Non-abelian Chabauty for the thrice-punctured line

Martin Lüdtke

Rijksuniversiteit Groningen

Belgian-Dutch Junior Algebraic Geometry seminar
Leiden
14 October 2022

Overview

Introduction: The S-unit equation

Non-abelian Chabauty

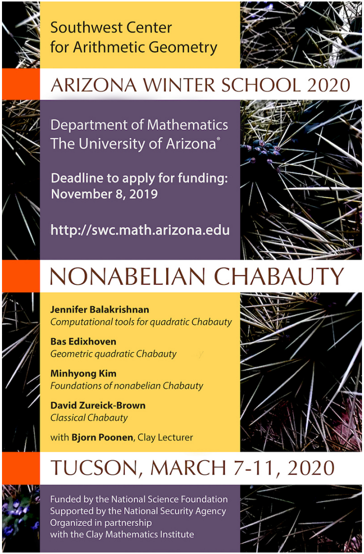
Refined non-abelian Chabauty

Selmer schemes

Chabauty–Kim for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ in depth 2

Further developments in higher depth

j/w Alex Best, *Alex Betts*, Theresa Kumpitsch, Angus McAndrew, Lie Qian, Elie Studnia, Yujie Xu



1. Introduction: The S-unit equation

The S-unit equation

Setup:

- S finite set of primes
- $\mathbb{Z}_S = \{n \in \mathbb{Q} : v_p(n) \geq 0 \ \forall p \notin S\}$ ring of S-integers
- $\mathbb{Z}_S^\times = \{n \in \mathbb{Q}^\times$ containing only prime factors in $S\}$
  $= \{\pm \prod_{\ell \in S} \ell^{e_\ell} : e_\ell \in \mathbb{Z}\}$
  group of S-units

S-unit equation

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

Solutions are S-units x such that $1 - x$ is also an S-unit.

The S-unit equation

S-unit equation

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

If x is a solution, so are $1 - x$ and $1/x$, since

$$1 - 1/x = -(1 - x)/x.$$

Thus, solutions come in S_3-orbits

$$x, \quad 1 - x, \quad \frac{1}{x}, \quad \frac{1}{1-x}, \quad \frac{x-1}{x}, \quad \frac{x}{x-1}.$$

The S-unit equation

S-unit equation

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

Solutions for small sets S:

- $S = \emptyset$: no solutions
- $S = \{\ell\}$, ℓ odd: no solutions
  $S = \{2\}$: solutions $\{2, -1, 1/2\} = S_3$-orbit of 2
- $S = \{\ell, q\}$, both odd: no solutions
  $S = \{2, q\}$
  - $q = 2^n + 1 > 3$ Fermat prime: S_3-orbits of 2 and q
  - $q = 2^n - 1 > 3$ Mersenne prime: S_3-orbits of 2 and 2^n
  - $q = 3$: S_3-orbits of $2, 3, 4, 9$
  - all other q: only the S_3-orbit of 2

The S-unit equation

Geometric re-interpretation:
Solutions of the S-unit equation are elements of $\mathcal{X}(\mathbb{Z}_S)$, where

$$\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\}.$$

Theorem (Siegel 1929)

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

The S-unit equation

Siegel's proof was not effective:

- no method to compute $\mathcal{X}(\mathbb{Z}_S)$
- no upper bound on $\#\mathcal{X}(\mathbb{Z}_S)$

Siegel's Theorem was reproved by Minhyong Kim in 2005 using a non-abelian generalisation of Chabauty's method.

2. Non-abelian Chabauty

Non-abelian Chabauty

Fix auxiliary prime $p \notin S$.

