The S-unit equation and non-abelian Chabauty in depth 2

Joint work with Alexander Betts, Theresa Kumpitsch, Martin Lüdtke,
Angus McAndrew, Lie Qian, Elie Studnia, Yujie Xu

Plan:

1. History / background
2. Chabauty.
3. Nonabelian extension
4. Refinements + applications

The S-unit Equation

Throughout let S be a finite set of primes of $\mathbb{Q}$ or in a number field K

$u \in \mathbb{Q}$ $\quad v_p(u) = 0 \quad \forall p \notin S$

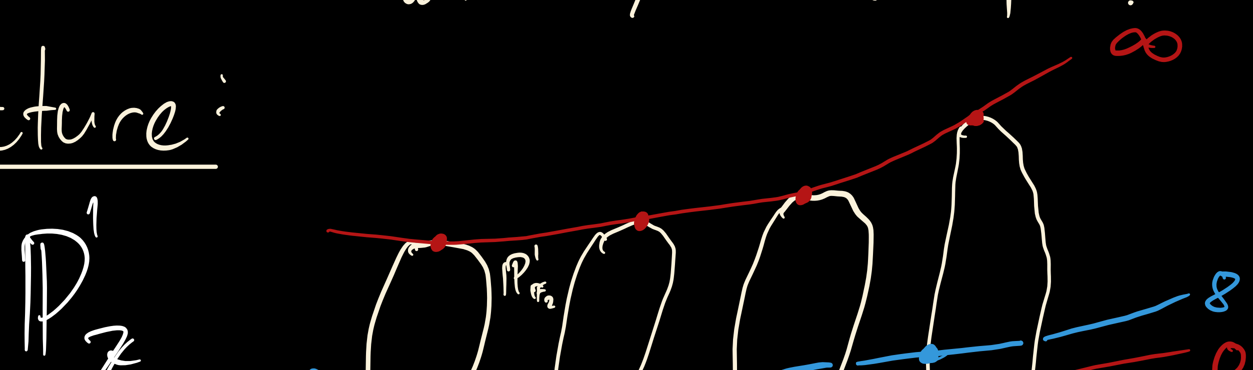
Def: A pair of S-units (u, v) such that u + v = 1 is called a solution to the S-unit equation.

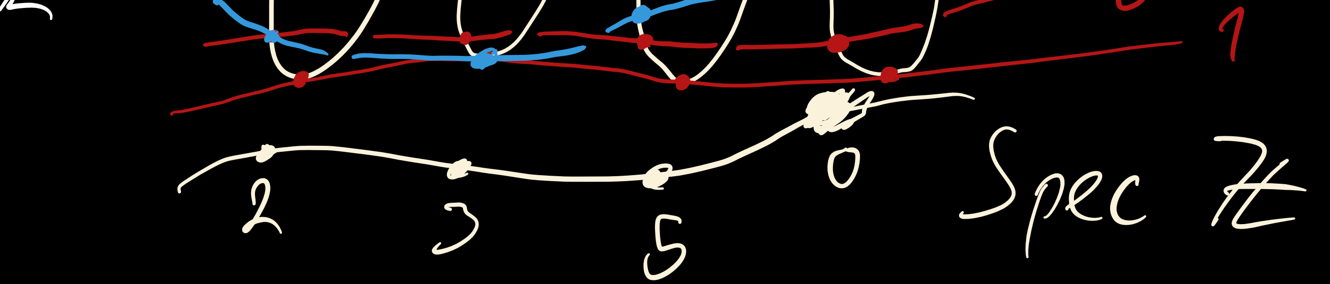
Ex: $S = \{2,3\}$, $K = \mathbb{Q}$ then $9 - 8 = 1$ so $(9, -8)$ is a solution to the $\{2,3\}$-unit equation, we can also take $(-8, 9)$ or $(\frac{9}{8}, -\frac{1}{8})$.

