Refined Chabauty–Kim for the thrice-punctured line

Martin Lüdtke

Rijksuniversiteit Groningen / MPIM Bonn

MPIM Number Theory Lunch Seminar
23 April 2025

$X/\mathbb{Q}$ smooth projective curve of genus $g \geq 2$

Mordell Conjecture (1922)

$\#X(\mathbb{Q}) < \infty$

- ▶ Chabauty (1941): proved finiteness if $r := \operatorname{rk} \operatorname{Jac}_X(\mathbb{Q}) < g$
- ▶ Faltings (1983): proved Mordell in general

Open problem: How to determine $X(\mathbb{Q})$ in practice?

Can use computer search to list points in $X(\mathbb{Q})$ but how do we know we found them all?

Chabauty's proof can be made effective but the condition $r < g$ is not always satisfied

The cursed curve

Example: $X_s(13)$ – the split Cartan modular curve of level 13 a.k.a. the cursed curve

$$y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$$

It has rational points

$$(0,0), \quad (0,2), \quad (1,1), \quad \left(\tfrac{1}{2}, \tfrac{1}{2}\right), \quad \left(-\tfrac{3}{2}, \tfrac{3}{2}\right)$$
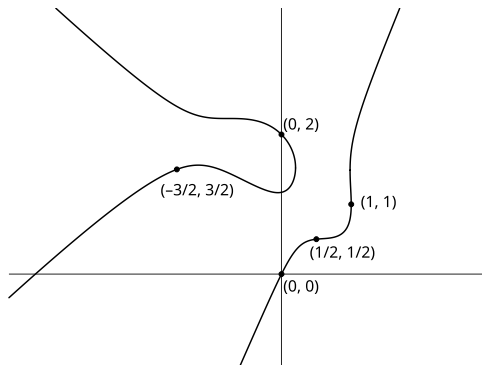
but how do we know there are no others? This question comes up in a uniformity question of Serre from 1972 about residual Galois representations of elliptic curves.

Chabauty does not apply since $r = g = 3$.

Idea: develop "non-abelian" generalisation of Chabauty

▶ Kim (2005): Chabauty–Kim method (aka non-abelian Chabauty)

The Chabauty–Kim method

For p a prime of good reduction, try to locate $X(\mathbb{Q})$ inside $X(\mathbb{Q}_p)$. Kim constructs a descending sequence of subsets

$$X(\mathbb{Q}_p) \supseteq X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \dots$$

all containing $X(\mathbb{Q})$. The set $X(\mathbb{Q}_p)_n$ is called the Chabauty–Kim locus of depth n.

- $X(\mathbb{Q}_p)_n$ is cut out inside $X(\mathbb{Q}_p)$ by p-adic analytic functions
  (more precisely: iterated Coleman integrals)
  $\Rightarrow X(\mathbb{Q}_p)_n$ finite or all of $X(\mathbb{Q}_p)$
- $X(\mathbb{Q}_p)_1$ is finite if $r < g$ (Chabauty)
- $X(\mathbb{Q}_p)_2$ is finite if $r < g + \rho - 1$, where $\rho := \operatorname{rk} \operatorname{NS}(\operatorname{Jac}_X)$ ("Quadratic Chabauty")
- Bloch–Kato or Fontaine–Mazur conjecture $\Rightarrow \#X(\mathbb{Q}_p)_n < \infty$ for $n \gg 0$

Kim's Conjecture

Kim's Conjecture

$X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$.

- ▶ Practical relevance: if true, can try to compute $X(\mathbb{Q})$ by computing $X(\mathbb{Q}_p)_n$ for $n = 1, 2, \dots$
- ▶ Theoretical relevance: Kim's Conjecture implies local-to-global principle for Grothendieck's Section Conjecture (Betts–Kumpitsch–L.)

Computing $X(\mathbb{Q}_p)_n$ is hard!

Photo credit: Jan Vonk

Construction of Chabauty–Kim loci

- Fix rational basepoint $b \in X(\mathbb{Q})$
- $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b) :=$ étale fundamental group of $X_{\overline{\mathbb{Q}}}$
- $U_X :=$ its $\mathbb{Q}_p$-prounipotent completion $= \text{``}\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b) \otimes_{\hat{\mathbb{Z}}} \mathbb{Q}_p\text{''}$
- $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $(X_{\overline{\mathbb{Q}}}, b)$, hence on U_X.