Chabauty–Kim method yields nested sequence

$$\mathcal{X}(\mathbb{Z}_p) \supseteq \mathcal{X}(\mathbb{Z}_p)_{S,1} \supseteq \mathcal{X}(\mathbb{Z}_p)_{S,2} \supseteq \dots \qquad \supseteq \mathcal{X}(\mathbb{Z}_S)$$

The $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ are zero sets of *Coleman-analytic* functions on $\mathcal{X}(\mathbb{Z}_p)$

Theorem (Kim 2005)

$\mathcal{X}(\mathbb{Z}_p)_{S,n}$ is finite for $n \gg 0$.

$\Rightarrow$ Siegel's Theorem

(This is not known for more general curves but is implied by various standard conjectures.)

Non-abelian Chabauty

Conjecture (Kim)

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

The Chabauty–Kim method can be made effective and the conjecture can be tested in some cases.

However:

- Complexity increases with n
- Larger sets S require larger *depth* n to get finiteness

Depth 1: shows finiteness only for $S = \emptyset$:

$$\begin{aligned}\mathcal{X}(\mathbb{Z}_p)_{\emptyset,1} &= \{z \in \mathcal{X}(\mathbb{Z}_p) : \log(z) = \log(1-z) = 0\} \\ &= \{\zeta_6, \zeta_6^{-1}\} \cap \mathbb{Z}_p.\end{aligned}$$

This agrees with $\mathcal{X}(\mathbb{Z}) = \emptyset$ if and only if $p \equiv 2 \bmod 3$.

Depth 2:

Theorem (Dan-Cohen, Wewers 2015)

Explicit equations defining $\mathcal{X}(\mathbb{Z}_p)_{S,2}$ for $\#S \leq 1$:

$$\mathcal{X}(\mathbb{Z}_p)_{\emptyset,2} = \{z \in \mathcal{X}(\mathbb{Z}_p) : \log(z) = \log(1-z) = \mathrm{Li}_2(z) = 0\},$$
$$\mathcal{X}(\mathbb{Z}_p)_{\{\ell\},2} = \{z \in \mathcal{X}(\mathbb{Z}_p) : 2\,\mathrm{Li}_2(z) = \log(z)\log(1-z)\}.$$

Here, $\mathrm{Li}_2(z)$ denotes the p-adic dilogarithm, i.e. the iterated Coleman integral

$$\mathrm{Li}_2(z) = \int_0^z \frac{\mathrm{d}t}{t}\frac{\mathrm{d}t}{1-t}.$$

3. Refined non-abelian Chabauty

Refined Chabauty–Kim

Betts–Dogra (2019): refinement of CK method

The refined Chabauty–Kim method yields a nested sequence

$$\mathcal{X}(\mathbb{Z}_p) \supseteq \mathcal{X}(\mathbb{Z}_p)^{\min}_{S,1} \supseteq \mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2} \supseteq \dots \qquad \supseteq \mathcal{X}(\mathbb{Z}_S)$$

with

$$\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,n} \subseteq \mathcal{X}(\mathbb{Z}_p)_{S,n}.$$

- $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,n}$ may be finite even if $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ is not
- $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,n}$ may agree with $\mathcal{X}(\mathbb{Z}_S)$ even if $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ does not

Conjecture (Refined Kim conjecture)

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

Refined Chabauty–Kim

Remark

Refined CK detects local obstructions: If $\mathcal{X}(\mathbb{Z}_\ell) = \emptyset$ for some $\ell \notin S$ or $\mathcal{X}(\mathbb{Q}_\ell) = \emptyset$ for some $\ell \in S$, then $\mathcal{X}(\mathbb{Z}_p)_{S,n}^{\min} = \emptyset = \mathcal{X}(\mathbb{Z}_S)$ automatically.

In particular, for $\mathcal{X} = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$:

$$\mathcal{X}(\mathbb{Z}_p)_{S,n}^{\min} = \emptyset = \mathcal{X}(\mathbb{Z}_S) \text{ whenever } 2 \notin S,$$

since $\mathcal{X}(\mathbb{F}_2) = \mathbb{P}^1(\mathbb{F}_2) \setminus \{0, 1, \infty\} = \emptyset$, hence $\mathcal{X}(\mathbb{Z}_2) = \emptyset$.