Observations: 1) There is an action of S_3 on solutions, generated by these symmetries: $(u,v) \mapsto (v,u)$, $(u,v) \mapsto (\frac{-u}{v}, \frac{1}{v})$.

2) We have $v = 1 - u$ so in terms of u we have a solution if and only if all of $u, 1-u, \frac{1}{u}, \frac{1}{1-u}$ are $\not\equiv 0 \pmod p$ $\forall p \notin S$.

Picture:





Solutions to the S-unit equation can be thought of as $\mathbb{Z}[\frac{1}{S}]$-points of $\mathbb{P}^1 \setminus \{0,1,\infty\}$, we will use $z = u$ from now on.

<u>Thm</u> (Siegel): For fixed S we have $\Big|\underset{\overset{\shortparallel}{\mathcal{X}}}{\mathbb{P}^1 \setminus \{0,1,\infty\}}(\mathbb{Z}[\tfrac{1}{S}])\Big| < \infty.$

This result is not constructive however!

Questions remain about this problem:

1. Can we bound the set of solutions in terms of S or |S| and K or deg(K)?
2. Can we (efficiently) determine the set of solutions given any S and K?
3. Can we bound the heights of solutions?

not complete history

These problems have a long history: Some examples:

1. <u>Thm</u> (Evertse):

$$\left|\mathbb{P}^1 \setminus \{0,1,\infty\}(\mathbb{Z}[\tfrac{1}{S}])\right| < 3 \cdot 7^{\deg K + |S|}$$

Lower bounds due to Konyagin-Soundararajan.

2. Matschke has a solver based on sieving using height bounds coming from modularity due to Matschke-von Känel.

3. Bugeaud, Győry, Le Fourn,....

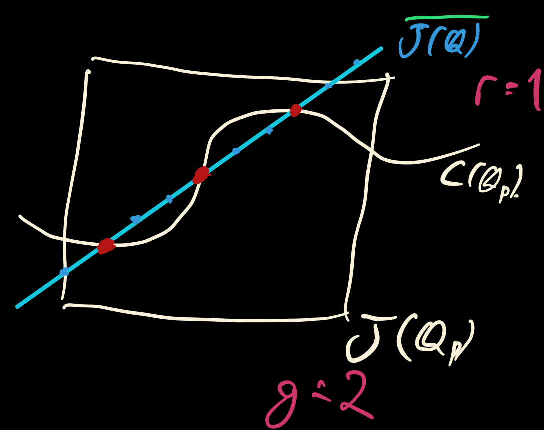
Goal of our work: Not to attack these well studied problems directly, instead we wish to test some conjectures in non-abelian Chabauty applied to $\mathbb{P}^1 \setminus \{0,1,\infty\}$.

2. Chabauty Methods:

Let $C/\mathbb{Q}$ be a nice curve of genus $g \geq 2$ and fix a prime p of good reduction for C, and a base point $P \in C(\mathbb{Q})$.
Then we can often determine $C(\mathbb{Q})$ using Chabauty's method.

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook] \arrow[d] & C(\mathbb{Q}_p) \arrow[d] \arrow[dr, "\text{analytic}\ j_p"] & \\
\mathrm{Jac}(C) = J(\mathbb{Q}) \arrow[r, hook] & J(\mathbb{Q}_p) \arrow[r, phantom, "\cong"] & \mathrm{Lie}\, J(\mathbb{Q}_p)
\end{tikzcd}$$

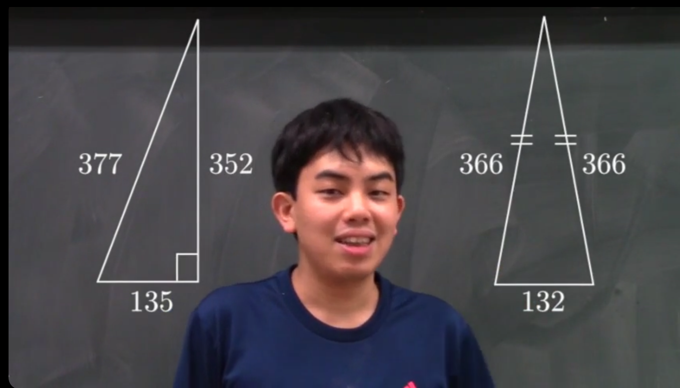
abelian group rank r — g-dimensional p-adic Lie group.



