A ROBUST IMPLEMENTATION FOR SOLVING THE $S$-UNIT EQUATION AND SEVERAL APPLICATIONS

ALEJANDRA ALVARADO, ANGELOS KOUTSIANAS, BETH MALMSKOG, CHRISTOPHER RASMUSSEN, CHRISTELLE VINCENT, AND MCKENZIE WEST

Abstract. Let $K$ be a number field, and $S$ a finite set of places in $K$ containing all infinite places. We present an implementation for solving the $S$-unit equation $x + y = 1$, $x, y \in \mathcal{O}_K^\times$ in the computer algebra package SageMath. This paper outlines the mathematical basis for the implementation. We discuss and reference the results of extensive computations, including exponent bounds for solutions in many fields of small degree for small sets $S$. As an application, we prove an asymptotic version of Fermat’s Last Theorem for totally real cubic number fields with bounded discriminant where 2 is totally ramified. In addition, we improve bounds for $S$-unit equation solutions that would allow enumeration of a certain class of genus 2 curves, and use the implementation to find all solutions to some cubic Ramanujan-Nagell equations.

1. Introduction

In 1909, Thue proved there are only finitely many integral solutions to what we now call the Thue equation; i.e, that for any $\mathbb{Q}$-irreducible binary form $F(X,Y)$ of degree at least 3, defined over the integers, there are only finitely many solutions $(x,y) \in \mathbb{Z}^2$ to the equation

$$F(x, y) = c,$$

where $c$ is any non-zero integer $^{[39]}$. Thue accomplished this by formally factoring $F$ into linear terms of the form $(x - \alpha y)$, where $\alpha$ is algebraic, then bounding the quality of rational approximations of $\alpha$ in terms of the size of $x$ and $y$. Thus bounds on integer solutions to the Thue equation arose out of the theory of approximating algebraic numbers by rationals. Thue’s theorem was generalized by Siegel $^{[34]}$ and then Mahler $^{[24]}$. These generalizations gave rise to a central fact of modern computational number theory: if $K$ is a number field, and $S$ a finite list of places of $K$ including all infinite places, then there are

$^{1}$See also the recent translation $^{[16]}$ by Fuchs.
only finitely many solutions \((x, y)\) to the equation
\[(1) \quad x + y = 1, \quad x, y \in \mathcal{O}_{K,S}^\times.\]
Here, \(\mathcal{O}_{K,S}^\times\) is the unit group of the ring \(\mathcal{O}_{K,S}\) of \(S\)-integers in \(K\). We refer to (1) as the \(S\)-unit equation. More generally, for fixed \(a, b \in \mathcal{O}_{K,S}\), the equation \(ax + by = 1\) is known to have only finitely many solutions, and can be solved with similar methods, but we focus on (1) for the present. In this paper, we describe an algorithm to determine the complete set of solutions to the \(S\)-unit equation for general \(K\) and \(S\).

The work of Gelfond and Schneider, resolving Hilbert’s seventh problem in the affirmative (all irrational algebraic powers of algebraic numbers are transcendental once trivial cases are ignored), determined lower bounds on the absolute value of a \(\mathbb{Q}\)-linear combination of two \(\mathbb{Q}\)-linearly independent logarithms of algebraic numbers. Alan Baker’s 1967 theorem \([1]\) generalized these results to the case of many logarithms. Baker, Wüstholz, and many others continued to improve these bounds. Naturally, one should ask if similar results are available over local fields, and indeed such results began to appear quickly. In 1968, Brumer proved the first analogue of Baker’s work for \(p\)-adic logarithms \([7]\), followed by many improvements and generalizations, such as the results of Yu \([44]\). Improvements in both the archimedean and nonarchimedean cases continue to appear, such as in \([19, 3, 47, 18]\).

For any choice of \(K\) and \(S\), \(\mathcal{O}_{K,S}^\times\) is a finitely generated \(\mathbb{Z}\)-module. Fixing a basis \(\rho_1, \ldots, \rho_t\) for the torsion free part, we can express any \(x \in \mathcal{O}_{K,S}^\times\) as \(x = \xi \cdot \prod_{i=1}^{t} \rho_i^{a_i}\) for some root of unity \(\xi \in K\) and some \(a_i \in \mathbb{Z}\). Building on the lower bounds for linear combinations of logarithms, Győry \([17]\) determined effectively computable bounds for the exponents \(a_i\). This was a great victory for computational number theory, as this provably restricted all solutions to (1) to a finite search space. Unfortunately, the demonstrated bounds were enormous and as a matter of practice, it was computationally infeasible to conduct an exhaustive search for solutions, even in the very simplest cases. However, in \([13]\), de Weger developed a method of algorithmically reducing the bounds to a manageable size, relying on the lattice basis reduction algorithm of Lenstra, Lenstra, and Lovász \([23]\) (henceforth referred to as the “LLL algorithm”). Though it is has not been proven that de Weger’s method will always reduce the bounds coming from the results in linear forms of logarithms, this is the rule in practice. In many cases, de Weger’s approach provides sufficient improvements that, with careful sieving (or sometimes even with only brute force), the entire search space can be exhausted and complete lists of solutions can be enumerated.
Beyond the improvements provided by LLL-based reduction, many mathematicians have developed further algorithms for efficiently searching below the “LLL bounds” provided by de Weger’s work. Two powerful examples are reported in [13] and [38]. Increasingly, the theoretical improvements (assisted by technological improvements) have pushed ambitious and interesting computational problems within reach. For example, Smart determined the entire set of all genus 2 curves over $\mathbb{Q}$ with good reduction away from 2, based in part on solving (1) for a family of number fields unramified away from 2 [36].

We have written a package of Python functions for inclusion in the computer algebra system SageMath [32], which solves the $S$-unit equation (1) over any number field $K$ and for any finite set $S$ of finite places. As experienced readers may expect, the package is not practical when either $[K : \mathbb{Q}]$ or $|S|$ is too large, although there is no theoretical obstruction. While this package is the independent creation of the authors, it is based in part on the descriptions of algorithms implemented by Smart [35, 36]. To the authors’ knowledge, our package is the first publicly available implementation for solving the $S$-unit equation over any field other than $\mathbb{Q}$; the present article describes the algorithm and its implementation. The implementation was a highly non-trivial undertaking, involving efforts spreading over more than five years on the parts of individuals and the entire team.

We also provide new results facilitated by our implementation. In particular, we first provide a discussion of and link to explicit exponent bounds for solutions of the $S$-unit equation in all cases $(K,S)$ where $K/\mathbb{Q}$ is ramified only at primes above some subset of $\{2,3\}$ and $2 \leq [K : \mathbb{Q}] \leq 5$, $S \subseteq \{p \subseteq \mathcal{O}_K : p \mid 6\}$.

We improve the best known exponent bounds for solutions of the $S$-unit equation over number fields related to a class of genus 2 curves over $\mathbb{Q}$ with good reduction away from 3. We solve the $S$-unit equation in the 13 totally real cubic number fields $K$ in which 2 is totally ramified and the absolute discriminant of $K$, $\Delta_K$, satisfies $|\Delta_K| \leq 2000$, and we use these results to verify that an asymptotic version of Fermat’s Last Theorem holds over these fields. Finally, we find all solutions to certain cubic Ramanujan-Nagell equations.

1.1. Overview. The organization of the paper proceeds as follows. We introduce certain notations in §2. In §3, we review the relevant work of Baker and Yu; this is necessary to establish a “pre-LLL” exponent bound for each place in $S$. In §4, we explain the process of
using LLL to reduce these exponent bounds – the approach is different for archimedean and nonarchimedean places. In §5, we describe the sieve for further constraining the final search space. We devote §6 to a discussion of our experimental observations, having now executed our algorithm in several dozen cases. We highlight a special condition ($S$ contains only one finite place) under which a significant improvement in the search space can be obtained. Although narrow in scope, the special condition is sufficiently natural, and the savings sufficiently nontrivial, as to warrant its discussion. In §7, we report several results on exponent bounds and explicit solutions. Finally, §8 introduces examples of applications: an asymptotic version of Fermat’s Last Theorem over totally real cubic fields, a reduction of bounds for search spaces for curves of genus 2 with good reduction away from 3, and a solution to a cubic variant of the Ramanujan-Nagell equation.