Let $U_X \twoheadrightarrow U$ be a $G_{\mathbb{Q}}$-equivariant quotient. We have the Chabauty–Kim diagram

$$
\begin{array}{ccc}
X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) \\
\downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j_p} \\
\text{Sel}_U(X)(\mathbb{Q}_p) & \xrightarrow{\text{loc}_p} & \text{H}^1_f(G_p, U)(\mathbb{Q}_p)
\end{array}
$$

$\text{Sel}_U(X)$ and $\text{H}^1_f(G_p, U)$ are affine $\mathbb{Q}_p$-schemes, the global and local Selmer scheme. They are moduli spaces for U-torsors with $G_{\mathbb{Q}}$- resp. $G_{\mathbb{Q}_p}$-action, and the vertical maps are constructed by taking path torsors: $x \mapsto \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}; b, x)$.

$$X(\mathbb{Q}) \longleftrightarrow X(\mathbb{Q}_p)$$

$$\downarrow j \qquad\qquad \downarrow j_p$$

$$\mathsf{Sel}_U(X)(\mathbb{Q}_p) \xrightarrow{\ \mathsf{loc}_p\ } \mathsf{H}^1_f(G_p, U)(\mathbb{Q}_p)$$

Fact: loc_p is an algebraic map of affine $\mathbb{Q}_p$-schemes

Strategy:

- show that loc_p is not dominant (e.g., for dimension reasons)
- find $0 \neq f\colon \mathsf{H}^1_f(G_p, U) \to \mathbb{A}^1$ vanishing on $\mathsf{im}(\mathsf{loc}_p)$
- the pullback $f \circ j_p\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ is a nonzero p-adic analytic function whose vanishing set is finite and contains $X(\mathbb{Q})$

Definition

The Chabauty–Kim locus associated to U is the set

$$X(\mathbb{Q}_p)_U := \{x \in X(\mathbb{Q}_p) \,:\, j_p(x) \in \mathrm{im}(\mathrm{loc}_p)\}$$
$$= \bigcap_{f \text{ as above}} V(f \circ j_p) \subseteq X(\mathbb{Q}_p).$$

Commutativity of the Chabauty–Kim diagram implies

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_U \subseteq X(\mathbb{Q}_p).$$

If $U = U_{X,n}$ is the n-th lower central series quotient of U_X, we write $X(\mathbb{Q}_p)_n$ for the associated "depth n" Chabauty–Kim locus.

$$\Rightarrow X(\mathbb{Q}_p) \supseteq X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$$

Quadratic Chabauty

▶ Quadratic Chabauty (Balakrishnan, Dogra,...) uses a certain intermediate quotient $U_{X,2} \twoheadrightarrow U_{QC} \twoheadrightarrow U_{X,1}$ to construct a subset

$$X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_{QC} \supseteq X(\mathbb{Q}_p)_2.$$

It can be described using p-adic heights and is finite whenever $r < g + \rho - 1$, where $\rho := \text{rk NS}(\text{Jac}_X)$. Very few results beyond that.

▶ Quadratic Chabauty broke the curse of the cursed curve:

$$X(\mathbb{Q}_{17})_{QC} = X(\mathbb{Q})$$

(Balakrishnan, Dogra, Müller, Tuitman, Vonk 2019)
→ Quanta article: "Mathematicians Crack the Cursed Curve" ⌐

We would like to have an algorithm for computing $X(\mathbb{Q}_p)_n$ for larger n.

The thrice-punctured line

Today: compute some (refined) Chabauty–Kim loci in the best-understood example

$$\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}.$$

Setting:
- S: finite set of primes
- $\mathbb{Z}_S = \mathcal{O}(\mathrm{Spec}(\mathbb{Z}) \smallsetminus S) = \mathbb{Z}[\frac{1}{\ell} : \ell \in S]$: ring of S-integers
- $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$: thrice-punctured line over $\mathbb{Z}_S$

We are interested in the S-integral points $X(\mathbb{Z}_S)$. *S-unit equation*:

$$x + y = 1 \quad \text{with } x, y \in \mathbb{Z}_S^\times$$

Solutions are $x \in \mathbb{Q}$ s.t. x and $1 - x$ are of the form $\pm \prod_{\ell \in S} \ell^{e_\ell}$ with $e_\ell \in \mathbb{Z}$.