If $r < g$ then $J(\mathbb{Q}) \cap C(\mathbb{Q}_p)$ should be finite, this proves the Mordell conjecture for these curves.
Coleman: defines an integration theory for curves over p-adic fields, which is p-adically valued. This makes the map j_p and hence Chabauty's method explicit, we can find $g - r$ independent

holomorphic differentials $\{\omega_i\}$ on $J(\mathbb{Q}_p)$ such that the integrals $\int_p^x \omega_i$ simultaneously vanish on $C(\mathbb{Q})$.

Application: <u>Thm:</u> (Hirakawa-Matsumura, 2019):
There exists a unique pair of a rational right triangle and a rational isosceles triangle with the equal areas and equal perimeters.



Hideki Matsumura

<u>Pf</u>: Chabauty on a genus 2 rank 1 curve: $r^2 = (-3w^3 + 2w^2 - 6w + 4)^2 - 8w^6$

<u>S-units</u>: Fix a prime $p \notin S$. We can form a similar diagram using the generalized Jacobian of $\mathcal{X}$. Assume $K = \mathbb{Q}$.

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

$$\begin{tikzcd}
\mathcal{X}(\mathbb{Z}[\frac{1}{S}]) \arrow[r] \arrow[d] & \mathcal{X}(\mathbb{Z}_p) \arrow[d] \\
\mathbb{G}_m(\mathbb{Z}[\frac{1}{S}]) \times \mathbb{G}_m(\mathbb{Z}[\frac{1}{S}]) \arrow[r] \arrow[d, phantom, "\cong"] & \mathbb{G}_m(\mathbb{Z}_p) \times \mathbb{G}_m(\mathbb{Z}_p) \arrow[d, phantom, "\cong"] \\
\{\pm 1\} \times \mathbb{Z}^{|S|} \times \{\pm 1\} \times \mathbb{Z}^{|S|} \arrow[r] & \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times
\end{tikzcd}$$

$z \mapsto (z, 1-z)$

$z \mapsto (\log_p z, \log_p 1-z)$

$((v_q)_q, (w_q)_q)_{q \in S} \longmapsto \left(\sum_{q \in S} v_q \log_p q, \sum_{q \in S} w_q \log_p q\right)$.

$(v_q(z))_{q \in S}$

Bottom left group has rank $2|S|$ and the bottom right is of dimension 2. So a naive application of Chabauty to this diagram would not apply.

$\pm q^n \pm 1 = 1.$

Consider the case of $|S| = 1$, $S = \{q\}$, and assume $\underline{v_q(1-z)=0.}$

$p \notin S$ prime

$$\begin{tikzcd}
\pm q^a = z \arrow[r, mapsto] \arrow[d] & z \arrow[d] \\
(a, 0) \arrow[r, mapsto] & (\log z, \log(1-z)) \\
 & (a \log_p q, 0)
\end{tikzcd}$$

then the bottom horizontal map has non-dense image.

So the set of z s.t. $v_q(1-z)=0$ lie in the locus where $\log(1-z)=0$.

The zeroes of log are precisely the roots of unity. (away from $0, \infty$)

$\log_3(1-z)=0$ 3-adically $\Rightarrow z=2.$

Eg:

If $q = 2$, $p = 3$ then this gives: Solutions to the $\{2\}$-unit equation for which $v_2(1-z) = 0$ have $1-z$ a root of log which is 3-adically near -1, hence $1-z = -1$ and $z = 2$ is the only solution.

Other solutions?

What about the complete set of solutions when $|S| = 1$?

