A general S-unit equation solver and tables of elliptic curves over number fields

Benjamin Matschke

Boston University

Modern Breakthroughs
in Diophantine Problems
BIRS, 2020


Carl Ludwig Siegel


Kurt Mahler

S-unit equations

S-UNIT EQUATIONS

Let

- K be a number field,
- S a finite set of primes of K,
- $\mathcal{O}_K$ the ring of integers of K,
- $\mathcal{O}_{K,S} = \mathcal{O}_K[1/S]$ the ring of **S-integers** of K,
- $\mathcal{O}_{K,S}^\times$ the group of **S-units** of K.

Let $a, b \in K^\times$. **S-unit equation**:

$$\boxed{ax + by = 1, \quad x, y \in \mathcal{O}_{K,S}^\times.}$$

[Siegel], [Mahler]: Finiteness of solution set.

S-UNIT EQUATIONS

Relevance:

- *abc*-conjecture [Masser, Oesterlé]
- many diophantine equations reduce to S-unit equations: Thue-, Thue–Mahler-, Mordell-, generalized Ramanujan–Nagell- equations, index form equations; Siegel method for superelliptic equations
- asymptotic Fermat over number fields [Freitas, Kraus, Özman, Şengün, Siksek]
- tables of (hyper-)elliptic curves over number fields [Parshin, Shafarevich, Smart, Koutsianas]

Classical approaches

Classical algorithms:

- $/\mathcal{O}_{\mathbb{Q},S}^{\times}$ [de Weger]
- $/\mathcal{O}_{K}^{\times}$ [Wildanger]
- $/\mathcal{O}_{K,S}^{\times}$ [Smart]

1. Initial height bound: $h(x), h(y) \leq H_0$ (via bounds in linear forms in logarithms [Baker], [Yu])
2. Reduction of local height bounds "via LLL".
3. Sieving.
4. Enumeration of tiny solutions.

New ideas

1. Efficient estimates (e.g. no unnecessary norm conversions).
2. Refined sieve [von Känel–M.]/$\mathbb{Q}$: Sieve with respect to several places.
   $\rightsquigarrow$ Can be extended/K.
3. Fast enumeration [von Känel–M.]/$\mathbb{Q}$.
   $\rightsquigarrow$ Can be extended/K!
4. Separate search spaces for ax, $1 - ax$, $1/(1 - ax)$, $1 - 1/(1 - ax)$, $1 - 1/ax$, $1/ax$.
5. Optimize ellipsoids (extending on Khachiyan's ellipsoid method).
6. Constraints (e.g. Galois symmetries, if possible).
7. More efficient handling of torsion.
8. Timeouts.
9. Generic code, suitable for extensions.

Difficulty: Balancing.

Comparison of S-unit equation solvers

Comparison with

- [von Känel–M.]: $x+y=1$ over $\mathbb{Q}$.
- [Alvarado-Koutsianas–Malmskog–Rasmussen–Vincent–West]: $x+y=1$ over K.

Comparison for $x+y=1$ over $\mathbb{Q}$:

Solver	$\{2\}$	$\{2,3\}$	$\{2,3,5\}$	$\{2,3,5,7\}$	$\{2,3,5,7,11\}$
[vKM]	0.01 s	0.03 s	0.12 s	0.3 s	1.0 s
[AKMRVW]	0.1 s	23 min	$>$ 30 days (7.2 GB)		
[M.]	1.8 s	3.0 s	6.2 s	15.4 s	47 s

Comparison for $x+y=1$ over $S=\{\text{primes above } 2,3\}$:

Solver	$K=\mathbb{Q}[x]/(x^6-3x^3+3)$
[AKMRVW]	$3.6\cdot 10^{17}$ candidates left
[M.]	29 s

Elliptic curves over number fields

Elliptic curves over number fields

Goal: Compute all elliptic curves$/K$ with good reduction outside of S.

Approach: [Parshin, Shafarevich, Elkies, Koutsianas]

- Write $\quad E : y^2 = x(x-1)(x-\lambda) \quad$ (Legendre form).
- $\lambda + (1-\lambda) = 1 \quad$ ($\widetilde{S}$-unit equation over $L = K(E[2])$)
- Set of possible $K(E[2])$ is finite, computable via Kummer theory.