Theorem (Siegel–Mahler, 1933)

$X(\mathbb{Z}_S)$ *is finite.*

- Example $S = \emptyset$:
$$X(\mathbb{Z}) = \emptyset$$

- Example $S = \{2\}$:
$$X(\mathbb{Z}[1/2]) = \left\{ 2, -1, \frac{1}{2} \right\}$$

- Example $S = \{2, 3\}$:
$$X(\mathbb{Z}[1/6]) = \left\{ 2, -1, \frac{1}{2}, 3, -2, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, -\frac{1}{2}, -3, 4, -\frac{1}{3}, \frac{4}{3}, \frac{3}{4}, \frac{1}{4}, 9, -8, \frac{1}{9}, \frac{8}{9}, \frac{9}{8}, -\frac{1}{8} \right\}$$

(Levi ben Gershon 1342, *The Harmony of Numbers*)

Some small sets S

- Example $S = \{2, q\}$, $q = 2^n + 1 > 3$ Fermat prime:

$$X(\mathbb{Z}[1/2q]) = \left\{ 2, -1, \frac{1}{2}, q, 1 - q, \frac{1}{q}, \frac{q-1}{q}, \frac{q}{q-1}, \frac{1}{1-q} \right\}$$

- Example $S = \{2, q\}$, $q = 2^n - 1 > 3$ Mersenne prime:

$$X(\mathbb{Z}[1/2q]) = \left\{ 2, -1, \frac{1}{2}, -q, q + 1, -\frac{1}{q}, \frac{q+1}{q}, \frac{q}{q+1}, \frac{1}{q+1} \right\}$$

- Example $S = \{2, q\}$, $q = 2^n - 1$ not Fermat or Mersenne:

$$X(\mathbb{Z}[1/2q]) = X(\mathbb{Z}[1/2]) = \left\{ 2, -1, \frac{1}{2} \right\}$$

Let $p \notin S$, so that $X(\mathbb{Z}_S) \subseteq X(\mathbb{Z}_p)$. Have Chabauty–Kim loci

$$X(\mathbb{Z}_p) \supseteq X(\mathbb{Z}_p)_{S,1} \supseteq X(\mathbb{Z}_p)_{S,2} \supseteq \ldots$$

all containing $X(\mathbb{Z}_S)$, as in the projective higher genus case.

Theorem (Kim, 2005)

$\#X(\mathbb{Z}_p)_{S,n} < \infty$ for $n \gg 0$

Kim's Conjecture

$X(\mathbb{Z}_p)_{S,n} = X(\mathbb{Z}_S)$ for $n \gg 0$

Known cases:

- $S = \emptyset$, $n = 2$, $p < 10^5$ (Balakrishnan, Dan-Cohen, Kim, Wewers, 2018)
- $S = \emptyset$, $n = \max(1, p - 3)$, p arbitrary (Betts, Kumpitsch, L., 2023)
- $S = \{2\}$, $n = 4$, $3 \le p \le 29$ (Dan-Cohen, Wewers, 2016)
- $S = \{3\}$, $n = 4$, $p \in \{5, 7\}$ (Corwin, Dan-Cohen, 2020)

Partial results for $S = \{2, 3\}$, $n = 6$ (Jarossay, Lilienfeldt, Saettone, Weiss, Zehavi, 2024)

Most of these results use a motivic variant of Chabauty–Kim method, using torsors under the "motivic fundamental group" rather than its étale realisation

Refined Chabauty–Kim

Betts–Dogra (2020): refined Chabauty–Kim loci

$$X(\mathbb{Z}_p) \supseteq X(\mathbb{Z}_p)_{S,1}^{\min} \supseteq X(\mathbb{Z}_p)_{S,2}^{\min} \supseteq \ldots$$

Idea: partition S-integral points by their reductions modulo primes $\ell \in S$

$$\mathrm{red}_\ell \colon X(\mathbb{Z}_S) \subseteq \mathbb{P}^1(\mathbb{Z}_S) = \mathbb{P}^1(\mathbb{Z}) \twoheadrightarrow \mathbb{P}^1(\mathbb{F}_\ell)$$

Refined Kim's Conjecture

$X(\mathbb{Z}_p)_{S,n}^{\min} = X(\mathbb{Z}_S)$ for $n \gg 0$

proved for $S = \{2\}$ and all odd p in depth $\max(1, p - 3)$ (Betts–Kumpitsch–L., 2023)
proved for $S = \{2, q\}$ and $p = 3$ in depth 2 when $q = 2^n \pm 1 > 3$ Fermat or Mersenne
(Best–Betts–Kumpitsch–L.–McAndrew–Qian–Studnia–Xu, 2024)
case $S = \{2, 3\}$: depth 2 does not suffice $\to$ go to depth 4 (later)

Depth 2 loci

Let $S = \{2, q\}$ for some odd prime q. Focus on

$$X(\mathbb{Z}_S)_{(1,0)} := \{x \in X(\mathbb{Z}_S) : \mathrm{red}_2(x) \in X \cup \{1\}, \ \mathrm{red}_q(x) \in X \cup \{0\}\}$$

and associated refined Chabauty–Kim loci $X(\mathbb{Z}_p)_{S,n}^{(1,0)}$.