If $v_q(z) > 0$ then $v_q(1-z) = 0$.

If $v_q(z) = 0$ then swapping z and $1-z$ reduces us to the first case.

If $v_q(z) < 0$ then $v_q(1-z) = v_q(z)$ and then $v_q(\frac{-y}{z}) = 0$, $v_q(\frac{1}{z}) > 0$ so the S_3-action reduces us to the previous case.

In fact, valuations of $(z, 1-z)$ look like:

$v_q(z)=0$ $\quad (v_q(z), v_q(1-z))$

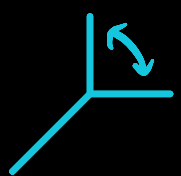
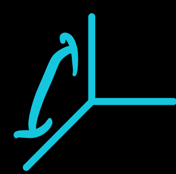
$v_q(1-z)=0$ Tropicalization of $\mathbb{P}^1\setminus\{0,1,\infty\}$

$v_q(z)=v_q(1-z)\leq 0$

Generators of S_3-action have the effect of swapping

$$u \longleftrightarrow v \quad \text{or} \quad (u,v) \leftrightarrow \left(-\frac{u}{v}, \frac{1}{v}\right)$$

In the tropicalization this acts via

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  $\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ 

---

3. Non-abelian Chabauty

- Minhyong Kim has introduced an extension of Chabauty's method that conjecturally gives another proof of Mordell's conjecture In many cases.
- This method reproves Siegel's theorem but remains to be fully understood.

Kim's idea: Extend the Chabauty diagram to non-linear objects on the second row (Selmer schemes).

Before we took the Jacobian which is an abelianized fundamental group, by including more non-abelian information we hope to retain more knowledge about the curve.

Let $\mathcal{X}/_{\mathbb{Z}[\frac{1}{S}]}$ be a model of a <u>hyperbolic</u> curve (eg. $\mathbb{P}^1\setminus\{0,1,\infty\}$) then:

- $U^{ét}$ denotes the $\mathbb{Q}_p$-pro-unipotent completion of $\pi_1^{ét}(\mathcal{X}_{\bar{\mathbb{Q}}})$
- $U_n^{ét}$ denotes the quotient by the nth step of the lower central series (n is called the depth).
- U^{dR}, U_n^{dR} are defined likewise for the de Rham fundamental group $\pi_1^{dR}(\mathcal{X})$

Then we consider the <u>local Selmer scheme</u>:

$\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

$$H^1_f(G_p, U_n^{ét}) \subseteq H^1(G_p, U_n^{ét})$$

Consisting of crystalline classes, and we have an isomorphism

$$H^1_f(G_p, U_n^{ét}) \cong F^0\backslash U_n^{dR} \qquad (J(\mathbb{Q}_p) \simeq \mathrm{Lie}\, J(\mathbb{Q}_p).)$$

Hodge

Similarly we define the <u>global Selmer scheme</u>:

$$Sel_{S,n} = Sel_{S,n}(\mathcal{X}) \subseteq H^1(G_S, U_n^{ét}).$$

containing those classes which are crystalline at p and are unramified at all $q \notin S \cup \{p\}$.

<u>Thm</u> (Kim): This fits into a commutative diagram (Kim's cutter) for each n:

$$\begin{tikzcd}
\mathcal{X}(\mathbb{Z}[\frac{1}{S}]) \arrow[r] \arrow[d, "j_S"] & \mathcal{X}(\mathbb{Z}_p) \arrow[d, "j_p"] \arrow[dr, "j_{dR}"] & \\
Sel_{S,n} & H^1_f(G_p, U_n^{ét}) \arrow[r, phantom, "\cong"] & F^0\backslash U_n^{dR}
\end{tikzcd}$$

analytic

algebraic

($\mathbb{Q}_p$-alg

(alg schemes) finite type $\quad \mathrm{Sel}_{S,n} \xrightarrow[\mathrm{loc}_p]{} H^1_f(G_p, U_n) \to F^{\ldots} U_n$

In the n = 1 case this recovers the classical Chabauty diagrams we saw before.