Our results

Theorem (Best, Betts, Kumpitsch, L., McAndrew, Qian, Studnia, Xu (Arizona 2020)[1])

(1) *Depth 1: explicit equations defining* $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,1}$ *for* $S = \{2\}$*:*

$$\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{2\},1} = S_3.\{z \in \mathcal{X}(\mathbb{Z}_p) : \log(z) = 0\}.$$

(2) *Depth 2: explicit equations defining* $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ *for* $S = \{2\}$ *and* $S = \{2, q\}$*:*

$$\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{2\},2} = S_3.\{z \in \mathcal{X}(\mathbb{Z}_p) : \log(z) = \mathrm{Li}_2(z) = 0\}$$
$$\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{2,q\},2} = S_3.\{z \in \mathcal{X}(\mathbb{Z}_p) : a_{2,q}\,\mathrm{Li}_2(z) = a_{q,2}\,\mathrm{Li}_2(1-z)\}$$

for certain constants $a_{2,q}, a_{q,2} \in \mathbb{Q}_p$*.*

---

[1] *Refined Selmer equations for the thrice-punctured line in depth two,* https://arxiv.org/abs/2106.10145

Our results

Theorem (cont.)

(3) *Bound on number of solutions for* $p = 3$*:* $\mathcal{X}(\mathbb{Z}_3)^{\min}_{\{2,q\},2}$ *consists of at most two* S_3*-orbits of points. Equality holds iff*

$$\min\{v_3(a_{2,q}), v_3(a_{q,2})\} = 1 + v_3(\log(q)). \qquad (\dagger)$$

Corollary

If $q > 3$ *is a Fermat or Mersenne prime, then the refined Kim conjecture holds for* $S = \{2, q\}$ *and* $p = 3$ *in depth 2:*

$$\mathcal{X}(\mathbb{Z}_3)^{\min}_{\{2,q\},2} = \mathcal{X}(\mathbb{Z}[\tfrac{1}{2q}]).$$

Our results

The coefficients $a_{2,q}$, $a_{q,2}$ can be calculated algorithmically. We implemented[2] the algorithm in SAGE and used the criterion (†) to verify:

Theorem (BBKLMcAQSX)

The refined Kim conjecture holds in depth 2 for $S = \{2, q\}$ and $p = 3$ when q is one of

$$19, 37, 53, 107, 109, 163, 181, 199, 269, 271, 379,$$
$$431, 433, 487, 523, 541, 577, 593, 631, 701, 739,$$
$$757, 809, 811, 829, 863, 883, 919, 937, 971, 991.$$

[2] `https://github.com/martinluedtke/dcw_coefficients`

4. Selmer schemes

Selmer schemes

The sets $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ are defined using a diagram as follows:

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{X}(\mathbb{Z}_p) \\ {\scriptstyle j_S}\big\downarrow & & \big\downarrow{\scriptstyle j_p} \\ \mathrm{Sel}_{S,n}(\mathcal{X}) & \xrightarrow[\mathrm{loc}_p]{} & \mathrm{H}^1_{\mathrm{f}}(G_p, U_n^{\text{ét}}) \end{array}$$

The localisation map loc_p is an algebraic map between (the $\mathbb{Q}_p$-points of) affine spaces over $\mathbb{Q}_p$.

$$\mathcal{X}(\mathbb{Z}_p)_{S,n} = \{z \in \mathcal{X}(\mathbb{Z}_p) : j_p(z) \in \mathrm{loc}_p(\mathrm{Sel}_{S,n}(\mathcal{X}))\}.$$

Selmer schemes

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{X}(\mathbb{Z}_p) \\ \downarrow {\scriptstyle j_S} & & \downarrow {\scriptstyle j_p} \\ \mathrm{Sel}_{S,n}(\mathcal{X}) & \xrightarrow[\mathrm{loc}_p]{} & \mathrm{H}^1_{\mathrm{f}}(G_p, U_n^{\text{ét}}) \end{array}$$

Theorem

If the localisation map loc_p *is not dominant, then* $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ *is finite.*

Proof (Sketch).