Acknowledgments. We are delighted to recognize the Institute for Computational and Experimental Research in Mathematics for both funding and hosting a 2017 collaboration during which a great deal of this project was completed. Part of this work began at the 2014 workshop SageDays 62, and we would like to thank Anna Haensch and Lola Thompson for organizing that workshop and Microsoft Research and The Beatrice Yormark Fund for Women in Mathematics for funding. Some of the work was supported by the van Vleck fund at Wesleyan University. The authors would like to thank many people for helpful conversations that led to improvements in the code and gave direction to this project, including Bjorn Poonen, Andrew Sutherland, and Norman Danner. We would also like especially to thank David Roe for his contributions to refining and reviewing the code for inclusion in SageMath. The third author was partially supported in this work by NSA Grant #H98230-16-1-0300.
2. Notation

2.1. S-units in number fields. Unless stated otherwise, we fix the following notation throughout:

- $K$ a number field (i.e., a finite extension of $\mathbb{Q}$)
- $d_K$ the absolute degree $[K : \mathbb{Q}]$
- $\omega$ the number of distinct roots of unity in $K$
- $\Delta_K$ the absolute discriminant of $K/\mathbb{Q}$
- $\mathcal{O}_K$ the ring of integers of $K$
- $f_p$ the inertial degree of the prime $p \subseteq \mathcal{O}_K$ over the rational prime $p$ intersecting $\mathbb{Z}$
- $r$ the rank of $\mathcal{O}_K^\times$ as a $\mathbb{Z}$-module
- $S_{\text{st}}$ a set $\{p_1, \ldots, p_s\}$ of $s$ finite places of $K$
- $S_{\infty}$ the set of all infinite places of $K$
- $S = S_{\text{st}} \cup S_{\infty}$
- $\mathcal{O}_{K,s}$ the ring of $S$-integers in $K$
- $\mathcal{O}_{K,s}^\times$ the group of $S$-units in $K$
- $t$ the rank of $\mathcal{O}_{K,s}^\times$ as a $\mathbb{Z}$-module (so $t = r + s$)
- $\rho_0$ a root of unity generating the torsion part of $\mathcal{O}_{K,s}^\times$
- $\rho_1, \ldots, \rho_t$ an ordered basis for the free $\mathbb{Z}$-module $\mathcal{O}_{K,s}^\times$
- $\rho$ the ordered list $[\rho_0, \rho_1, \ldots, \rho_t]$

For a nonzero prime ideal $p \subseteq \mathcal{O}_K$, we let $\text{ord}_p$ denote the ordinal function for $p$; for any nonzero $\beta \in \mathcal{O}_K$, $\text{ord}_p(\beta) = m$ if $\beta \in p^m - p^{m+1}$. The function $\text{ord}_p$ is extended to $K$ in the obvious way. If $f(x) \in \mathbb{Z}[x]$ is a monic and irreducible polynomial, we let $K_f$ denote the number field $\mathbb{Q}(\xi)$, where $\xi$ is a root of $f(x)$.

2.2. Solutions to the S-unit equation. We let $A_{K,s}$ denote the additive $\mathbb{Z}$-module $(\mathbb{Z}/w\mathbb{Z}) \times \mathbb{Z}^t$. This is isomorphic to $\mathcal{O}_{K,s}^\times$, and the generating set $\rho$ determines an isomorphism

$$\Phi_\rho : A_{K,s} \longrightarrow \mathcal{O}_{K,s}^\times, \quad a := (a_0, a_1, \ldots, a_t) \mapsto \prod_{i=0}^t \rho_i^{a_i}.$$

We use the shorthand $\rho^a := \Phi_\rho(a)$. For obvious reasons, we call the elements of $A_{K,s}$ exponent vectors. Much of our discussion will focus on bounds for the entries of an exponent vector. For $a \in A_{K,s}$, we use the notation $|a| \leq B$ to signify

$$\max_{0 \leq i \leq t} |a_i| \leq B.$$
Within $O_{K,S}^\times$, we wish to determine
\[ X_{K,S} := \{ \tau \in O_{K,S}^\times : 1 - \tau \in O_{K,S}^\times \}. \]
Solving the $S$-unit equation is equivalent to determining the set $X_{K,S}$.
We let $E_{K,S}$ denote the corresponding subset $\Phi^{-1}(X_{K,S})$ of $A_{K,S}$.

2.3. Absolute values and height functions. Each place of $K$ determines an associated absolute value, $|\cdot|_p$, which we now describe. Let $|\cdot|$ denote the usual absolute value on $C$.

First, if $p$ is a finite place of $K$, let $p \in \mathbb{Q}$ be the unique rational prime below $p$. In this case, we define the absolute value $|\cdot|_p$ on $K$ by
\[ |\alpha|_p := p^{-f_p \cdot \text{ord}_p(\alpha)}. \]

If $p$ is an infinite place of $K$, we let $\sigma_p$ denote an embedding of $K \rightarrow C$ corresponding to $p$. The corresponding absolute value depends on whether $p$ is a real or complex (meaning non-real) place of $K$:
\[ |\alpha|_p := \begin{cases} 
|\sigma_p(\alpha)| & \text{if } p \text{ is real}, \\
|\sigma_p(\alpha)|^2 & \text{if } p \text{ is complex}.
\end{cases} \]

We let $h$ denote the standard logarithmic Weil height on $\mathbb{P}^n(K)$ ($n \geq 1$), defined as follows. For any $x = (x_0 : \cdots : x_n) \in \mathbb{P}^n(K)$,
\[ h(x) = \frac{1}{d_K} \sum_p \log (\max_j \{|x_j|_p\}), \]
where the sum runs over all places of $K$. It is a consequence of the product formula ([20, Ch. 20, pgs. 326–327]) that $h(x)$ is independent of the choice of coordinates for $x$. For any $\alpha \in K$, we take $h(\alpha) = h((1 : \alpha))$. Note that this height is absolute in the sense that it is not dependent on which field extension $K$ containing the coordinates of $x$ is considered.

We introduce modified versions of this height function, used in §3. Suppose $\alpha_1, \ldots, \alpha_n \in K$, and let $K' = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq K$.
For any element $\beta \in K'$, we define the function $h'$ by
\[ h'(\beta) = \frac{1}{d_{K'}} \max \{d_{K'} \cdot h(\beta), |\log \beta|, 1\}. \]

Alternatively, suppose $p$ is a finite place of $K$ over the rational prime $p$, and $p' = p \cap K'$. Let $\mu_N$ denote the set of $N$th roots of unity in $K$.
We set
\[ D = \begin{cases} 
d_{K'} & p > 2 \text{ and } \mu_4 \subseteq K', \\
d_{K'} & p = 2 \text{ and } \mu_3 \subseteq K', \\
2d_{K'} & \text{otherwise}.
\end{cases} \]
Associated to $p'$ we have the height function on $K'$,
\[ h_{p'}(\beta) = \max \left\{ h(\beta), \frac{|\log \beta|}{2\pi D}, \frac{f_{p'} \log p}{d_{K'}} \right\}. \]

2.4. $p$-adic logarithms. As usual, we let $\mathbb{C}_p$ denote the completion of the algebraic closure of $\mathbb{Q}_p$, the $p$-adic field; we let $|\cdot|_p$ denote the natural extension of $|\cdot|_p$ on $\mathbb{Q}_p$ to $\mathbb{C}_p$. On the open disk $\Delta_1 := \{z : |z-1|_p < 1\}$, we define the $p$-adic logarithm by the series
\[ \log_p(z) = -\sum_{n \geq 1} \frac{(1-z)^n}{n}. \]

The series is convergent on $\Delta_1$; moreover, on $\Delta_1$ it satisfies the identity
\[ (2) \quad \log_p(xy) = \log_p(x) + \log_p(y). \]

We also extend $\text{ord}_p$ to $\mathbb{C}_p$ in the standard way. For any number field $K$ and any prime $p \subseteq \mathcal{O}_K$ above $p$, let $e_p$ denote the ramification index of $p$ over $p$. Then $\text{ord}_p$ satisfies
\[ \text{ord}_p \beta = e_p \text{ord}_p \beta, \quad \beta \in K_p. \]

If $|z|_p < p^{-\frac{1}{p-1}}$ we have
\[ \text{ord}_p \left( \log_p(1+z) \right) = \text{ord}_p(z). \]

Based on an idea due to Iwasawa, the $p$-adic logarithm can be extended to any $z \in \mathbb{C}_p$ such that $|z|_p = 1$; this extension continues to satisfy (2) (see [37, II.2.4]).