<u>Thm</u> (Kim): If $\dim \mathrm{Sel}_{S,n} < \dim H^1_f(G_p, U_n^{\text{ét}})$ then $\mathcal{X}(\mathbb{Z}[\frac{1}{S}])$ is finite and lies in $\mathcal{X}(\mathbb{Z}[\frac{1}{S}])_n := j_p^{-1}(\mathrm{loc}_p(\mathrm{Sel}_{S,n}(\mathcal{X})))$ for all n.

<u>Conjecture</u> (Kim): We always have

$$\mathcal{X}(\mathbb{Z}[\tfrac{1}{S}]) = \mathcal{X}(\mathbb{Z}[\tfrac{1}{S}])_n$$

eventually. $\quad n \gg 0$

<u>Motivating question</u>: How deep do we need to go?

<u>4. Refinements and application to $\mathbb{P}^1 \setminus \{0,1,\infty\}$.</u>

For $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ in depth 2 we have

$$\mathrm{Sel}_{S,2} \underset{\text{Soulé vanishing}}{\cong} \mathrm{Sel}_{S,1} \cong \mathbb{A}^{|S|} \times \mathbb{A}^{|S|}$$

$$H^1_f(G_p, U_2^{\text{ét}}) \cong \mathbb{A}^3 \cong \mathbb{A}^2 \times \mathbb{A}$$

$\uparrow \mathbb{G}_m \times \mathbb{G}_m$ from before

$$\begin{array}{ccccccc} z & & \mathcal{X}(\mathbb{Z}[\frac{1}{S}]) & \longrightarrow & \mathcal{X}(\mathbb{Z}_p) & & z \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ ((v_q(z))_q, (v_q(1-z))_q) & & \mathbb{A}^{|S|} \times \mathbb{A}^{|S|} & \longrightarrow & \mathbb{A}^3 & & (\log(z), \log(1-z), \mathrm{Li}_2(z)) \end{array}$$

$$((x_q)_q, (y_q)_q) \longrightarrow \left(\sum x_q \log q, \sum y_q \log q, h(x_q, y_q)\right)$$

$\mathrm{Li}_2(z)$ is an iterated Coleman integral: $\int \frac{\log(1-z)}{z} dz$

Defined near 0 by the classical power series $\sum_{k=0}^{\infty} \frac{z^k}{k^2}$.

h_3 is the most mysterious part of this diagram.

Thm (Dan-Cohen, Wewers):

1. h_3 is a bilinear form
2. The coefficients of this form satisfy

$$a_{\ell,q} + a_{q,\ell} = \log q \log \ell \quad \text{for } \ell, q \in S.$$

We give new proofs of these facts.

Problem: $2|S| > 2$ as soon as $|S| > 1$, image of loc_p will be dense!

To directly apply this version of Kim's cutter we need to go to $n = 3$ at least!

Corwin & Dan-Cohen go to depth 4 and find the function

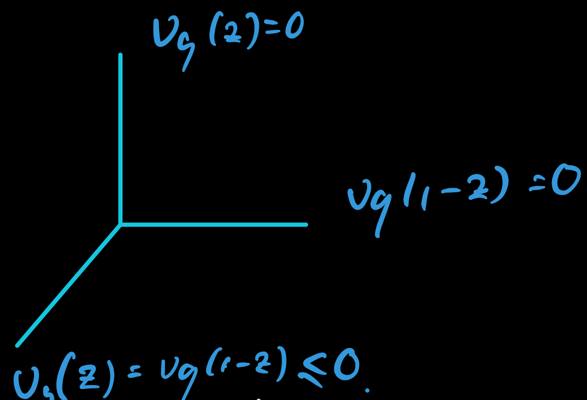
$$\zeta^{\mathfrak{u}}(3)\log^{\mathfrak{u}}(3)\,\mathrm{Li}_4^{\mathfrak{u}} - \left(\frac{18}{13}\mathrm{Li}_4^{\mathfrak{u}}(3) - \frac{3}{52}\mathrm{Li}_4^{\mathfrak{u}}(9)\right)\log^{\mathfrak{u}}\mathrm{Li}_3^{\mathfrak{u}}$$
$$-\frac{(\log^{\mathfrak{u}})^3\,\mathrm{Li}_1^{\mathfrak{u}}}{24}\left(\zeta^{\mathfrak{u}}(3)\log^{\mathfrak{u}}(3) - 4\left(\frac{18}{13}\mathrm{Li}_4^{\mathfrak{u}}(3) - \frac{3}{52}\mathrm{Li}_4^{\mathfrak{u}}(9)\right)\right)$$