Theorem (BBKLMQSX, 2024)

The depth 2 locus $X(\mathbb{Z}_p)_{\{2,q\},2}^{(1,0)}$ is defined inside $X(\mathbb{Z}_p)$ by

$$\mathrm{Li}_2(z) - a \log(z) \, \mathrm{Li}_1(z) = 0$$

for some computable p-adic constant $a = a(q) \in \mathbb{Q}_p$.

Here, log is the *p*-adic logarithm and Li_m is the *p-adic polylogarithm*

$$\mathrm{Li}_m(z) = \int_0^z \frac{\mathrm{d}x}{x} \cdots \frac{\mathrm{d}x}{x} \frac{\mathrm{d}x}{1-x} \qquad (\textit{m-fold iterated integral})$$

Computing depth 2 loci

L. (2024): Sage code for computing $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ for arbitrary p and q

  $\rightarrow$ https://github.com/martinluedtke/RefinedCK

Example: $S = \{2,3\}$, $p = 5$. Have $X(\mathbb{Z}[1/6])_{(1,0)} = \{-3, -1, 3, 9\}$.

```
p = 5; q = 3
a = -Qp(p)(3).polylog(2)
CK_depth_2_locus(p,q,10,a)
```

Output:

```
[2 + O(5^9),
 2 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + O(5^9),
 3 + O(5^6),
 3 + 5^2 + 2*5^3 + 5^4 + 3*5^5 + O(5^6),
 4 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + O(5^9),
 4 + 5 + O(5^9)]
```

How does the size of $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$ vary with the choice of auxiliary prime p?

p	5	7	11	13	17	19	23	29	31	...	1091	1093	1097	...
$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$	6	8	18	16	22	20	20	26	36	...	1076	2154	1078	...

Observations:

▶ size always seems to be even

▶ 0 or 2 points in each residue disc

▶ almost always of size $\approx p$, but for $p \in \{1093, 3511\}$ of size $\approx 2p$

Can explain this. Related to 1093 and 3511 being (the only known) Wieferich primes, i.e., primes with $2^{p-1} \equiv 1 \bmod p^2$.

Similar observations for $S = \{2, q\}$ with q different from 3.

$$\boxed{\mathrm{Li}_2(z) - a(q)\log(z)\,\mathrm{Li}_1(z) = 0}$$

How to compute the zero locus in $X(\mathbb{Z}_p)$?

1. Compute the p-adic constant $a(q)$ using modified algorithm of Dan-Cohen–Wewers
   $\to$ https://github.com/martinluedtke/dcw_coefficients

2. Compute power series for polylogarithms on residue discs around roots of unity ζ

$$\mathrm{Li}_m(\zeta + pt) = \sum_{k=1}^{\infty} a_{m,k} t^k$$

   $\to$ Besser–de Jeu's "Li$^{(p)}$-service" paper

3. Implemented Hensel's Lemma for finding roots of p-adic power series with correct precision: function `Zproots`
   $\to$ https://github.com/martinluedtke/RefinedCK

Depth 4 loci

Adapting work of Corwin and Dan-Cohen to the refined setting, we derive a new function for the refined depth 4 locus in the case $S = \{2, 3\}$:

Theorem (L. 2024)

Let $S = \{2, 3\}$ and $p \notin S$. Any point z in the refined Chabauty–Kim locus $X(\mathbb{Z}_p)_{\{2,3\},4}^{(1,0)}$ satisfies, in addition to the depth 2 equation, the equation

$$\det \begin{pmatrix} \mathrm{Li}_4(z) & \log(z)\,\mathrm{Li}_3(z) & \log(z)^3\,\mathrm{Li}_1(z) \\ \mathrm{Li}_4(3) & \log(3)\,\mathrm{Li}_3(3) & \log(3)^3\,\mathrm{Li}_1(3) \\ \mathrm{Li}_4(9) & \log(9)\,\mathrm{Li}_3(9) & \log(9)^3\,\mathrm{Li}_1(9) \end{pmatrix} = 0.$$

Also have a depth 4 equation for general $S = \{2, q\}$ but it is less explicit.