3. THE EXPONENT BOUNDS OF BAKER AND YU

Suppose $\tau_1, \tau_2 \in \mathcal{O}_{K,S}^\times$ provide a solution to the $S$-unit equation, so that
\[ \tau_1 + \tau_2 = 1. \]

With respect to the ordered generating set $\rho$, there are unique vectors $b_i = (b_{i,0}, \ldots, b_{i,t}) \in A_{K,S}$ such that
\[ \tau_i = \rho^{b_i} = \prod_{j=0}^{t} \rho_j^{b_{i,j}}, \quad i = 1, 2. \]

The techniques of lattice reduction discussed in §4 will not produce an absolute bound for $|b_{i,j}|$ on their own; they can only be used to improve a known bound. So in this section, we recall bounds established by Baker and Yu. Though sharper bounds have been proven in more recent work (e.g. [16]), the algorithm we have constructed follows the approach of Smart [35], using results of Baker-Wüstholz [2] and Yu.
we also rely on some modifications described in \[25\]. An excellent treatment of the background material appears in \[14\].

We present a description of the implemented algorithm, attempting to be as self-contained as possible. To aid the reader, we use the same numbering for the constants that appears in \[35\], referencing the specific results used in the implemented functions.

We begin with a statement of an effective version of Baker’s theorem. Let \(\alpha_1, \ldots, \alpha_n \in K\), and let \(K' \subseteq K\) such that \(K' = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)\). (Notations are as in §2.3.)

**Theorem 3.1** (Baker-Wüstholz, [2, pg. 20]). Let \(L\) be a linear form in \(t + 1\) indeterminates,

\[
L(z_0, \ldots, z_t) = b_0 z_0 + \cdots + b_t z_t, \quad b_i \in \mathbb{Z}.
\]

Let \(B = \max\{|b_0|, \ldots, |b_t|\}\), and let \(\rho_0, \ldots, \rho_t \in \overline{\mathbb{Q}} - \{0, 1\}\). Let \(K'\) be the subfield of \(\overline{\mathbb{Q}}\) generated by the \(\rho_i\). If \(B > 3\) and

\[
\Lambda = L(\log \rho_0, \log \rho_1, \ldots, \log \rho_t) \neq 0,
\]

then

\[
\log |\Lambda| > -C(t, d_{K'}) \log(B) \prod_{j=0}^t h'(\rho_j),
\]

where the constant \(C(t, d_{K'})\) is defined by

\[
C(t, d_{K'}) = 18(t + 2)!/(t + 1)^{(t+2)}(32d_{K'})^{(t+3)} \log (2(t + 1)d_{K'}) .
\]

Note that we may be sure \(\Lambda \neq 0\) if the set \(\{\log \rho_i\}\) is linearly independent over \(\mathbb{Q}\).

We now describe a similar result for \(p\)-adic logarithms. The original reference for this result is \[45\] Cor. 1. The version quoted here has slightly improved constants and appears in the appendix of \[40\], as well as \[37\] Thm. A.2. Let \(\mathfrak{p}\) be a finite place of a number field \(K\), and let \(\alpha_1, \ldots, \alpha_n \in K\). Let \(K' \subseteq K\) such that \(K' = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)\).

**Theorem 3.2** (Yu, [40]). Suppose \(\text{ord}_\mathfrak{p}(\alpha_j) = 0\) for all \(1 \leq j \leq n\) and let \(b_i \in \mathbb{Z}\) with \(\prod_{j=1}^n \alpha_j^{b_j} \neq 1\). If \(B = \max\{|b_1|, \ldots, |b_n|\}\), then

\[
\text{ord}_\mathfrak{p} \left( \prod_{j=1}^n \alpha_j^{b_j} - 1 \right) < k_2k_3k_4(\log(B) + k_5),
\]

where the constants \(k_2, k_3, k_4, k_5\) are defined by

\[
\begin{align*}
k_2 &= \frac{18(32d_{K'})^{(t+3)}}{(t + 1)^{(t+2)}}, \\
k_3 &= \frac{18(32d_{K'})^{(t+3)}}{(t + 1)^{(t+2)}} \log (2(t + 1)d_{K'}). \\
k_4 &= 18(32d_{K'})^{(t+3)} \log (2(t + 1)d_{K'}). \\
k_5 &= \frac{18(32d_{K'})^{(t+3)}}{(t + 1)^{(t+2)}}.
\end{align*}
\]
where

$$k_2 = \begin{cases} 
3509 \cdot \left(\frac{45}{7}\right)^n & \text{if } p \equiv 1 \pmod{4}, \\
30760 \cdot (25)^n & \text{if } p \equiv 3 \pmod{4}, \\
197142 \cdot (36)^n & \text{if } p = 2,
\end{cases}$$

$$k_3 = (n + 1)^{2n+4}p^{Df_p/d_K}(f_p \log p)^{-(n+1)}D^{n+2} \prod_{j=1}^{n} h'_p(\alpha_j),$$

$$k_4 = \begin{cases} 
\log (2^{11} \cdot (n + 1)^2D^2H) & \text{if } p > 2, \\
\log (3 \cdot 2^{10} \cdot (n + 1)^2D^2H) & \text{if } p = 2,
\end{cases}$$

$$k_5 = 2 \log D,$$

$$H = \max\{h'_p(\alpha_1), \ldots, h'_p(\alpha_n)\}.$$ 

The theorems of Baker and Yu both provide inequalities of the form “a polynomial function of $B$ is bounded by a polynomial function of $\log(B)$,” which in turn guarantee an absolute bound on $B$. The analysis to determine such a bound explicitly is standard; we will use the following result of Petho and de Weger for this purpose.

**Lemma 3.3** (Petho and de Weger [28, Lemma 2.2]). Suppose the real numbers $a, b, h$ satisfy $a \geq 0$, $h \geq 1$, $b > \left(\frac{e^2}{h}\right)^h$, and let $x \in \mathbb{R}$ be the largest solution to the equation

$$x = a + b(\log x)^h.$$ 

Then

$$x < 2^h \left(a^\frac{1}{h} + b^\frac{1}{h} \log (h^h b)\right)^h.$$ 

### 4. Baker/Yu bounds

**4.1. An upper bound at the extremal place.** Suppose $(\tau_1, \tau_2)$ is a solution to the $S$-unit equation, with $\tau_i$ specified as in (3). We set $B = \max_{i,j} |b_{i,j}|$. Relabeling $\tau_1$ and $\tau_2$ if necessary, we assume $B = |b_{1,j}|$ for some $1 \leq j \leq t$. Recall that $S$ contains precisely $t + 1$ places, $p_1, \ldots, p_{t+1}$. We choose the indices $k, \ell \in \{1, 2, \ldots, t + 1\}$ so that

$$|\log |\tau_1|_{p_k}| = \max_{p \in S} |\log |\tau_1|_p|, \quad |\tau_1|_{p_\ell} = \min_{p \in S} |\tau_1|_p.$$ 