If $\mathrm{loc}_p(\mathrm{Sel}_{S,n}(\mathcal{X}))$ is not Zariski-dense, there exists a function $f \neq 0$ on $\mathrm{H}^1_{\mathrm{f}}(G_p, U_n^{\text{ét}})$ vanishing on $\mathrm{loc}_p(\mathrm{Sel}_{S,n}(\mathcal{X}))$. Then $f \circ j_p$ is nonzero and p-adic analytic on each residue disk of $\mathcal{X}(\mathbb{Z}_p)$. It has only finitely many zeroes and vanishes on $\mathcal{X}(\mathbb{Z}_S)$. □

Selmer schemes

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{X}(\mathbb{Z}_p) \\ \downarrow j_S & & \downarrow j_p \\ \mathrm{Sel}_{S,n}(\mathcal{X}) & \xrightarrow[\mathrm{loc}_p]{} & \mathrm{H}^1_f(G_p, U_n^{\text{ét}}) \end{array}$$

Remark

The schemes $\mathrm{Sel}_S(\mathcal{X})$ and $\mathrm{H}^1_f(G_p, U^{\text{ét}})$ are moduli spaces of torsors under the $\mathbb{Q}_p$-prounipotent étale fundamental group $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}, b)$ (for some base point $b \in \mathcal{X}(\mathbb{Z}_S)$), and the vertical maps j_S and j_p assign to each point x of $\mathcal{X}$ its path torsor:

$$x \mapsto \pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b, x).$$

Working in depth n corresponds to replacing the fundamental group by its n-th lower central series quotient.

Refined Selmer schemes

We also have ℓ-adic localisation maps for $\ell \in S$:

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Q}_\ell) \\ \downarrow j_S & & \downarrow j_\ell \\ \mathrm{Sel}_{S,n}(\mathcal{X}) & \xrightarrow{\mathrm{loc}_\ell} & \mathrm{H}^1(G_\ell, U_n^{\text{ét}}). \end{array}$$

The refined Selmer scheme is defined as the subscheme $\mathrm{Sel}_{S,n}^{\min}(\mathcal{X}) \subseteq \mathrm{Sel}_{S,n}(\mathcal{X})$ of points α satisfying local conditions at primes in S:

$$\mathrm{loc}_\ell(\alpha) \in \overline{j_\ell(X(\mathbb{Q}_\ell))}^{\mathrm{Zar}} \quad \text{for all } \ell \in S.$$

Then we can define the refined Chabauty–Kim locus

$$\mathcal{X}(\mathbb{Z}_p)_{S,n}^{\min} = \{z \in \mathcal{X}(\mathbb{Z}_p) : j_p(z) \in \mathrm{loc}_p(\mathrm{Sel}_{S,n}^{\min}(\mathcal{X}))\}.$$

5. Chabauty–Kim for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ in depth 2

Chabauty–Kim for $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ in depth 2

For the thrice-punctured line, the Selmer scheme in depth 2 is given by

$$\mathrm{Sel}_{S,2}(\mathcal{X}) = \mathbb{A}^S \times \mathbb{A}^S.$$

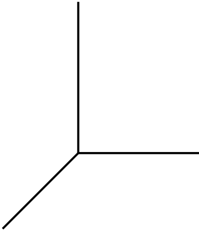
The localisation map for $\ell \in S$ is the projection

$$\begin{aligned} \mathrm{loc}_\ell \colon \mathbb{A}^S \times \mathbb{A}^S &\to \mathbb{A}^2, \\ ((x_\ell)_{\ell \in S}, (y_\ell)_{\ell \in S}) &\mapsto (x_\ell, y_\ell). \end{aligned}$$

Chabauty–Kim for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ in depth 2

The map $j_\ell \colon X(\mathbb{Q}_\ell) \to \mathbb{A}^2$ is given by

$$j_\ell(z) = (v_\ell(z), v_\ell(1 - z)).$$



Lemma

$j_\ell(X(\mathbb{Q}_\ell))^{\mathrm{Zar}} = \{x = 0\} \cup \{y = 0\} \cup \{x = y\}$ *in* $\mathbb{A}^2$

Proof.

