An open source implementation for solving S-unit equations

Christopher Rasmussen

Wesleyan University

University of Debrecen
Online Number Theory Seminar
November 18, 2022

Outline

1. Introductions / Background / History
2. A Selection of Applications
3. How the Solver Works
4. What's Good / What's Bad / What's Next

Outline

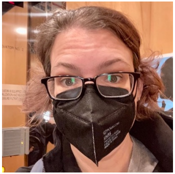
S-unit equation Collaborators

Alejandra Alvaro
Eastern Illinois University

Angelos Koutsianas
Aristotle University, Thessaloniki

Beth Malmskog
Colorado College

Christopher Rasmussen
Wesleyan University



Christelle Vincent
University of Vermont

Mckenzie West
University of Wisconsin-Eau Claire

S-unit equation Collaborators

With assistance from:

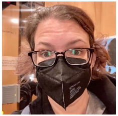
Norman Danner, Bjorn Poonen, David Roe, Andrew Sutherland, . . .

And support from:

SageDays 62, ICERM, Microsoft Research, Beatrice Yormark Fund for Women in Mathematics, van Vleck Fund @ Wesleyan, . . .








And building on the past work of:

Baker, Baker-Wüstholz, Bremner, Brumer, de Weger, Evertse-Győry, Gelfond, Győry, Győry-Yu, Koutsianas, Lenstra-Lenstra Lovász, Mahler, Malmskog-R., Merriman-Smart, Pethö-de Weger, SageMath Developers, Schneider, Siegel, Smart, Tzanakis-de Weger, Wildanger, Yu, . . .

Independent Efforts

The community is fortunate to have *multiple* efforts to solve unit equations under active development.

- Joint work of von Känel and Matschke on arithmetic of elliptic curves with good reduction outside S (includes S-unit equations over $\mathbb{Q}$, S-integral points on curves, Thue-equations, ...)
  More Information

- Benjamin Matschke has a general S-unit solver, currently in development.
  More Information

General Unit Equation In Two Variables

K	a number field of degree d	
Γ_0, Γ_1	finitely generated subgroups of $K^\times$	$\boldsymbol{\Gamma} := \Gamma_0 \times \Gamma_1$
τ_0, τ_1	variables (view $\tau_i \in \Gamma_i$)	$\boldsymbol{\tau} := (\tau_0, \tau_1) \in \boldsymbol{\Gamma}$
α_0, α_1	fixed elements of $K^\times \times K^\times$	$\boldsymbol{\alpha} := (\alpha_0, \alpha_1)$

$$\boldsymbol{\alpha} \cdot \boldsymbol{\tau} = \alpha_0\tau_0 + \alpha_1\tau_1$$

Problem

Determine the set $T = \{\boldsymbol{\tau} \in \boldsymbol{\Gamma} : \boldsymbol{\alpha} \cdot \boldsymbol{\tau} = 1\}$.

An Incomplete History

$$T = \{\tau \in \mathbf{\Gamma} : \alpha \cdot \tau = 1\}$$

1921 (Siegel) $\#T < \infty$ for any number field K, $\Gamma_0 = \Gamma_1 = \mathcal{O}_K^\times$.

1933 (Mahler) $\#T < \infty$ for $K = \mathbb{Q}$, $\Gamma_0 = \Gamma_1 = \mathbb{Z}[\frac{1}{p_1}, \ldots, \frac{1}{p_r}]^\times$.

1934 (Gelfond, Schneider) For $\alpha, \beta \in \overline{\mathbb{Q}}$ with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$, $\alpha^\beta \in \mathbb{C} - \overline{\mathbb{Q}}$.

1950 (Parry) $\#T < \infty$ for any number field K, $\Gamma_i = \mathcal{O}_{K,S}^\times$, any finite S.