For any choice of $U := \{u_1, \ldots, u_t\} \subseteq S$ define the $t \times t$ matrix

$$M = (m_{i,j}), \quad m_{i,j} = \log |\rho_j|_{u_i}.$$
One may always choose $U$ so that $M$ is invertible (see [14, §5.1]), and so we assume this is the case. We have

$$
\begin{pmatrix}
  b_{1,1} \\
  b_{1,2} \\
  \vdots \\
  b_{1,t}
\end{pmatrix} = M^{-1} \begin{pmatrix}
  \log |\tau_1|_{u_1} \\
  \log |\tau_1|_{u_2} \\
  \vdots \\
  \log |\tau_1|_{u_t}
\end{pmatrix}.
$$

Let $\|M\|$ be the row norm of $M^{-1}$, i.e. $\|M\| = \max_i \sum_{j=1}^t |m_{i,j}|$, and set $c_1 := \max \left\{ \|M\| : M \text{ is invertible} \right\}$

Then $B \leq c_1 |\log |\tau_1|_{p_k}|$. We define

$$
c_2 := \frac{1}{c_1} \quad \quad c_3 := \frac{0.9999999c_2}{r + s}.
$$

By [35] Lemma 1, we have

$$(4) \quad |\tau_1|_{p_\ell} \leq e^{-c_3 B}.$$ 

**Remark 4.1.** In the sequel, we number our constants in an effort to stay consistent with the enumeration given in Smart’s paper [35]. There, Smart considers a more general unit equation, and so introduces certain constants $c_4(i)$, $c_6(i)$, $c_7(i), \ldots$ whose values are trivial in the present application. So while the alert reader may notice gaps in the enumeration of constants, this is intentional. (Adjusting our implementation to the more general setting is not difficult, but we are satisfied to limit the discussion to match the current state of the implementation.)

Regardless, we now have an upper bound on $|\tau_1|_{p_\ell}$ in terms of $B$. We next establish a lower bound, also involving $B$, which will force a limit on the size of $B$. The precise argument depends on whether $p_\ell$ is a finite or infinite place. For the purposes of the algorithm, we must compute this bound on $B$ for each possible index $1 \leq \ell \leq t$; we have no choice but to take the largest possible bound, i.e., the larger of the two values $K_0$ and $K_1$ determined in the remainder of this section.

4.2. **Case I: $p_\ell$ is finite.** If $p_\ell$ is finite, then let $p_\ell$ also denote the associated prime ideal in $O_K$. Let $p$ be the prime of $\mathbb{Z}$ lying below $p_\ell$, and let $e_\ell$ and $f_\ell$ denote the ramification index and inertial degree of $p_\ell$ over $p$, respectively. From (4) we have

$$N_{K/Q}(p_\ell)^{-\ord_{p_\ell}(\tau_1)} \leq e^{-c_3 B}.$$
Consequently,
\[
\text{ord}_{p_\ell}(\tau_1) \geq \frac{c_3 B}{\log N_{K/Q}(p_\ell)}.
\]

We define
\[
c_5(\ell) := \frac{c_3}{e_\ell \log N_{K/Q}(p_\ell)}.
\]

We then have
\[
\text{ord}_{p_\ell}(\tau_1) \geq e_\ell c_5(\ell) B.
\]

Excepting the trivial case \( B = 0 \), we have \( \text{ord}_{p_\ell}(\tau_1) > 0 \). Thus \( \text{ord}_{p_\ell}(\tau_2) = 0 \), since \( \tau_1 + \tau_2 = 1 \). As at least one of the generators \( \rho_i \) lies in the ideal \( p_\ell \), it must be possible to determine \( \mu_i \in K, 0 \leq i \leq t - 1 \), such that
\[
\tau_2 = \mu_0 \prod_{i=1}^{t-1} \mu_i^{d_i}, \quad |d_i| \leq B.
\]

These \( \mu_i \) are derived from the \( \rho_i \) in such a way as to force \( \text{ord}_{p_\ell}(\mu_i) = 0 \) for all \( i \) [824-825]. Theorem 3.2 now applies, and we obtain constants \( c_8(\ell) \) and \( c_9(\ell) \) such that
\[
\text{ord}_{p_\ell}(\tau_1) = \text{ord}_{p_\ell}(\tau_2 - 1) \leq c_8(\ell) \log(B) + c_9(\ell).
\]

Combining equations (5) and (6), we have
\[
e_\ell c_5(\ell) B \leq c_8(\ell) \log(B) + c_9(\ell).
\]

We define
\[
K_0(\ell) := \frac{2}{e_\ell c_5(\ell)} \left( c_9(\ell) + c_8(\ell) \log \left( \frac{c_8(\ell)}{e_\ell c_5(\ell)} \right) \right).
\]

By Lemma 3.3, \( B \leq K_0(\ell) \). Define \( K_0 \) to be the maximum of the \( K_0(\ell) \) for all \( p_\ell \in S_{\text{fin}} \). This means that if \( \ell \) corresponds to a finite place, \( B \leq K_0 \).

In our implementation, the functions \texttt{mus} and \texttt{possible\_mu0s} are used to recover the \( \mu_i \) for each finite place \( p_\ell \). The constants from Yu’s Theorem are determined in the function \texttt{c8\_c9\_func}, while the constant \( K_0 \) (which may be of interest on its own) is computed by \texttt{K0\_func}.

4.3. Case II: \( p_\ell \) is infinite. We now assume \( p_\ell \) is infinite. As in §2.3, we let \( \sigma_{p_\ell} \) denote the embedding of \( K \) into \( \mathbb{C} \) such that
\[
|\alpha|_{p_\ell} = |\sigma_{p_\ell}(\alpha)|^{\delta(\ell)}, \quad \text{where} \quad \delta(\ell) = \begin{cases} 
1 & \text{if } p_\ell \text{ is real,} \\
2 & \text{if } p_\ell \text{ is complex.}
\end{cases}
\]
We let $\alpha^{(\ell)}$ denote $\sigma_p(\alpha)$ for any $\alpha \in K$, and we define
\[
c_{11}(\ell) := \frac{\delta(\ell) \log 4}{c_3}, \quad c_{13}(\ell) := \frac{c_3}{\delta(\ell)}.
\]
The condition (4) can now be expressed as
\[
\left| \tau_1^{(\ell)} \right| \leq e^{-c_{13}(\ell)B}.
\]
The choices of $c_{11}(\ell)$ and $c_{13}(\ell)$ guarantee that
\[
B \geq c_{11}(\ell) \implies \left| \tau_1^{(\ell)} \right| \leq \frac{1}{4}.
\]
Set $\Lambda := \log \tau_2^{(\ell)}$. The estimate $|\log z| \leq 2|z - 1|$ holds for $|z - 1| \leq \frac{1}{4}$, and so
\begin{equation}
(7) \quad |\Lambda| \leq 2 \left| \tau_2^{(\ell)} - 1 \right| = 2 \left| \tau_1^{(\ell)} \right| \leq 2e^{-c_{13}(\ell)B}.
\end{equation}
The next step is to view $\Lambda$ as a linear form in logarithms and apply the theorem of Baker and Wüstholz. Set $\zeta := \exp \frac{2\pi \sqrt{-1}}{w} \in \mathbb{C}$. Since $\rho_0$ is a $w$th root of unity, there exists $0 \leq k < w$ such that $(\rho_0^{(\ell)})^{b_{2,0}} = \zeta^k$. By (3), we have
\[
\Lambda = \log \left( \left( \rho_0^{(\ell)} \right)^{b_{2,0}} \cdot \prod_{j=1}^t \left( \rho_j^{(\ell)} \right)^{b_{2,j}} \right)
\]
\[
= \log \zeta^k + \sum_{j=1}^t b_{2,j} \log \rho_j^{(\ell)} + A \cdot 2\pi \sqrt{-1}
\]
\[
= k \log \zeta + \sum_{j=1}^t b_{2,j} \log \rho_j^{(\ell)} + Aw \log \zeta
\]
\[
= (Aw + k) \log \zeta + \sum_{j=1}^t b_{2,j} \log \rho_j^{(\ell)},
\]
where we have introduced $A \in \mathbb{Z}$ to adjust for the principal branch of the logarithm. Certainly $|A| \leq tB$, and so $|Aw + k| \leq (t + 1)Bw$. Set
\[
b_{2,j}^{'} := \begin{cases} Aw + k & j = 0 \\ b_{2,j} & j > 0 \end{cases}
\]
and $L'(z_0, \ldots, z_t) := \sum_{j=0}^t b_{2,j}^{'} z_j$. We now have
\[
|\Lambda| = \left| L'(\log \zeta, \log \rho_1^{(\ell)}, \ldots, \log \rho_t^{(\ell)}) \right|.
\]
SOLVING S-UNIT EQUATIONS