If $z \in X(\mathbb{Q}_\ell)$, then $z + z' = 1$ with $z, z' \in \mathbb{Q}_\ell^\times$.
Then $0 = v_\ell(1) \geq \min\{v_\ell(z), v_\ell(z')\}$ with equality if $v_\ell(z) \neq v_\ell(z')$.

$$\Rightarrow v_\ell(z) = 0 \quad \text{or} \quad v_\ell(z') = 0 \quad \text{or} \quad v_\ell(z) = v_\ell(z'). \qquad \square$$

Chabauty–Kim for $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ in depth 2

Thus, the refined Selmer scheme $\mathrm{Sel}^{\mathrm{min}}_{S,2}(\mathcal{X})$ in depth 2 is the union of $3^{\#S}$ linear subspaces of $\mathbb{A}^S \times \mathbb{A}^S$ of dimension $\#S$, given by refinement conditions

$$x_\ell = 0 \text{ resp. } y_\ell = 0 \text{ resp. } x_\ell = y_\ell$$

for each $\ell \in S$.

Chabauty–Kim for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ in depth 2

Dan-Cohen, Wewers:

$$z \mapsto (v_\ell(z))_{\ell \in S}, (v_\ell(1-z))_{\ell \in S}$$

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{X}(\mathbb{Z}_p) \\ \downarrow j_S & & \downarrow j_p \\ \mathbb{A}^S \times \mathbb{A}^S & \xrightarrow[\mathrm{loc}_p]{} & \mathbb{A}^3 \end{array}$$

$$z \mapsto \begin{pmatrix} \log(z) \\ \log(1-z) \\ -\mathrm{Li}_2(z) \end{pmatrix}$$

$$\mathrm{loc}_p((x_\ell)_{\ell \in S}, (y_\ell)_{\ell \in S}) = \begin{pmatrix} \sum_{\ell \in S} \log(\ell) x_\ell \\ \sum_{\ell \in S} \log(\ell) y_\ell \\ \sum_{\ell, q \in S} a_{\ell,q} x_\ell y_q \end{pmatrix}$$

Chabauty–Kim for $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ in depth 2

If $S = \{2, q\}$, then the localisation map

$$\mathrm{loc}_p \colon \mathbb{A}^S \times \mathbb{A}^S \to \mathbb{A}^3$$

has Zariski-dense image.

However, the *refined* Selmer scheme has dimension $\#S = 2$, hence its image in $\mathbb{A}^3$ is not Zariski-dense.

If $f = 0$ is a nontrivial equation on $\mathbb{A}^3$ vanishing on $\mathrm{loc}_p(\mathrm{Sel}^{\mathrm{min}}_{S,2}(\mathcal{X}))$, then pulling back along $j_p \colon \mathcal{X}(\mathbb{Z}_p) \to \mathbb{A}^3$ gives a nontrivial equation cutting out $\mathcal{X}(\mathbb{Z}_p)^{\mathrm{min}}_{S,2}$:

$$a_{2,q}\,\mathrm{Li}_2(z) = a_{q,2}\,\mathrm{Li}_2(1 - z).$$

6. Further developments in higher depth

Kim's conjecture in higher depth

With Alex Betts and Theresa Kumpitsch, building on work by Corwin and Dan-Cohen, we are looking at higher depth.