cutting out solutions for the {3}-unit equation.

Alternative approach: Betts-Dogra (arXiv:1909.05734) introduce refined Selmer schemes of smaller dimension, that take into account local behavior at primes in S.

This works out to be precisely the tropical decomposition we considered above: For any $z \in \mathbb{P}^1 \setminus \{0,1,\infty\}(\mathbb{Z}[\frac{1}{S}]), q \in S$

$v_q(z), v_q(1-z)$ lies on one of the rays



each of $\dim = 2 < 3$

So $j_S(z)$ lands in one of $3^{|S|}$ different refined Selmer schemes depending on which ray z lay on for each prime in S.

We denote these as $\mathrm{Sel}_{S,2}^{1,/}$ for example.

<u>Upshot</u>: $\dim \mathrm{Sel}_{S,2}^{1,/} = 2 < 3$ so we can apply "refined non-abelian Chabauty" in depth 2 to bound the solutions to the S-unit equation.

<u>Remark</u>: this method in depth 1 is exactly what we did in the first example of finding $\{q\}$-units with $v_q(1-z) = 0$.

<u>Thm</u> (BBKLMQSX): Let $S = \{\ell, q\}$ and $p \notin S$ then up to the S_3-action the solutions to the S-unit equation lie in

$$\mathcal{X}(\mathbb{Z}_p)^{1,-}_{S,2}$$

Which is given by $a_{\ell,q}\mathrm{Li}_2(z) = a_{q,\ell}\mathrm{Li}_2(1-z)$

When we know one solution we can determine $a_{\ell,q}$ and then control all other possible solutions.

Thm (BBKLMQSX): Let $S = \{\ell\}$ and $p \neq \ell$ be prime, then

$$\mathcal{X}(\mathbb{Z}_p)^{min}_{\{\ell\}}$$

is cut out by $\log(z) = 0$, $Li_2(z) = 0$ (Up to the S_3-action)

Thm (BBKLMQSX): Let $S = \{q, \ell\}$ and let $p \notin S$ be prime then

$$\mathcal{X}(\mathbb{Z}_p)^{min}_{\{q,\ell\}}$$

is cut out by

$$a_{\ell,q} Li_2(z) = a_{q,\ell} Li_2(1-z).$$

Up to the S_3-action.

When we know a solution we can go further and find the $a_{\ell,q}$'s.

Thm (BBKLMQSX): Let $q = 2^n \pm 1$, be a Fermat or Mersenne prime then $\mathcal{X}(\mathbb{Z}_p)^{1,-}_{\{2,q\},2}$ is cut out by

$$\underbrace{Li_2(1 \mp q)}_{a_{2,q}} Li_2(z) = Li_2(\pm q) Li_2(1-z).$$

We also show that working with refined Selmer schemes in depth 2 gives an easily checkable condition for extra solutions, this completely resolves the $|S| = 1$ case.

arXiv:1812.05707v5 [math.NT] 21 Aug 2020

arXiv:1812.05707v5 [math.NT] 21 Aug 2020

arXiv:1812.05707v5 [math.NT] 21 Aug 2020