Taking $K' = \mathbb{Q}(\rho_0, \ldots, \rho_t) \cong \mathbb{Q}(\zeta, \rho_1^{(\ell)}, \ldots, \rho_t^{(\ell)})$, we define

$$c_{14}(\ell) := C(t, d_{K'}) \prod_{j=0}^{t} h'(\rho_j).$$

(Recall that $C(t, d_{K'})$ is defined in Theorem 3.1) We have $|b'_{2,j}| \leq B' := (t + 1)Bw$. Applying Theorem 3.1 to $\Lambda$, we obtain

$$\log |\Lambda| > -c_{14}(\ell) \cdot \log B' = -c_{14}(\ell) \log ((t + 1)wB).$$

Combining this inequality with (7), we obtain

$$2e^{-c_{13}(\ell)B} \geq |\Lambda| \geq e^{-c_{14}(\ell) \log B'}.$$

As in the previous case, we apply Lemma 3.3 Set

$$c_{15}(\ell) := \frac{2}{c_{13}(\ell)} \left( \log 2 + c_{14}(\ell) \log \left( \frac{(t + 1)w \cdot c_{14}(\ell)}{c_{13}(\ell)} \right) \right).$$

We obtain $B < c_{15}(\ell)$ (provided $B \geq c_{11}(\ell)$). Thus, setting

$$K_1(\ell) := \max\{c_{11}(\ell), c_{15}(\ell)\},$$

$$K_1 := \max\{K_1(\ell) : p_\ell \text{ is infinite}\},$$

we may be sure $B \leq K_1$.

In our implementation, the constant $K_1$ is computed in the function $K1\_func$.

5. LLL Reduction

In this section we explain how we can reduce the upper bound we have computed in Section 4. This is necessary, because in practice the size of the initial bound is extremely large and cannot be used for practical computations. The idea of the method we will present here has its origin in de Weger’s thesis [12, 11, 13] where he develops a method based on multi-dimensional approximation lattices of linear form of $p$-adic numbers to solve (among many other equations) $S$-unit equations over $\mathbb{Q}$. These ideas of de Weger have been extended by himself and others to apply over any number field $K$, and have also been used for the solution of other exponential Diophantine equations [40, 41, 42, 35].

In the reduction step we use the LLL reduction algorithm on lattices generated by integer matrices. So instead of the classical LLL algorithm

\[\text{It is worth mentioning the recent results of von Kānel and Matschke [29], who solve S-unit equations using modularity.}\]
If \( L \) is a lattice in \( \mathbb{R}^n \), let \( L^* = L - \{0\} \). For \( y \in \mathbb{R}^n \), we define
\[
\ell(L, y) = \begin{cases} 
\min_{x \in L^*} \|x\|, & \text{if } y \in L, \\
\min_{x \in L} \|x - y\|, & \text{otherwise.}
\end{cases}
\]
In practice, for a given lattice \( L \) and vector \( y \) we can compute a lower bound for \( \ell(L, y) \) using LLL (see the function \texttt{minimal_vector}). As in the previous section, we follow Smart’s notation in [35]. Most of the material we present in this section can also be found in [37, 14].

5.1. Finite places. Suppose \( p_\ell \) is a finite place. From (5) and §2.4, we obtain \( \text{ord}_{p_\ell} \tau_1 \geq c_5(\ell)B \). Define
\[
c_{16}(\ell) := \frac{1}{c_5(\ell)}. 
\]
If \( B > c_{16}(\ell) \), then as shown in §4.2 there exist \( \mu_i \in K^\times \), \( 0 \leq i \leq t - 1 \), such that
\[
\tau_2 = \mu_0 \prod_{i=1}^{t-1} \mu_i^{d_i}, \quad |d_i| \leq B \text{ for all } i. 
\]
Define \( \Delta_2 \in K_{p_\ell} \) by
\[
\Delta_2 := \log_{p_\ell} \tau_2 = \log_{p_\ell} \mu_0 + \sum_{i=1}^{t-1} d_i \log_{p_\ell} \mu_i.
\]
As \( B > c_{16}(\ell) \), \( \text{ord}_{p_\ell} \Delta_2 \geq 1 \), which guarantees \( |\Delta_2|_{p_\ell} < p^{-\frac{1}{p-1}} \). Thus,
\[
\text{ord}_{p_\ell} \Delta_2 = \text{ord}_{p_\ell} \log_{p_\ell} \tau_2 = \text{ord}_{p_\ell} \log_{p_\ell}(-\tau_1 + 1)
= \text{ord}_{p_\ell} \tau_1 \geq c_5(\ell)B.
\]
Choose \( \theta \in K_{p_\ell} \) such that \( K_{p_\ell} = \mathbb{Q}_p(\theta) \), and let \( \text{Disc}(\theta) \) denote the discriminant of \( \theta \). Set \( D_p(\theta) = \text{ord}_{p_\ell} \text{Disc}(\theta) \) and \( n = [K_{p_\ell} : \mathbb{Q}_p] \), so that \( n = e_{f_\ell}f_\ell \). Expressing \( \Delta_2 \) with respect to the power basis, we obtain \( \Delta_{2,i} \in \mathbb{Q}_p \) such that \( \Delta_2 = \sum_{i=0}^{n-1} \Delta_{2,i} \theta^i \). Further, we may express
\[
\Delta_{2,i} = a_{0,i} + \sum_{j=1}^{t-1} d_j a_{j,i}, \quad a_{j,i} \in \mathbb{Q}_p, \ 0 \leq i \leq n - 1.
\]
Using an idea due to Evertse [42, p.257], we have
\[
\text{ord}_{p_\ell} \Delta_{2,i} \geq c_5(\ell)B - \frac{D_p(\theta)}{2}.
\]
Define
\[ c_{17}(\ell) := \min \{ \text{ord}_p a_{j,i} : 1 \leq j \leq t - 1, \ 0 \leq i \leq n - 1 \}, \]
\[ c_{18}(\ell) := c_{17}(\ell) + \frac{D_p(\theta)}{2}, \]
and choose \( \lambda \in \mathbb{Q}_p \) such that \( \text{ord}_p \lambda = c_{17}(\ell) \).

Should there be some index \( i \) such that \( c_{17}(\ell) > \text{ord}_p(a_{0,i}) \), then \( \text{ord}_p \Delta_{2,i} = \text{ord}_p a_{0,i} < c_{17}(\ell) \), and consequently
\[ B < \frac{c_{18}(\ell)}{c_{5}(\ell)}. \]

For the remainder, then, we assume \( c_{17}(\ell) \leq \min \{ a_{0,i} : 0 \leq i \leq n - 1 \} \).

By the choice of \( \lambda \), \( \kappa_{j,i} := a_{j,i}/\lambda \) is a \( p \)-adic integer for all \( i, j \), and we may rewrite (8) as
\[ \frac{\Delta_{2,i}}{\lambda} = \kappa_{0,i} + \sum_{j=1}^{t-1} d_j \kappa_{j,i}, \quad \text{with} \quad \text{ord}_p \left( \frac{\Delta_{2,i}}{\lambda} \right) \geq c_{5}(\ell) B - c_{18}(\ell). \]

For any \( a \in \mathbb{Z}_p \) and a positive integer \( k \), let \( a^{(k)} \) denote the unique integer between 0 and \( p^k \) such that \( a \equiv a^{(k)} \pmod{p^k} \). For a positive integer \( u \), let \( \mathcal{L} \) be the lattice generated by the columns of the matrix
\[
\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \kappa_{1,0}^{(u)} & \cdots & \kappa_{1,t-1,0}^{(u)} & p^u \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \kappa_{1,n-1}^{(u)} & \cdots & \kappa_{1,t-1,n-1}^{(u)} & 0 \\
\end{pmatrix} \in \mathbb{Z}^{(t+n-1) \times (t+n-1)}. 
\]

Define
\[ y = \begin{pmatrix} 0 & \cdots & 0 & -\kappa_{0,0}^{(u)} & \cdots & -\kappa_{0,n-1}^{(u)} \end{pmatrix}^T \in \mathbb{Z}^{t+n-1}. \]

The following lemma [35, Lemma 5] now provides an opportunity to improve the bound on \( B \).