1960 (Lang) $\#T < \infty$ for any K with char $K = 0$, any f.g. $\Gamma_i \leq K^\times$

1967 (Baker) For $\beta_i \in \overline{\mathbb{Q}}$ with $\{\log \beta_i\}$ $\mathbb{Q}$-independent, and for any nonzero linear form $L \in \overline{\mathbb{Q}}[\mathbf{X}]$,

$$|L(\log \beta_1, \ldots, \log \beta_r)| > H(L)^{-C}, \qquad C: \text{ effective}$$

1968 (Bremner) For $\alpha_i \in \overline{\mathbb{Q}}_p^\wedge$, $\mathbb{Q}$-independence of $\{\log_p \alpha_i\}$ implies $\overline{\mathbb{Q}}$-independence.

An Incomplete History

$$T = \{\tau \in \mathbf{\Gamma} : \alpha \cdot \tau = 1\}$$

1974 (Győry) First explicit bounds on solutions in T.

1984 (Evertse) Bound on $\#T$ when $\Gamma_0 = \Gamma_1 = \mathcal{O}_{K,S}^{\times}$.

1985 (Evertse-Győry) Explicit bounds on $\#$ of solutions in $\mathcal{O}_{K,S}^{\times}$ to Thue eqns. $F(\mathbf{X}) = \beta$.

1988 (Evertse-Győry-Stewart-Tijdeman) Fix $K, \Gamma \leq K^{\times}$. For $\alpha \in \Gamma^2$, define $N(\alpha) := \#\{\tau \in \Gamma^2 : \alpha \cdot \tau = 1\}$.

There exist only finitely many α with $N(\alpha) > 2$.

An Incomplete History

$$T = \{\tau \in \mathbf{\Gamma} : \alpha \cdot \tau = 1\}$$

1988 (Yu) Fix $\mathfrak{p} \subseteq \mathcal{O}_K$. For $\rho_i \in K^\times$ with $\operatorname{ord}_\mathfrak{p} \rho_i = 0$, either $\rho_0^{b_0}\rho_1^{b_1}\cdots\rho_t^{b_t} = 1$, or

$$\operatorname{ord}_\mathfrak{p}\left(\rho_0^{b_0}\rho_1^{b_1}\cdots\rho_t^{b_t} - 1\right) < C, \qquad C : \text{effective}$$

1993 (Baker-Wüstholz) Improvements to bounds in (Baker, 1967).

1996 (Beukers-Schlickewei) Bounds for $\#T$ in terms of $\operatorname{rank}_\mathbb{Z} \Gamma_i$ only.

2006 (Győry-Yu) For $\Gamma_0 = \Gamma_1 = \mathcal{O}_{K,S}^\times$ and $s = \#S$, any $\tau \in T$ satisfies

$$h(\tau_i) < (16ds)^{2s+6}\left(1 + \frac{\max\{1, \log R_S\}}{\max\{1, \log P_S\}}\right) \cdot \max_i\{h(\alpha_i)\}$$

An Incomplete History

$$T = \{\tau \in \boldsymbol{\Gamma} : \alpha \cdot \tau = 1\}$$

2016 (von Känel-Matschke) For $K = \mathbb{Q}$, $\Gamma_i = \mathcal{O}_{K,S}^{\times}$, can obtain bounds without methods of Baker, Yu. Solutions induce elliptic curves of specific conductor.

2019 (Győry) Best known bounds for $\Gamma_0 = \Gamma_1 = \mathcal{O}_{K,S}^{\times}$. Formulas avoid self-exponential factors, e.g., s^s.

Outline

Application: Asymptotic Fermat

$$\mathcal{C}_p \colon x^p + y^p + z^p = 0, \qquad abc \neq 0, p > 3 \text{ prime}$$

Theorem (Wiles)

$\#\mathcal{C}_p(\mathbb{Q}) = \varnothing$.

- $\#\mathcal{C}_p(K) < \infty$ by Faltings.
- We say K satisfies **asymptotic Fermat** if $\mathcal{C}_p(K) = \varnothing$ for $p > B_K$.

