho > 1$, that X has everywhere potentially good reduction, and $p \geq 3$ is a prime of good reduction. Then

$$\#X(\mathbb{Q}) \leq \left(1 + \frac{p-1}{(p-2)\log p}\right)(16g^3 + 15g^2 - 16g + 10)\#X(\mathbb{F}_p).$$

generalised by Müller–Leonhardt–Lüdtke

Bounds from higher Chabauty

Theorem (B. 2023):

One can attach Hilbert series to $\mathrm{Sel}_U(X/\mathbb{Q})$ and $\mathrm{H}^1_f(G_p, U)$, and prove a theorem of the kind

``global < local'' bound on Hilbert series

$\Rightarrow$ explicit bound on $\#X(\mathbb{Q})$

e.g. for $X = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0,1,\infty\}$, we have $\#X(\mathbb{Z}_S) \leq 8 \times 6^{\#S} \times 2^{4^{\#S}}$

$\#X(\mathbb{Z}_S) \leq 3 \times 7^{2\#S+3}$
(Evertse 1984)

Bounds from higher Chabauty

Theorem (B. 2023):

One can attach Hilbert series to $\mathrm{Sel}_U(X/\mathbb{Q})$ and $\mathrm{H}^1_f(G_p, U)$, and prove a theorem of the kind

``global < local'' bound on Hilbert series

$\Rightarrow$ explicit bound on $\#X(\mathbb{Q})$

e.g. assuming Fontaine–Mazur, we have $\#X(\mathbb{Q}) \leq B(g, r, \mathrm{redn})$ (B.–Corwin–Leonhardt 2024)

Theme 4:
Motivic and geometric aspects

Motivic fundamental groups

According to Deligne, we expect $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)$ to be the p-adic étale realisation of a ``motivic fundamental group''.

$\Rightarrow \mathrm{Sel}_U(X/\mathbb{Q})$ has a $\mathbb{Q}$-structure, independent of p.

For $X = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0,1,\infty\}$, $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)$ is the realisation of a mixed Tate motivic fundamental group (Deligne–Goncharov 2005).

Dan-Cohen–Wewers (2015, 2016) and Dan-Cohen–Corwin gave the $\mathbb{Q}$-structure on $\mathrm{Sel}_U(X/\mathbb{Q})$ and determined its geometry.

Geometric quadratic Chabauty

For $U = U_1$, $\mathrm{Sel}_1(X/\mathbb{Q}) = \mathbb{Q}_p \otimes J(\mathbb{Q})$ has a $\mathbb{Q}$-structure.

There is also a $\mathbb{Q}$-structure for $U = U_{\mathrm{QC}}$, coming from integral points on a $\mathbb{G}_m^{\rho-1}$-torsor on J (Edixhoven–Lido 2021).

Leads to a geometric approach to quadratic Chabauty, at least as strong as usual quadratic Chabauty, and sometimes stronger (Duque-Rosero–Hashimoto–Spelier 2023).

Theme 5:

Number fields, unlikely intersections

One can also use Chabauty–Kim to study rational points over number fields K.

Main difficulty: Chabauty–Kim functions are $\mathbb{Q}_p$-analytic functions on $\prod_{v|p} X(K_v)$, which has dimension $d = [K: \mathbb{Q}]$ as a $\mathbb{Q}_p$-analytic manifold.

Naïve guess:

If $\dim \mathrm{Sel}_U(X/K) \leq \sum_{v|p} \dim \mathrm{H}^1_f(G_v, U) - d$, then the common vanishing locus of Chabauty–Kim functions is finite.

e.g. if $r \leq (g-1)d$, then is the vanishing locus of the integrals coming from Chabauty–Coleman finite? (~Siksek 2013)

counterexample by Dogra (2023)

Number fields: known results

- Finiteness theorems for $\mathbb{P}^1_{\mathcal{O}_{K,S}} \setminus \{0,1,\infty\}$, curves with CM Jacobians, … (Hast 2021, Dogra 2023)
- $\mathbb{Z}[\phi]$-integral points on $y^2 + y = x^3 + \phi^2 x + \phi x$ (Balakrishnan–Besser–Bianchi–Müller 2021)
- $\mathbb{Q}(\sqrt{34})$-rational points on $y^2 = x^6 + x^2 + 1$ (BBBM 2021)
- $\mathbb{Z}[\zeta_3]$-integral points on $y^2 = x^3 - 4$ (Bianchi 2020)
- $\mathbb{Z}[\zeta_3]$-integral points on $y^2 + (\zeta_3 + 2)y = x^3 - (\zeta_3 + 2)x^2 - \zeta_3^2 x$ (Jha 2024)

Some speculative questions

Other p-adic methods

Other methods such as Lawrence–Venkatesh are of a similar flavour to Chabauty–Kim.

- More successful in proving Siegel–Faltings finiteness.
- Less successful in explicit computations.

Can we produce a common generalisation of both methods?
Can we use it to compute rational points in new cases?

Initial work by Noam Kantor.

A Chabauty–Kim algorithm

One might dream of developing an algorithm for computing rational points, where:

1. If the algorithm terminates for a curve X, it computes $X(\mathbb{Q})$ provably correctly.
2. Assuming some reasonable conjectures, the algorithm always terminates.
3. The algorithm actually terminates in practice for many X.

Can Chabauty–Kim provide such an algorithm?

needs Chabauty–Kim for large quotients U, and without needing rational points on X

Equation-free Chabauty–Kim

Current quadratic Chabauty computations for modular curves use `QCModAffine`, which needs explicit equations for affine patches.

Can we compute rational points on modular curves using the moduli interpretation instead of explicit equations?

Some work in progress by Ellenberg–Hashimoto–Wen, and Huang–Lau–Xu from different perspectives.

Thanks for listening!