**Lemma 5.1.** If \( \ell(\mathcal{L}, y) > \sqrt{t-1} \cdot K_1 \), then \( B < (u + c_{18}(l))/c_{5}(l) \).

In the function p_adicLLL_bound we have implemented the above analysis. In more detail, the functions log_p and embedding_to_Kp are used to compute the constants \( a_{j,i} \in \mathbb{Q}_p \) up to a given precision. In p_adicLLL_bound_one_prime we apply Lemma 5.1 for a fixed prime \( p \). Computing the exact value of \( \ell(\mathcal{L}, y) \) is a very challenging problem.
in general. Instead, the function \texttt{minimal_vector} computes a lower bound using standard properties of a reduced basis of a lattice and the LLL algorithm (see [37, Chapter V]). The parameter \( u \) is chosen inside the function to meet the hypotheses of Lemma 5.1 without mention to the user.

5.2. \textbf{Infinite places.} We now consider briefly the case where \( p_\ell \) is an infinite place. The reduction is quite analogous to the \( p \)-adic case; again the standard references are [35, 37, 14]. We keep the notations from §4.3 and for any \( 0 \leq j \leq t \) we define complex numbers

\[
\kappa_j := \begin{cases} 
\log \zeta & j = 0 \\
\log \rho_j^{(\ell)} & j > 0
\end{cases}
\]

As \( p_\ell \) is an infinite complex place, we have established already that \( \Lambda = \log \tau_2^{(\ell)} \) satisfies

\[
\Lambda = \sum_{j=0}^{t} b_{2, j} \kappa_j, \quad |b_{2, j}| \leq (t + 1) B w.
\]

We assume for the remainder that not every \( \kappa_i \) is real and not every \( \kappa_i \) is pure imaginary. (These exceptional cases are handled by the analysis in [37, Ch. VI].) Without loss of generality we assume \( \Re(\kappa_t) \neq 0 \). Let \([\cdot]\) denote the nearest integer function. We choose a positive constant \( C \) and let \( L \) be the lattice generated by the columns of the matrix

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots \\
0 & \cdots & 1 & 0 \\
[C \cdot \Re(\kappa_1)] & \cdots & [C \cdot \Re(\kappa_{t-1})] & [C \cdot \Re(\kappa_t)] \\
[C \cdot \Im(\kappa_1)] & \cdots & [C \cdot \Im(\kappa_{t-1})] & [C \cdot \Im(\kappa_t)] \\

\end{pmatrix}
\in \mathbb{Z}^{(t + 1) \times (t + 1)}.
\]

Suppose \( m_\mathcal{L} \) is a positive lower bound for \( \ell(\mathcal{L}, 0) \), and set

\[
S := (t - 1) K_1^2, \\
T := \frac{1}{\sqrt{2}} (1 + (t + w + tw) K_1).
\]

Applying [37, Lemma VI.2], we have

\textbf{Lemma 5.2.} If \( m_\mathcal{L}^2 > T^2 + S \), then

\[
B \leq \frac{1}{c_{13}(\ell)} (\log 2 C - \log(S - T)).
\]
In the implementation, the function \texttt{minimal\_vector} computes a value for \(m^2\). In the function \texttt{cx\_LLL\_bound}, we have implemented the reduction step for the infinite places applying the above idea. As in the finite case, the parameter \(C\) is chosen inside the function and changed as necessary to meet the bound \(m^2 > T^2 + S\).

6. Further reducing the search space: Sieving

The approach taken here, for sieving against primes outside of \(S\), is based on an algorithm described by Smart in [35]. Smart credits Tzanakis and de Weger with this approach [41]: Tzanakis reports that these ideas date back to Andrew Bremner.

6.1. Setup for the sieve. Recalling the notations of §2.2, we define for any \(m > 0\),

\[ A_{K,S,m} := \left( \mathbb{Z}/w\mathbb{Z} \right) \times \left( \mathbb{Z}/m\mathbb{Z} \right)^t. \]

This finite set will provide a useful search space for exponent vectors in a way we will make more precise below. There is an obvious surjective map \(\pi_m: A_{K,S} \to A_{K,S,m}\). Despite the fact that this map is the identity (and not a reduction map) in the 0th coordinate, we will refer to this as the \textit{reduction modulo} \(m\) map, and call an element \(a \in A_{K,S,m}\) an \textit{exponent vector modulo} \(m\).

Let \(\tau \in \mathcal{O}_{K,S}^\times\). The \textit{exponent vector} for \(\tau\) (relative to \(\rho\)) is \(\Phi_{\rho}^{-1}(\tau)\). That is, it is the unique \(a \in A_{K,S}\) such that \(\tau = \rho^a\). Given any bound \(B\) for the exponent vector of a \(\tau \in X_{K,S}\), we obtain a finite subset of \(\mathcal{O}_{K,S}^\times\) that contains every solution of the \(S\)-unit equation. Unfortunately, this is usually still too large of a search space to be practical (see §7), so we must sieve this finite set (or rather, the equivalent finite set of exponent vectors) prior to the exhaustive search. The sieve attempts to provide an efficient solution to the following problem:

**Problem 6.1.** Find a small set \(Y_{K,S}\) satisfying \(E_{K,S} \subseteq Y_{K,S} \subseteq A_{K,S}\).

If we can find a small enough superset \(Y_{K,S}\) in a fast enough way, the \(S\)-unit equation solutions can then be found by brute force search over \(Y_{K,S}\).

Suppose \(a \in A_{K,S}\). We call \(b \in A_{K,S}\) a \textit{complement vector} for \(a\) if \(\rho^a + \rho^b = 1\). If a complement vector exists, it must be unique; the existence of a complement vector is equivalent to \(a \in E_{K,S}\), and a pair of complement exponent vectors correspond to a solution of the \(S\)-unit equation.

Suppose \(q \in \mathbb{Z}\) is a prime number. We say \(q\) \textit{avoids} \(S\) if \(q \not\in p\) for all ideals \(p \in S\). If \(q\) splits completely in \(\mathcal{O}_K\), then there are \(d_K\) prime ideals above \(q\) in \(\mathcal{O}_K\), say \(q_0, \ldots, q_{d_K-1}\). We let \(\mathbb{F}_q\) denote the residue
field of $q_j$. Since $q$ is completely split, we of course have $\mathbb{F}_{q_j} \cong \mathbb{F}_q$ for all $j$.

Suppose $\tau \in \mathcal{O}_{K,S}$, and $q$ is a rational prime number which splits completely in $\mathcal{O}_K$ and which avoids $S$. The residue field vector for $\tau$ (with respect to $q$) is

$$rfv_q(\tau) := (\tau + q_0, \tau + q_1, \ldots, \tau + q_{d_K-1}) \in \prod_{i=0}^{d_K-1} \mathbb{F}_{q_i},$$

where $\tau + q_j \in \mathbb{F}_{q_j}$ is the reduction of $\tau$ modulo $q_j$. The residue field vector depends on the ordering of the primes $q_j$ above $q$; we fix one ordering once and for all whenever we consider residue field vectors with respect to $q$.

Notice that we have the following commutative diagram, whose horizontal rows are exact.