Theorem (Freitas-Siksek)

There exists a family of real quadratic number fields of density at least $\frac{5}{6}$ which satisfy asymptotic Fermat.

Application: Asymptotic Fermat

$$S = \{\mathfrak{p} : \mathfrak{p} \mid 2 \text{ and } f_{\mathfrak{p}} = 1\}.$$

Theorem (Freitas-Siksek)

Suppose K is totally real, and suppose $[K : \mathbb{Q}]$ is odd or $S \neq \varnothing$. If for every solution $\tau \in T$, $\operatorname{ord}_{\mathfrak{p}} \tau_i \leq 4 \operatorname{ord}_{\mathfrak{p}} 2$, then K satisfies asymptotic Fermat.

Theorem (AKMRVW)

Suppose $[K : \mathbb{Q}] = 3$, K is totally real, 2 is totally ramified in K, and $|\Delta_K| \leq 2000$. Then K satisfies asymptotic Fermat.

Application: Cubic Ramanujan-Nagell

Theorem (Nagell, 1948)

If $x, n \in \mathbb{Z}^{\geq 0}$ *satisfy* $x^2 + 7 = 2^n$*, then* $x \in \{1, 3, 5, 11, 181\}$.

Cubic Ramanujan-Nagell equations: $x^3 + p^k = q^n$.

For $p = 3$ and fixed q, solutions (x, k, n) may be found by solving the S-unit equation over $\mathbb{Q}(\sqrt[3]{3})$ with $S = \{\mathfrak{p} : \mathfrak{p} \mid 3q\} \cup M_K^\infty$.

Theorem (AKMRVW)

For $q < 500$*, there are exactly* 11 *solutions* (x, k, n, q) *to* $x^3 + p^k = q^n$*, and all have* $n = 1$.

Application: Curves with bad reduction at one prime

- Suppose $C \to \mathbb{P}^1$ is a cyclic degree p cover and C has good reduction outside p.

- Differences of branch points, $\alpha_i - \alpha_j$, must be S-units.

$$(\alpha_i - \alpha_j) + (\alpha_j - \alpha_k) = \alpha_i - \alpha_k$$
$$\frac{\alpha_i - \alpha_j}{\alpha_i - \alpha_k} + \frac{\alpha_j - \alpha_k}{\alpha_i - \alpha_k} = 1.$$

- $K = \mathbb{Q}(\{\alpha_i\})$ has $\Delta_K = \pm p^m$.

Theorem (Smart, 1994)

Every genus 2 curve $C/\mathbb{Q}$ with good reduction away from 2 is isomorphic over $\mathbb{Q}$ to a curve appearing in an explicit finite list.

Theorem (Malmskog, R., 2014)

Up to $\mathbb{Q}$-isomorphism, there are exactly 63 Picard curves $C/\mathbb{Q}$ with good reduction away from 3 and a complete list of representative curves has been produced.

Many Other Applications

- Enumerative problems, e.g. C/K with good reduction outside S
- Effective finiteness for binary forms (Evertse-Győry)
- Effective results for discriminant form, index form equations. (Győry)
- Effective methods on deciding monogeneity ($\exists ?\, \alpha$ s.t. $\mathcal{O}_K = \mathbb{Z}[\alpha]$) in number fields, and for determining all integral bases (Győry)
- Strong and effective bounds towards abc-Conjecture (Győry)
- among others . . .

Outline

Notation

For the remainder: $\alpha = (1,1)$, $\Gamma_0 = \Gamma_1 = \mathcal{O}_{K,S}^\times$.