[Koutsianas]:

- $K = \mathbb{Q}$ and $S = \{2, 3, 23\}$
- $K = \mathbb{Q}(i)$ and $S = \{\text{prime above } 2\}$

ELLIPTIC CURVES OVER NUMBER FIELDS

Disclaimer: $*$ will refer to:

- assuming GRH
- modulo a bug in UnitGroup (Sage 9.0/9.1, using Pari 2.11.2), which I detected only through heuristics. Fixed in Pari 2.11.4, soon in Sage 9.2.
- modulo computations in Magma (proprietary, closed-source).

Elliptic curves/$\mathbb{Q}$

All elliptic curves/$\mathbb{Q}$ with good reduction outside the first n primes:

- $n = 0$: attributed to Tate by [Ogg]
- $n = 1$: [Ogg]
- $n = 2$: [Coghlan], [Stephens]
- $n = 3, 4, 5$: [von Känel–M.],
  recomputed by [Bennett–Gherga–Rechnitzer]
- $n = 6$: [Best–M.] (heuristically)
- $n = 7, 8$: [M.]*

Number of curves: $217,923,072$.
Maximal conductor: $N = 162,577,127,974,060,800$.

Elliptic curves over number fields

Same over number fields:

All* elliptic curves/K with good reduction outside S [M.]:

- $K = \mathbb{Q}(i)$, $S = \{\text{primes above } 2, 3, 5, 7, 11\}$.
- $K = \mathbb{Q}(\sqrt{3})$, $S = \{\text{primes above } 2, 3, 5, 7, 11\}$.
- Many fields K, $S = \{\text{primes above } 2\}$, including one of $\deg K = 12$.

Corollary ([M.])

All elliptic curves/K with* <u>*everywhere good reduction*</u> *for all K with*

$$|\mathrm{disc}(K)| \leq 20000.$$

Elliptic curves/$\mathbb{Q}$

Cremona's DB: $\boxed{N \leq 500,000.}$

[von Känel–M.]: $\boxed{\text{radical}(N) \leq 1,000.}$

[M.]:* $\boxed{\text{radical}(2N) \leq 1,000,000.}$

Comparison:

- Cremona's table $\subset$ [M.].
- $\text{radical}(2N) \leq 30$ requires curves with $N = 1,555,200$.
- Maximal conductor: $N = 1,727,923,968,836,352$.

Alternative approach to compute elliptic curves via Thue–Mahler equations [Bennett–Gherga–Rechnitzer]. Together with Gherga, von Känel, Siksek, we are working on a new Thue–Mahler solver; one goal is to extend Cremona's DB.

Conjectures

abc-conjecture:

$$\limsup_{gcd(a,b)=1} \frac{\log \max(a,b,a+b)}{\log \mathrm{radical}(ab(a+b))} \leq 1.$$

Szpiro's conjecture:

$$\limsup_{E/\mathbb{Q}} \frac{\log |\Delta_E|}{\log N} \leq 6.$$

Conjecture 1: (updated)

$$\limsup_{j\in\mathbb{Q}} \inf_{\substack{E/\mathbb{Q}:\\ j(E)=j}} \frac{\log |\Delta_E|}{\log \mathrm{radical}(N)} \leq 6$$

Thank you

OMISSIONS

S-unit equations:

- Height bounds via linear forms in logarithms: [Baker], [Yu], [Győry–Yu]
- Height bounds via modularity: [von Känel], [Murty–Pasten], [von Känel–M.], [Pasten]
- Number of solutions: [Győry], [Evertse],
- Algorithms: [Tzanakis–de Weger],
- Finiteness (+ algorithms?): [Faltings], [Kim], [Corwin–Dan-Cohen], [Lawrence–Venkatesh]

Elliptic curve tables:

- [Setzer], [Stroeker], [Agrawal–Coates–Hunt–van der Poorten], [Takeshi], [Kida], [Stein–Watkins], [Cremona–Lingham], [Cremona], [Bennett–Gherga–Rechnitzer], [LMFDB], . . .
- Frey–Hellegouarch curves: Reduce S-unit equations to elliptic curve tables.