Computing depth 4 loci for $S = \{2, 3\}$

Use the new equation to compute depth 4 locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},4}$:

```
p = 5; q = 3; N = 10
coeffs = Z_one_sixth_coeffs(p,N)
CK_depth_4_locus(p,q,N,coeffs)
```

Output:

```
[2 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + O(5^9),
 3 + O(5^6),
 4 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + O(5^9),
 4 + 5 + O(5^9)]
```

This is $\{-3, 3, -1, 9\} = X(\mathbb{Z}[1/6])_{(1,0)}$, extra points are eliminated.

$\Rightarrow$ Refined Kim's Conjecture holds for $S = \{2, 3\}$ and $p = 5$

Verifying Kim's Conjecture

Compute the depth 4 locus for many other primes to obtain:

Theorem (L. 2024)

The Refined Kim's Conjecture holds for $S = \{2, 3\}$ and all primes $3 < p < 10{,}000$.

Some ongoing work

- Higher number fields.
  Work in progress with Xiang Li: $K = \mathbb{Q}(\zeta_8)$, $S = \{(1 - \zeta_8)\}$, depth 2

- Use also *multiple* polylogarithms $\mathrm{Li}_{k_1,\ldots,k_r}$.
  Work in progress with Corwin, Dan-Cohen

- Higher genus curves.
  Work in progress with Corwin, Dan-Cohen: $g = 1$, depth 3;
  Work in progress with Leonhardt: (classical) Chabauty for general affine curves

References

[BBK+24]   A. Best, L. A. Betts, T. Kumpitsch, M. Lüdtke, A. McAndrew, L. Qian, E. Studnia, and Y. Xu. "Refined Selmer equations for the thrice-punctured line in depth two". In: *Math. Comp.* 93 (2024), pp. 1497–1527.

[BD20]   L. A. Betts and N. Dogra. *The local theory of unipotent Kummer maps and refined Selmer schemes*. 2020. arXiv: 1909.05734v2 [math.NT].

[BKL23]   L. A. Betts, T. Kumpitsch, and M. Lüdtke. *Chabauty–Kim and the Section Conjecture for locally geometric sections*. 2023. arXiv: 2305.09462v1 [math.NT].

[Bro17]   F. Brown. *Integral points on curves, the unit equation, and motivic periods*. 2017. arXiv: 1704.00555v1 [math.NT].

[CD20]   D. Corwin and I. Dan-Cohen. "The polylog quotient and the Goncharov quotient in computational Chabauty–Kim theory I". In: *Int. J. Number Theory* 16 (2020), pp. 1859–1905.

[DW15]   I. Dan-Cohen and S. Wewers. "Explicit Chabauty–Kim theory for the thrice punctured line in depth 2". In: *Proc. Lond. Math. Soc.* 110.1 (2015), pp. 133–171.

[Kim05]   M. Kim. "The motivic fundamental group of $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ and the theorem of Siegel". In: *Invent. Math.* 161.3 (2005), pp. 629–656.

[Lüd25]   M. Lüdtke. "Refined Chabauty–Kim computations for the thrice-punctured line over $\mathbb{Z}[1/6]$". In: *Res. Number Theory* 11 (2025).

Thanks for listening...

Hereweg Groningen in 1906.
Source: https://www.groningerarchieven.nl

(**18**) In the summer of 1936 at Groningen in the Netherlands, when I was still working at the University there, a bicycle rider ran into me. As a consequence, the tuberculosis in my right knee bone, which had been dormant for many years, flared up again. It therefore became necessary to undergo several bone operations in 1936 and 1937. This was naturally a very painful period and I was given many morphine injections, although my doctor warned me against their danger.

After a further operation the pains and hence also the injections finally stopped. Then I tried to convince myself that the drug had not damaged my brain by studying the problem of the possible transcendency of the decimal fraction

$$D = 0.123456789101112...$$

in which the successive integers are written one after the other. I found that I could still do mathematics and succeeded in proving the transcendency of both D and of infinitely many more general decimal fractions.

From: K. Mahler, *Fifty years as a mathematician*

...and watch out for cyclists when in Groningen!