- K, a number field, $\quad d_K := [K : \mathbb{Q}]$, $\qquad w := \#\mu_K$.
- $S = S_{\text{fin}} \cup M_K^\infty$, a finite set of places (incl. all infinite places)

$$S_{\text{fin}} = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\},$$
$$M_K^\infty = \{\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_{s+r+1}\}.$$

- $\mathcal{O}_{K,S}^\times$, the group of S-units in $K^\times$

$$\mathcal{O}_{K,S}^\times = \langle \rho_0 \rangle \times \langle \rho_1, \ldots, \rho_t \rangle \cong \frac{\mathbb{Z}}{w\mathbb{Z}} \times \mathbb{Z}^t$$

Shorthand : $\qquad \boldsymbol{\rho} = (\rho_0, \rho_1, \ldots, \rho_t)$.

Exponent Vectors

- $A_{K,S} := \frac{\mathbb{Z}}{w\mathbb{Z}} \times \mathbb{Z}^t$, $\qquad \Phi_\rho : A_{K,S} \xrightarrow{\cong} \mathcal{O}_{K,S}^\times$,

$$\mathbf{a} = (a_0, a_1, \ldots, a_t) \mapsto \rho^{\mathbf{a}} := \rho_0^{a_0} \rho_1^{a_1} \cdots \rho_t^{a_t}.$$

- Elements $\mathbf{a} \in A_{K,S}$ are called **exponent vectors**.

$$|\mathbf{a}| := \max\{|a_i| : 0 \leq i \leq t\}.$$

- $X_{K,S} := \{x \in \mathcal{O}_{K,S}^\times : 1 - x \in \mathcal{O}_{K,S}^\times\}$, $\qquad E_{K,S} := \Phi_\rho^{-1} X_{K,S}$.

- Solving $\tau_0 + \tau_1 = 1$ is equivalent to finding $E_{K,S}$ inside $A_{K,S}$.

Outline of Algorithm

1. Use bounds on linear forms in logarithms (Baker-Wüstholz, Yu), determine K_0 such that $\mathbf{a} \in E_{K,S} \implies |\mathbf{a}| \leq K_0$.
    - quick (run time < 1 second)
    - K_0 hopelessly large
2. Run a LLL argument to deduce a better bound $|\mathbf{a}| \leq K_1$.
    - quick (run time in seconds)
    - effective ($K_1 \approx (\log K_0)^c$)
    - *not* guaranteed to work
    - *requires* a known K_0
3. Extract $E_{K,S}$ from search space of size $\approx w(2K_1)^t$ by sieve
    - slow and expensive (time and memory)
    - sensitive to which primes $q \in \mathbb{Z}$ split completely in K

Finding the initial bounds

Suppose (τ_0, τ_1) is a solution with $\tau_i = \rho^{\mathbf{b}_i}$, $\quad B := |\mathbf{b}_0| \geq |\mathbf{b}_1|$

- Loop over $\ell \in \{1, 2, \dots, t+1\}$:
  - Suppose $|\tau_0|_{\mathfrak{p}_\ell} = \min \left\{ |\tau_0|_{\mathfrak{p}_k} : 1 \leq k \leq t+1 \right\}$.
  - By standard argument[1] we have $|\tau_0|_{\mathfrak{p}_\ell} \leq \exp\left(-c_3 B\right)$.
  - Calculate explicit bound $K_0(\ell)$ satisfying $B \leq K_0(\ell)$.
    - Case I: $\mathfrak{p}_\ell \in M_K^\infty$
    - Case II: $\mathfrak{p}_\ell \in S_{\text{fin}}$
- Set $K_0 := \max\{K_0(\ell) : 1 \leq \ell \leq t+1\}$.

[1] Smart, The solution to TCDF equations, *Math. Comp.*, 1995.

Initial Bounds – Case I: $\mathfrak{p}_\ell \in M_K^\infty$

- $\mathfrak{p}_\ell$ corresp. to some $\sigma_\ell \colon K \to \mathbb{C}$. Work in $\sigma_\ell(K)$.

- τ_0 near 0 $\implies$ τ_1 near 1 $\implies$ $\log \tau_1$ near 0:

$$|\log \tau_1| \leq 2 \exp(-c_{13} B).$$

- But $\log \tau_1 = b_{1,0} \log \rho_0 + b_{1,1} \log \rho_1 + \cdots + b_{1,t} \log \rho_t$!

