Solving the $S$-unit equation in Sage

Mckenzie West
Kalamazoo College

July 3, 2018

joint with

Alejandra Alvarado  Angelous Koutsianas  Beth Malmskog
Eastern Illinois University  Ulm University  Villanova University

Christopher Rasmussen  Christelle Vincent
Wesleyan University  University of Vermont
Goal
Have Sage solve the equation \( x + y = 1 \) in an *infinite family of rational numbers* the \( S \)-units.

Idea
The \( S \)-integers are

\[
\text{integers where we're allowed to divide by some primes.}
\]

Definition
Let \( S = \{p_1, \ldots, p_n\} \), a finite set of primes. Define the \( S \)-integers

\[
\mathcal{O}_S := \{a/b : a, b \in \mathbb{Z}, \gcd(a, b) = 1, b = p_1^{e_1} \cdots p_n^{e_n}\}
\]

The \( S \)-units are the units \( \mathcal{O}_S^\times \).
Example

\[ S = \{2, 3\}, \quad \mathcal{O}_S^\times = \{(-1)^a 2^{e_1} 3^{e_2}\} \]

Sage - trac ticket #22148
(Alvarado, Koutsianas, Malmskog, Rasmussen, Vincent, W.)

```python
sage: K.<a> = NumberField(x)
....: S = (K.ideal(2), K.ideal(3))
....: %time solns = solve_S_unit_equation(K, S)
CPU times: user 24min 15s, sys: 10.6 s, total: 24min 26s
Wall time: 24min 17s
sage: len(solns)
11```

Why??

- (Original Motivation) Classify Picard curves over $\mathbb{Q}$ with good reduction away from 3
- Sums of products of primes
- Finitely generated subgroups of $\mathbb{C}^\times$
- Recurrence sequences of complex or algebraic numbers
- Irreducible polynomials and arithmetic graphs
- Decomposable form equations (Thue-Mahler equations)
- Algebraic number theory
- Transcendental number theory
S-unit Structure

\[ S = \{ p_1, \ldots, p_n \} \]
\[ \mathcal{O}_S^\times = \{ (-1)^a p_1^{e_1} \cdots p_n^{e_n} : e_1, \ldots, e_n \in \mathbb{Z} \} \].

“Theorem” (Hasse)

\[ \mathcal{O}_S^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^n \]

Theorem (Baker-Wüstholz, Smart, Pethö-de Weger)

Finitely many pairs \((\tau_0, \tau_1) \in \mathcal{O}_S^\times\) satisfy \(\tau_0 + \tau_1 = 1\).

Proof.

A bound on the exponents exists.
Preliminary bound

\[ \sigma + \tau = 1 \]
\[
\sigma = (-1)^a p_1^{e_1} \cdots p_n^{e_n} \quad \tau = (-1)^b p_1^{f_1} \cdots p_n^{f_n}
\]
\[ H = \max\{|e_1|, \ldots, |e_n|, |f_1|, \ldots, |f_n|\} \]

Baker-Wüstholz

\[ \log |\sigma| = e_1 \log(p_1) + \cdots + e_n \log(p_n) > e^{-c_4 \log(H)} \]

Smart

\[ \log |\sigma| < c_5 e^{-c_6 H} \]

\[ c_4 \log(H) > - \log(c_5) + c_6 H \]
Pethö-de Weger

There is a constant $K_0$ such that

$$\max(|\text{exponents}|) < K_0$$

Bad News

The $K_0$ constructed this way are HUGE.
Example \[ S = \{2, 3\}, \quad \mathcal{O}_S^\times = \{(-1)^a 2^{e_1} 3^{e_2}\} \]

```
sage: K.<a> = NumberField(x)
....: S = (K.ideal(2), K.ideal(3))
....: Sunits = UnitGroup(K, S=S)
....: %time K0_func(Sunits, [1,-1])
CPU times: user 232 ms, sys: 8 ms, total: 240 ms
Wall time: 237 ms
7.150369969667384570286131254306e17
```
LLL Reduction

LLL allows us to construct a significantly “better” basis.

LLL uses the Gram Schmidt process but restricts to a lattice.

The perk of LLL is that it acts like magic to reduce our bound!

****IN POLYNOMIAL TIME****
Example

$$S = \{2, 3\}, \quad \mathcal{O}_S^\times = \{(-1)^a 2^{e_1} 3^{e_2}\}$$

sage: K.<a> = NumberField(x)
....: S = (K.ideal(2), K.ideal(3))
....: Sunits = UnitGroup(K, S=S)
....: K0_func(Sunits, [1,-1])
7.150369969667384570286131254306e17
....: cx_LLL_bound(Sunits, [1,-1])
CPU times: user 568 ms, sys: 24 ms, total: 592 ms
Wall time: 575 ms
30
Baker bound and standard LLL only guaranteed to work if the maximum exponent occurs at an infinite prime. i.e. The absolute value is bigger than the exponents. 

Malmskog–Rasmussen: We can assume this is true if $S$ contains but one finite prime.

Yu: There is a $p$-adic Baker bound that works for this finite place.

Koutsianas: Coded Yu’s bound as part of his PhD work.
Example

\[ S = \{2, 3\}, \ O_S^\times = \{(-1)^a2^{e_1}3^{e_2}\} \]

```python
sage: K.<a> = NumberField(x)
....: S = (K.ideal(2), K.ideal(3))
....: Sunits = UnitGroup(K, S=S)
....: v = K.places()[0]
....: %time K1_func(Sunits, v, [1,-1])
CPU times: user 100 ms, sys: 0 ns, total: 100 ms
Wall time: 95.3 ms
2.20465029120522566538006217583e15
sage: p_adic_LLL_bound(Sunits, [1,-1])
CPU times: user 1.65 s, sys: 20 ms, total: 1.67 s
Wall time: 1.68 s
52```
Now that we have an upper bound, what are the actual solutions?