Suppose $a \in A_{K,S,q^{-1}}$. Since any two lifts $a', a''$ of $a$ to $A_{K,S}$ differ by a multiple of $(q - 1)$, we see that $\Phi^{-1}(a')$ and $\Phi^{-1}(a'')$ differ by a perfect $(q - 1)$th power, and so determine the same residue field vector. In other words, the dashed arrow in the diagram corresponds to a well-defined map $A_{K,S,q^{-1}} \rightarrow \prod_i \mathbb{F}_{q_i}^\times$, and so the notion of a residue field vector for $a$ is well-defined. With this in mind, we abuse notation slightly and also write $rfv_q a := rfv_q(\Phi^{-1}(a'))$, where $a' \in A_{K,S}$ is any lift of $a$.

**Lemma 6.1.** Suppose $\tau \in X_{K,S}$ and set $\eta = 1 - \tau$. Then

(a) $rfv_q (\tau + rfv_q \eta) = (1, 1, \ldots, 1) \in \prod_i \mathbb{F}_{q_i}$.

(b) $rfv_q \tau \in \prod_i \mathbb{F}_{q_i}^\times$.

(c) no entry of $rfv_q \tau$ is 1.
Proof. Since $\tau + \eta = 1$, it follows that for any $j$, $\tau + \eta \equiv 1 \pmod{q_j}$, verifying (a). As $q$ avoids $S$, $\tau \not\in q_j$ for every $j$. This proves (b). Since (b) holds for both $\eta$ and $\tau$, (c) follows from (a). \qed

Suppose $a$ is an exponent vector modulo $q - 1$; i.e., $a \in A_{K,S,q-1}$. We call $b \in A_{K,S,q-1}$ a $(q - 1)$-complement vector for $a$ if

$$\operatorname{rfv}_q(a) + \operatorname{rfv}_q(b) = (1, 1, \ldots, 1) \in \prod_i \mathbb{F}_{q_i}.$$ 

Existence of a $(q - 1)$-complement vector is a necessary, but not sufficient, condition for $a$ to lift to the exponent vector of a unit in a solution to the $S$-unit equation. Further, any particular $a$ may have more than one $(q - 1)$-complement vector associated to it. We set $E_{K,S}(q - 1) := \{a \in A_{K,S,q-1} : a \text{ has a } (q - 1)\text{-complement vector}\}$.

6.2. Execution of the sieve. The strategy for the sieve is to play the sets $E_{K,S}(q - 1)$ off of one another for multiple values of $q$. Choose a finite list $Q$ of rational prime numbers

$$Q = [q_0, q_1, \ldots, q_k]$$

each of which splits completely in $K$, and such that

$$\operatorname{lcm}(q_0 - 1, q_1 - 1, \ldots, q_k - 1) \geq 2B + 1.$$ 

Any true solution to the $S$-unit equation corresponds to exponent vectors found in the set $E_{K,S}$, and such vectors must reduce modulo $(q_j - 1)$ to vectors in $E_{K,S}(q_j - 1)$ for each $q_j \in Q$. Conversely, given a choice $a_i \in E_{K,S}(q_i - 1)$ for each $0 \leq i < k$, there is at most one vector $a \in A_{K,S}$ such that $\pi_{q_i - 1}(a) = a_i$ for each $i$, while also satisfying $|a| \leq B$. Define $\pi_Q$ to be the product of the maps $\pi_{q_i - 1}$:

$$\pi_Q : A_{K,S} \rightarrow \prod_i A_{K,S,q_i - 1}.$$ 

Certainly we have

$$E_{K,S} \subseteq \pi_Q^{-1}(\prod_i E_{K,S}(q_i - 1)).$$ 

Because lifts from $\prod_i E_{K,S}(q_i - 1)$ to $E_{K,S}$ are unique when they exist, $\prod_i E_{K,S}(q_i - 1)$ provides a reasonable proxy for the search space. We seek to replace each $E_{K,S}(q_i - 1)$ with a subset $Y_i \subseteq E_{K,S}(q_i - 1)$ such that we still have

$$E_{K,S} \subseteq \pi_Q^{-1}(\prod_i Y_i).$$ 

(9)
Suppose $q_i, q_j$ are distinct primes in $Q$, and suppose $a_i \in Y_i$, $a_j \in Y_j$. We say $a_i$ and $a_j$ are compatible if there exists $a \in A_{K,S}$ such that $\pi_{q_i-1}(a) = a_i$ and $\pi_{q_j-1}(a) = a_j$. Notice that for any $i \neq j$, an element $\hat{a} \in E_{K,S}$ reduces modulo $q_i - 1$ and $q_j - 1$ to produce a compatible pair of exponent vectors.

When $a_i$ and $a_j$ are compatible, we further call the pair complement compatible if there exist $b_i \in Y_i$ and $b_j \in Y_j$ such that

- $b_i$ is $(q_i - 1)$-complementary to $a_i$,
- $b_j$ is $(q_j - 1)$-complementary to $a_j$,
- $b_i$ and $b_j$ are compatible.

**Lemma 6.2.** Suppose the sets $Y_i \subseteq E_{K,S}(q_i - 1)$ satisfy condition $[9]$. Further, suppose $a_i \in Y_i$, and set

$$Y_j' := \begin{cases} Y_j & j \neq i \\ Y_i - \{a_i\} & j = i \end{cases}$$

If there exists $j \neq i$ such that $Y_j$ contains no vectors which are complement compatible to $a_i$, then

$$E_{K,S} \subseteq \pi_Q^{-1}(\prod_i Y_i').$$

In other words, under the given condition, we will lose no true solutions by removing $a_i$ from $Y_i$.

**Proof.** Towards a contradiction, suppose $a \in E_{K,S}$ satisfies

$$\pi_{q_i-1}(a) = a_i.$$ 

There is a unique $b \in E_{K,S}$ satisfying $\Phi_p(a) + \Phi_p(b) = 1$. Set

$$a_j = \pi_{q_j-1}(a), \quad b_i = \pi_{q_i-1}(b), \quad b_j = \pi_{q_j-1}(b).$$

Then $a_i$ and $a_j$ are compatible by definition. But since $a_i$ and $a_j$ cannot be complement compatible, the vectors $b_i$ and $b_j$ cannot be compatible. This is impossible, since $b \in E_{K,S}$. Thus, no such $a_i$ exists and the claim holds.

The algorithm based on this lemma is the following.

**Algorithm 6.2** (Sieve). Assume that $K$, $S$ are fixed and a representation of $\mathcal{O}_K^n$ has been computed.

**INPUT:** $Q = \{q_0, q_1, \ldots, q_{k-1}\}$

**OUTPUT:** $Y_0, Y_1, \ldots, Y_{k-1}$ satisfying $[9]$.

1. Set $Y_i \leftarrow E_{K,S}(q_i - 1)$ for each $i$.
2. Loop over $i \in \{0, 1, \ldots, k-1\}$:
   (a) Loop over $a_i \in Y_i$:
SOLVING S-UNIT EQUATIONS

i. If $Y_i$ contains no $(q_i - 1)$-complement vector for $a_i$, remove $a_i$ from $Y_i$.

ii. Loop over $j \in \{0, 1, \ldots, i - 1, i + 1, \ldots, k - 1\}$:
   - If there are no $a_j \in Y_j$ which are complement compatible with $a_i$, then remove $a_i$ from $Y_i$.

3. Did Step 2 remove any elements from any set $Y_i$?
   - If YES, return to Step 2.
   - If NO, then STOP.

Once the sieve has been completed, we may find all solutions to the $S$-unit equation by doing an exhaustive search over $\pi^{-1}_Q(\prod_i Y_i)$.

7. EXPERIMENTAL OBSERVATIONS AND COMPUTATIONAL CHOICES

In developing this code and in pursuit of applications, we have computed a very large number of examples. Some observations and discussion may be enlightening to a reader who wishes to solve the $S$-unit equation for their own application.