- (Baker-Wüstholz) $\qquad |\log \tau_1| \geq \exp(-c_{14} \log B)$.

- $\therefore B < a + b \log B \quad \implies \quad B \leq K_0(\ell)$.

Initial Bounds – Case II: $\mathfrak{p}_\ell \in S_{\text{fin}}$

- $|\tau_0|_{\mathfrak{p}_\ell} \leq \exp(-c_3 B) \implies \text{ord}_{\mathfrak{p}_\ell} \tau_0 \geq c_5' B > 0$
- $\text{ord}_{\mathfrak{p}_\ell} \tau_0 > 0 \quad \implies \quad \text{ord}_{\mathfrak{p}_\ell} \tau_1 = 0.$
- Replace ρ with $\mu := (\mu_0, \mu_1, \ldots, \mu_{t-1})$, $\text{ord}_{\mathfrak{p}_\ell} \mu_i = 0$.

$$\tau_1 = \mu^{\mathbf{d}}, \qquad |\mathbf{d}| \leq B.$$

- (Yu) $\text{ord}_{\mathfrak{p}_\ell} \tau_0 < c_8' \log B$
- $\therefore B < b \log B \quad \implies \quad B \leq K_0(\ell)$.

Reduction via LLL - Preliminaries

- Suppose $\mathcal{L} = \mathbb{Z}\langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N \rangle \subseteq \mathbb{R}^N$, $\quad \mathcal{L}^* := \mathcal{L} - \{\mathbf{0}\}$

- For $\mathbf{y} \in \mathbb{R}^N$, $\ell(\mathcal{L}, \mathbf{y}) := \begin{cases} \min\{||\mathbf{x}|| : \mathbf{x} \in \mathcal{L}^*\} & \text{if } \mathbf{y} \in \mathcal{L}, \\ \min\{||\mathbf{x} - \mathbf{y}|| : \mathbf{x} \in \mathcal{L}\} & \text{if } \mathbf{y} \notin \mathcal{L}. \end{cases}$

LLL Theorem

The reduced basis $\mathbf{x}_1, \ldots, \mathbf{x}_N$ produced when the LLL algorithm is applied to $\mathcal{L}$ satisfies $\ell(\mathcal{L}, \mathbf{0}) \geq m_{\mathcal{L},\mathbf{0}} := (\text{constant}) \cdot ||\mathbf{x}_1||$.

- Idea: Build integer lattice $\mathcal{L}$ from $\tau_1 = \rho^{\mathbf{b}_1}$. If $\ell(\mathcal{L}, \mathbf{y})$ is large, the bound K_0 may be replaced with $K_1(\ell) \ll K_0$.

- Again depends on the "extremal" place $\mathfrak{p}_\ell$: $K_1 := \max\{K_1(\ell)\}$.

Case: $\mathfrak{p}_\ell$ complex

- Write $\log \rho_j = \kappa_j + \lambda_j\sqrt{-1}, \qquad \kappa_j, \lambda_j \in \mathbb{R}$.
- Pick C large. (On the order of K_0.)
- Take $\mathcal{L}$ spanned by columns $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{t+1}$ of

$$\begin{pmatrix} 1 & & 0 & 0 & 0 \\ & \ddots & & \vdots & \vdots \\ 0 & & 1 & 0 & 0 \\ [C\kappa_1] & \cdots & [C\kappa_{t-1}] & [C\kappa_t] & 0 \\ [C\lambda_1] & \cdots & [C\lambda_{t-1}] & [C\lambda_t] & [C\cdot\frac{2\pi}{w}] \end{pmatrix}$$

- Apply LLL and compute the bound $m_{\mathcal{L},\mathbf{0}}$.
- Take $\mathbf{y} = b_{1,1}\mathbf{v}_1 + \cdots + b_{1,t}\mathbf{v}_t + b_{1,0}\mathbf{v}_{t+1} \in \mathcal{L} \qquad (\tau_1 = \rho^{\mathbf{b}_1})$