Theorem (Betts, Kumpitsch, L. 2021)

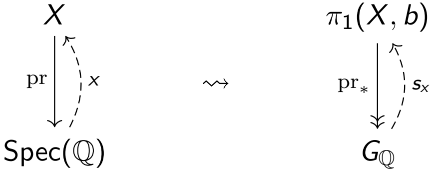
1. *The Kim conjecture holds for $S = \emptyset$ and all odd primes $p > 3$ in depth $n = p - 3$.*
2. *The refined Kim conjecture holds for $S = \{2\}$ and all odd primes $p > 3$ in depth $n = p - 3$.*

In the second case, equations for $\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{2\},p-3}$ (up to S_3-orbits) are given by

$$\log(z) = 0, \quad \mathrm{Li}_k(z) = 0 \text{ for } 2 \leq k \leq p-3 \text{ even.}$$

Selmer section conjecture

Let $X/\mathbb{Q}$ be a smooth hyperbolic curve, $b \in X(\mathbb{Q})$, and let $\pi_1^{\text{ét}}(X, b)$ be the profinite étale fundamental group. Every point $x \in X(\mathbb{Q})$ induces a Galois section $s_x \colon G_{\mathbb{Q}} \to \pi_1^{\text{ét}}(X, b)$:



Conjecture (Grothendieck 1986)

The map

$$X(\mathbb{Q}) \to \left(\begin{array}{c} \textit{conjugacy classes} \\ \textit{of sections of } \mathrm{pr}_* \end{array} \right)$$

is a bijection.

Let $\mathcal{X}/\mathbb{Z}_S$ be a smooth regular model of $X/\mathbb{Q}$ and $b \in \mathcal{X}(\mathbb{Z}_S)$.

Conjecture (Selmer section conjecture)

Let $s\colon G_{\mathbb{Q}} \to \pi_1(X, b)$ be a Galois section such that for every prime ℓ, the restriction of s to the local Galois group G_ℓ is induced by a point

$$\begin{cases} \textit{in } X(\mathbb{Q}_\ell) & \textit{if } \ell \in S, \\ \textit{in } \mathcal{X}(\mathbb{Z}_\ell) & \textit{if } \ell \notin S. \end{cases}$$

Then s is induced by a point in $\mathcal{X}(\mathbb{Z}_S)$.

Selmer section conjecture

Theorem (Betts, Kumpitsch, L. (in progress))

If $\mathcal{X}/\mathbb{Z}_S$ satisfies the refined Kim conjecture, then it satisfies the Selmer section conjecture.

Corollary

$\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \smallsetminus \{0, 1, \infty\}$ satisfies the Selmer section conjecture for $S = \emptyset$ and for $S = \{2\}$.

Uniform bounds in the S-unit equation

Consider the localisation map

$$\mathrm{loc}_p\colon \mathrm{Sel}^{\mathrm{min}}_{S,n}(\mathcal{X}) \to \mathrm{H}^1_f(G_p, U_n^{\text{ét}}).$$

Betts (2021): The rings of functions on both schemes have a weight filtration by finite-dimensional subspaces, and the map

$$\mathrm{loc}_p^\sharp\colon \mathcal{O}(\mathrm{H}^1_f(G_p, U_n^{\text{ét}})) \to \mathcal{O}(\mathrm{Sel}^{\mathrm{min}}_{S,n}(\mathcal{X}))$$

is filtered. Any $f \neq 0$ in the kernel with weight $\leq m$ yields a Coleman function of weight $\leq m$ vanishing on $\mathcal{X}(\mathbb{Z}_S)$. Its number of zeroes is bounded in terms of m.

Uniform bounds in the S-unit equation

Theorem (Leonhardt, L. (2022))

Let $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\}$. *There exists a constant* $\gamma > 0$ *such that*

$$\#\mathcal{X}(\mathbb{Z}_S) \leq e^{\gamma s^2 \log(s)^2},$$

where $s = \#S$.

This is worse than the bound $\#\mathcal{X}(\mathbb{Z}_S) \leq 3 \cdot 7^{2s+1}$ due to Evertse.

Thank you