$$\max(|\text{exponents}|) \leq H = 52$$

The number of pairs \((\sigma, \tau)\) in this range is:

$$\frac{(2H + 1)^{2n}}{2} = \frac{(2(52) + 1)^4}{2} \approx 6.7 \times 10^7$$

Time to be creative!
Preliminary steps

Let $q \in \mathbb{Z}$ be a prime such that $q \not\in S$. Then $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_q$, and we can define

$$\Phi_q : \mathcal{O}_S^\times \rightarrow \mathbb{F}_q^\times$$

$$\sigma \mapsto \sigma \pmod{q}.$$

Notice that if $\sigma, \tau \in \mathcal{O}_S^\times$ such that $\sigma + \tau = 1$ then

$$\Phi_q(\sigma) + \Phi_q(\tau) = 1.$$

Let $Y_q \subseteq \mathbb{F}_q^\times$ be the intersection of the image of $\Phi_q$ with the solutions to $x + y = 1$ in $\mathbb{F}_q^\times$. 
\[ \mathcal{O}_S^\times = \{(-1)^a p_1^{e_1} \cdots p_n^{e_n}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^n, \quad q \in \mathbb{Z} \setminus S \]

\[ Y_q = \text{im}(\Phi_q) \cap \text{solutions} \]

S-units \quad \mathcal{O}_S^\times \quad \Phi_q \quad \mathbb{F}_q^\times

Exponent Vectors \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^n \quad \Psi_q

\[ \alpha \in \mathbb{F}_q^\times \Rightarrow \alpha^{q-1} = 1 \]

New Vertical Map: Take exponent vectors modulo \( q - 1 \)
Sieve

\[ \mathcal{O}_S^\times \xrightarrow{\Phi_q} \mathbb{F}_q^\times \supseteq Y_q \]

\[ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^n \xrightarrow{\Psi_q} (\mathbb{Z}/(q-1)\mathbb{Z})^{n+1} \]

\[ \Xi_q \]

\[ X_q = \text{all possible vectors mod } q - 1 \]
Narrowing using $X_q$ and $Y_q$

\[
X_q \subseteq (\mathbb{Z}/(q - 1)\mathbb{Z})^{n+1} \quad \Xi_q \quad \mathbb{F}_q^\times \supseteq Y_q
\]

Definitions

- Two vectors $x, x' \in X_q$ are complementary if
  \[
  \Xi_q(x) + \Xi_q(x') = 1.
  \]

- Let $r$ be another prime not in $S$. The vectors $x \in X_q$ and $x' \in X_r$ are compatible if there is a $y \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^n$ s.t.
  \[
  y \equiv x \pmod{q - 1} \text{ and } y \equiv x' \pmod{r - 1}.
  \]

Next Step: Do complementary and compatibility check for all $x \in X_q$ and drop them as we go.
We have solutions!

\[ S = \{2, 3\}, \quad O_S^\times = \{(-1)^a 2^{e_1} 3^{e_2}\} \]

Sage - trac ticket #22148
(Alvarado, Koutsianas, Malmskog, Rasmussen, Vincent, W.)

```
sage: K.<a> = NumberField(x)
....: S = (K.ideal(2), K.ideal(3))
....: %time solns = solve_S_unit_equation(K, S)
CPU times: user 24min 15s, sys: 10.6 s, total: 24min 26s
Wall time: 24min 17s
sage: len(solns)
11
```
Solutions

\[ S = \{2, 3\}, \quad O_S^\times = \{(-1)^a 2^{e_1} 3^{e_2}\} \]

\[
\text{sage: solns}
[[0, -1, 1], (1, -1, 0), 3/2, -1/2],
[(0, 1, 0), (1, 0, 0), 2, -1],
[(0, 0, -1), (0, 1, -1), 1/3, 2/3],
[(1, 1, 0), (0, 0, 1), -2, 3],
[(0, 2, 0), (1, 0, 1), 4, -3],
[(0, 0, -2), (0, 3, -2), 1/9, 8/9],
[(1, 0, -1), (0, 2, -1), -1/3, 4/3],
[(0, -2, 1), (0, -2, 0), 3/4, 1/4],
[(0, 0, 2), (1, 3, 0), 9, -8],
[(1, -3, 0), (0, -3, 2), -1/8, 9/8],
[(0, -1, 0), (0, -1, 0), 1/2, 1/2]]
A Larger Number Field

```python
sage: K.<xi> = NumberField(x^2+x+1)
....: S = K.primes_above(3)
....: %time solve_S_unit_equation(K,S)
CPU times: user 872 ms, sys: 56 ms, total: 928 ms
Wall time: 1.81 s

[[(2, 1), (4, 0), xi + 2, -xi - 1],
 [(5, -1), (4, -1), 1/3*xi + 2/3, -1/3*xi + 1/3],
 [(5, 0), (1, 0), -xi, xi + 1],
 [(1, 1), (2, 0), -xi + 1, xi]]
```
Thus taking $\mathbb{Q}(\xi)$ to be the number field defined by $x^2 + x + 1$, and $S = \{p_1, p_2\}$ where $p_1p_2 = (3)$, the solutions to $x + y = 1$ in $\mathcal{O}_S^\times$ are:

$$(\xi + 2, -\xi - 1), \left(\frac{1}{3}\xi + \frac{2}{3}, -\frac{1}{3}\xi + \frac{1}{3}\right), (-\xi, \xi + 1), \text{ and } (-\xi + 1, \xi).$$