Case: $\mathfrak{p}_\ell$ complex

$$\mathbf{y} = b_{1,1}\mathbf{v}_1 + \cdots + b_{1,t-1}\mathbf{v}_{t-1} + b_{1,t}\mathbf{v}_t + b_{1,0}\mathbf{v}_{t+1}$$

$$= \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,t-1} & \Phi_1 & \Phi_2 \end{pmatrix}^{\mathsf{T}}$$

- By design, $\Phi_1 + \Phi_2\sqrt{-1}$ is "close" to $C \log \tau_1$.

$$\begin{aligned} m_{\mathcal{L},\mathbf{0}}^2 \leq ||\mathbf{y}||^2 &= \sum_{j=1}^{t-1} b_{1,j}^2 + \left|\Phi_1 + \Phi_2\sqrt{-1}\right|^2 \\ &\leq tK_0^2 + (twK_0 + C\log\tau_1)^2 \\ &\leq tK_0^2 + (twK_0 + 2C\exp(-c_{13}B))^2 \end{aligned}$$

- If $m_{\mathcal{L},\mathbf{0}} \gg twK_1^2$, this is a stronger constraint on B:

$$\therefore B \leq K_1(\ell) \approx \frac{1}{c_{13}} \log\left(\frac{2C}{\sqrt{m_{\mathcal{L},\mathbf{0}} - tK_0} - twK_0}\right).$$

Case: $\mathfrak{p}_\ell$ complex

If $m_{\mathcal{L},\mathbf{0}} \gg twK_1^2$,

$$B \leq K_1(\ell) \approx \frac{1}{c_{13}} \log\left(\frac{2C}{\sqrt{m_{\mathcal{L},\mathbf{0}} - tK_0} - twK_0}\right).$$

- WHILE $m_{\mathcal{L},\mathbf{0}} < twK_1^2$:
  - $C \leftarrow 2C$ (changes $\mathcal{L}$)
  - Re-run LLL and re-compute $m_{\mathcal{L},\mathbf{0}}$
- Record new exponent bound $K_1(\ell)$.
- If so inclined, replaced K_0 with $K_1(\ell)$ and run again!

The approach when $\mathfrak{p}_\ell$ is real is similar – slightly different lattice $\mathcal{L}$.

Case: $\mathfrak{p}_\ell$ finite

- Same idea, but we use a different lattice $\mathcal{L}$.

$$\Delta := \log_p \tau_1 = \log_p \mu_0 + \sum_i d_i \log_p \mu_i$$

- $K_{\mathfrak{p}_\ell} = \mathbb{Q}_p(\theta)$. Express Δ in the power basis:

$$\Delta = \Delta_0 + \Delta_1\theta + \Delta_2\theta^2 + \cdots + \Delta_{n-1}\theta^{n-1}$$

- By power series expansion of $\log_p$:

$$\Delta_k = a_{0,k} + \sum_{j=1}^{t-1} d_j a_{j,k}, \qquad a_{j,k} \in \mathbb{Q}_p$$

- By appropriate scaling,

$$\lambda^{-1}\Delta_k = \kappa_{0,k} + \sum_{j=1}^{t-1} d_j \kappa_{j,k}, \qquad \kappa_{j,k} \in \mathbb{Z}_p$$

Case: $\mathfrak{p}_\ell$ finite

- Pick a large u. For $\mathcal{L}$, we take the columns of $\begin{pmatrix} I_{t-1} & O \\ \kappa & p^u I_n \end{pmatrix}$,

  where $\kappa := \begin{pmatrix} \kappa_{1,0} & \cdots & \kappa_{t-1,0} \\ \vdots & & \vdots \\ \kappa_{1,n-1} & \cdots & \kappa_{t-1,n-1} \end{pmatrix}$ "(mod p^u)".

- $\mathbf{y} = -(0, \cdots, 0, \kappa_{0,0}, \cdots, \kappa_{0,n-1})^\intercal$ ("mod p^u") Note: $\mathbf{y} \notin \mathcal{L}$

- Similar to complex case: if $\ell(\mathcal{L}, \mathbf{y}) > t^{\frac{1}{2}} K_0$, we may conclude

$$B < K_1(\ell) \approx (\text{constant}) \cdot u$$

- (If not, $u \leftarrow 2u$ and rerun LLL, etc.)

After the LLL Reduction

- This LLL step is *AMAZING* . . .

$$K_0 \approx 10^{300} \quad \xrightarrow{\text{LLL}} \quad K_1 \approx 4000 \quad \xrightarrow{\text{LLL}} \quad K_1 \approx 300$$

- . . . but not amazing *ENOUGH*, e.g.:

$$K_1 \approx 300, t = 6, w = 2 \quad \Longrightarrow \quad w(2K_1 + 1)^t \approx 4.7 \times 10^{16}.$$

- Need a sieving procedure to execute the final search efficiently.

Sieving against primes away from S

- $d = [K : \mathbb{Q}]$, q splits completely in K, $q \notin \mathfrak{p}$ for all $\mathfrak{p} \in S_{\text{fin}}$.

- $q\mathcal{O}_K = \mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_{d-1}$, each $\mathbb{F}_{\mathfrak{q}_i} \cong \mathbb{F}_q$.

- Set $A_{K,S,q-1} := (\mathbb{Z}/w\mathbb{Z}) \times (\mathbb{Z}/(q-1)\mathbb{Z})^t$.

$$\pi_{q-1} \colon A_{K,S} \to A_{K,S,q-1}$$

- **residue field vector**: For $\tau \in \mathcal{O}_{K,S}^\times$,

$$\mathrm{rfv}_q\, \tau := (\tau + \mathfrak{q}_0, \tau + \mathfrak{q}_1, \ldots, \tau + \mathfrak{q}_{d-1}) \in \mathbb{F}_q^d.$$

Sieving against primes away from S

$$\operatorname{rfv}_q \tau := (\tau + \mathfrak{q}_0, \tau + \mathfrak{q}_1, \ldots, \tau + \mathfrak{q}_{d-1}) \in \mathbb{F}_q^d.$$

- Suppose $\mathbf{a}, \mathbf{b} \in A_{K,S}$ with $\rho^{\mathbf{a}} + \rho^{\mathbf{b}} = 1$. Then:
    - $\operatorname{rfv}_q \rho^{\mathbf{a}} + \operatorname{rfv}_q \rho^{\mathbf{b}} = \mathbf{1} := (1, 1, \ldots, 1) \in \mathbb{F}_q^d$.
    - No entry of $\operatorname{rfv}_q \rho^{\mathbf{a}}$ is 0 or 1.
    - $\operatorname{rfv}_q \rho^{\mathbf{a}}$ is determined by $\pi_{q-1}(\mathbf{a})$.

- rfv_q is not surjective: there might not exist $\mathbf{b}$ such that

$$\operatorname{rfv}_q \rho^{\mathbf{a}} = \mathbf{1} - \operatorname{rfv}_q \rho^{\mathbf{b}}.$$

- Using several q gives a large collection of congruences that the exponent vectors in $\rho^{\mathbf{a}} + \rho^{\mathbf{b}} = 1$ must satisfy.

Outline

What's Good / What's Bad / What's Next

- The Good
  - 100% public and open source
  - Integrated into CoCalc/Sage

In [3]:
```
from sage.rings.number_field.S_unit_solver import *
K.<a> = NumberField(x^2 + 7)
S = K.primes_above(14)
OKSx = K.S_unit_group(S=S)
solve_S_unit_equation(K, S, prec=200)
```

  - Reviewed many times (us, referee(s), Sage submission)
  - Well documented (arXiv:1903.00977, now in *Simons Symposia*)

- The Bad
  - The case $K = \mathbb{Q}$ is handled poorly
  - The current sieve is slow
  - Currently restricted to $\alpha = (1, 1)$, $\mathbf{\Gamma} = \mathcal{O}_{K,S}^\times \times \mathcal{O}_{K,S}^\times$

- Next Steps
  - Many improvements within reach

Planned Improvements

- Best known height bounds on solutions (Győry, 2019) may improve Step 1 bounds
- Taking $K_1 = \max K_1(\ell)$ is inefficient. We can track bounds on each exponent and shrink the search space.
- Use ideas of Smart and Wildanger to eliminate "extreme corners" of the search space.
- Replace the existing sieve with a faster exhaustive search based on Fincke-Pohst.

(These should address both items in blue on the previous slide.)

Smart/Wildanger Decompositions

- Define certain sets of solutions:

$$L := \{\tau \in \boldsymbol{\Gamma} : \tau_0 + \tau_1 = 1\}$$
$$L_H := \{\tau \in L : \tau_i = \rho^{\mathbf{b}_i},\ |\mathbf{b}_i| \leq H\}$$
$$L_H(R) := \{\tau \in L_H : R^{-1} \leq |\alpha|_{\mathfrak{p}} \leq R, \forall\, \mathfrak{p} \in S_{\text{fin}}\}$$

- There are large H, R such that $L = L_H(R)$.

- For $H' \leq H$ and $R' \leq R$,

$$L_H(R) = L_{H'}(R') \cup \bigcup_{j=1}^{4} \bigcup_{\mathfrak{p}\in S} T_{j,\mathfrak{p},H,R,R'}$$

where elements of $T_{i,\mathfrak{p}} := T_{i,\mathfrak{p},H,R,R'}$ are "extreme" with respect to $\mathfrak{p}$ or some exponent on ρ.

Smart/Wildanger Decompositions

$$L_H(R) = L_{H'}(R') \cup \bigcup_{j=1}^{4} \bigcup_{\mathfrak{p} \in S} T_{j,\mathfrak{p}}$$

- "LLL-type" arguments allow us to argue $T_{j,\mathfrak{p}} = \varnothing$. This leads to improvements on each exponent bound $K_1(\ell)$.
- Nonempty? Solutions in $T_{j,\mathfrak{p}}$ still correspond to vectors which ...
  - belong to a lattice generated by an explicit matrix, A, and
  - belong to a "small" ellipsoid.
- The algorithm of Fincke-Pohst can search for all such lattice points.
- Once H and R are sufficiently small, Fincke-Pohst can also search for solutions inside $L_H(R)$!

Other To-Dos

- Allow $\alpha \neq (1,1)$, or $\Gamma_i \neq \mathcal{O}_{K,S}^{\times}$.
- Allow Galois constraints.
- Decompose search into disjoint pieces (for parallelization/pausing).
- Python to Cython where possible.

S-Unit Community

With assistance from:

Norman Danner, Bjorn Poonen, David Roe, Andrew Sutherland, . . .

And support from:

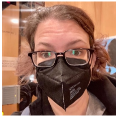
SageDays 62, ICERM, Microsoft Research, Beatrice Yormark Fund for Women in Mathematics, van Vleck Fund @ Wesleyan, . . .

A. Alvarado

A. Koutsianas

B. Malmskog

C. Rasmussen



C. Vincent

M. West

And building on the past work of:

Baker, Baker-Wüstholz, Bremner, Brumer, de Weger, Evertse-Győry, Gelfond, Győry, Győry-Yu, Koutsianas, Lenstra-Lenstra Lovász, Mahler, Malmskog-R., Merriman-Smart, Pethö-de Weger, SageMath Developers, Schneider, Siegel, Smart, Tzanakis-de Weger, Wildanger, Yu, . . .