Our implementation provides the function `sieve_below_bound(K, S, B)`, which returns all solutions to the $S$-unit equation in $\mathcal{O}_{K, S}^x$ up to a specified bound $B$ (the maximum absolute value of an entry in an exponent vector). This may be useful in settings where an exhaustive list of solutions is not needed. For example, in the field $K_g$ with $g(x) = x^3 - 3x + 1$, and $S_{\text{fin}}$ the set of primes dividing 2, the provable LLL-reduced exponent bound is 101. However, all solutions actually satisfy the exponent bound 5, and the command `sieve_below_bound(K, S, 5)` executes in under 2 seconds.

7.1. Sieving vs. simple exhaustion. Once a bound has been reduced as much as possible by LLL, this search space must be somehow exhausted. This general problem can be solved in multiple ways. Those appearing in the literature can be generally described by the following three ideas:

1. simple (non-number theory-based) exhaustion,
2. sieve by reducing the problem modulo primes not in $S$, and
3. sieve by reducing the problem modulo powers of primes in $S$.

Idea (1) could be looked at through the more general lens of efficient programming, and a good programmer may be able to develop their own code to exhaust the search space effectively. The current implementation uses idea (2), inspired by Smart’s earlier exposition in [35] and is described here in Section 6. Item (3) paraphrases an interesting idea due to Wildanger [43], which was generalized by Smart [38]. This is an extremely promising and potentially effective method of reducing
the search space, and has been implemented recently in special cases by several people, including Kousianas [22], Bennett, Gherga, and Rechnitzer [5], von Känel and Matschke [29], and others. Future work will certainly focus on including this sieving technique for our functions.

In all these methods, we begin with the same search space as in (1), and the computational complexity of a brute force search is easy to estimate. Let $B$ be a bound for the maximum absolute value of an exponent in a solution to the $S$-unit equation. Since we are searching for a pair $(\tau, \eta) \in \left( \mathcal{O}_{K,S}^\times \right)^2$, the size of our search space is given by

$$|A_{K,S}|^2 = w^2(2B + 1)^{2t}.$$ 

Thus a naïve brute force search has complexity $O\left(w^2(2B + 1)^{2t}\right)$. In practice, a simple exhaustive search can be carried out by checking, for each element $\tau$ of $A_{K,S}$, whether $1 - \tau$ is an $S$-unit. Assuming this check has constant time for a fixed $K$ and $S$, we get the less extreme complexity of $O\left(w(2B + 1)^t\right)$.

In carrying out computations, we find that the resources required to sieve a search space vary greatly, even for number fields of the same degree and $S$-unit groups of the same rank. For example, we give the run time for three fields $K_g$, where $S_f$ is the set of primes above 3 in $K_g$, in Table 1. The column $N$ gives the total number of distinct solutions found. In each case, the LLL-reduced bound is below 40, so complete sets of solutions are found in each case. Computations were performed in a paid account on the CoCalc platform in late 2018.

| $g(x)$            | $t$ | $w$ | $N$ | Runtime (in seconds) |
|------------------|-----|-----|-----|----------------------|
| $x^4 - x^2 + 1$  | 2   | 12  | 16  | 1.16                 |
| $x^4 + 9$        | 2   | 4   | 0   | 2.06                 |
| $x^4 + 12x^2 + 18$ | 2  | 2   | 0   | 64.                  |

The resources required depend on the size of the search space, but also can vary greatly based on the particular list of primes $Q$ chosen for the sieve, and even the order of those primes! In many cases, the sieve greatly reduces the time required to exhaust the space. In others, a brute force search of the reduced search space can actually be a better choice, as the sieving computation can require large amounts of memory, or take a long time even if memory is not an issue. Finding a way to understand and predict these difficulties is a priority for future work. The implementation of idea (3) could also make this unnecessary.
In all cases, it is worthwhile to find the smallest reduced bound possible, whether as input for the built-in sieve or for use in a brute force search.

7.2. Finite place vs. infinite place bounds. In general, we find that the LLL-reduced bounds corresponding to $p_\ell$ infinite are smaller than the bounds for $p_\ell$ finite. To illustrate this, let $\mathcal{K}$ be the set of 84 number fields $K$ satisfying

$$2 \leq [K : \mathbb{Q}] \leq 5, \quad \Delta_K = \pm 2^a 3^b.$$ 

If $N \in \mathbb{Z}$, we set

$$S_{\text{fin},K,N} := \{p \subseteq \mathcal{O}_K : p \mid N\},$$

$$S_{K,N} := S_{\text{fin},K,N} \cup S_\infty.$$

For any choice of $K \in \mathcal{K}$ and $S = S_{K,N}$ where $N \in \{2, 3, 6\}$, we have computed the LLL-reduced bounds under the assumption that $p_\ell$ is finite and under the assumption that $p_\ell$ is infinite. Complete bound data is available at https://github.com/akoutsianas/Sunits_data. Here we will consider only the case $S = S_{K,2}$. Now, let $B_1(K)$ and $B_2(K)$ be the bounds obtained in §5 under the assumption that $p_\ell$ is a finite or infinite place, respectively. In Figure 1, we plot both $B_1(K)$ and $B_2(K)$ against the root discriminant of $K$ (which ranges from 1.74 to 26.56 in $\mathcal{K}$) The bound $B_1(K)$ usually exceeds $B_2(K)$, on average by a factor of $\approx 3.73$.

Because the disparity between these bounds is so large, we would prefer to use $B_2(K)$. Generally, we have no control over whether $p_\ell$ is finite or infinite. However, if $S$ contains only one finite place, a small trick allows us to use $B_2(K)$. If $(\tau, \eta) \in \mathcal{O}_{K,S}^\times$ is a solution to the $S$-unit equation, note that $(\frac{1}{\tau}, \frac{-2}{\eta})$ and $(\frac{1}{\eta}, \frac{-\tau}{\eta})$ are also $S$-unit equation solutions. We define the solution cycle of $\tau$ to be

$$C(\tau) := \left\{ \tau, 1 - \tau, \frac{1}{\tau}, 1 - \frac{1}{\tau}, \frac{1}{1 - \tau}, 1 - \frac{1}{1 - \tau} \right\}.$$

The following result is a restatement of [25, Lemma 6.3].

**Lemma 7.1.** Let $K$ be a number field, and suppose $S$ is a finite set of places of $K$ containing all infinite places and at most one finite place, (i.e. $|S_{\text{fin}}| = 1$). Let $(\tau, \eta)$ be a solution to the $S$-unit equation over $K$. Then at least one element of $C(\tau)$ belongs to a solution with $p_\ell$ corresponding to an infinite place.

This implies that under the hypothesis of the lemma, some representative of each solution cycle has an exponent vector bounded by $B_2(K)$; recovering the entire solution cycle from one representative is trivial. Thus, we can determine all solutions to the $S$-unit equation.
Figure 1. Bounds $B_1(K)$, $B_2(K)$ for $S = S_{K,2}$ and $K \in \mathcal{K}$, plotted against $\Delta_{K}^{1/d_K}$.

It may seem that the hypothesis of Lemma 7.1 – that there is only one finite place in $S$ – is a rather specialized condition. However, many interesting arithmetic applications involve searching for objects with “good” behavior away from one prime $p$. In such cases, we take $S = S_{K,p}$. Should $p$ ramify in $K$, the condition $|S_{\text{fin}}| = 1$ is equivalent to $p$ being totally ramified, and this is not so uncommon when $[K : \mathbb{Q}]$ is small. Here, with $S = S_{K,2}$, the lemma applies for 72 of the 84 number fields in $\mathcal{K}$.

To illustrate the utility of Lemma 7.1, consider the ratio of the sizes of the search spaces for two bounds $B_1(K)$ and $B_2(K)$, given by

$$R(K) = \frac{w^2(2B_1(K) + 1)^{2t}}{w^2(2B_2(K) + 1)^{2t}} \approx \left( \frac{B_1(K)}{B_2(K)} \right)^{2t}.$$ 

This quantifies the potential savings when the better bound may be used. For $S = S_{K,2}$, Figure 2 plots the savings $R(K)$ against the root discriminant of $K$ for the 72 fields $K$ in $\mathcal{K}$ for which $|S_{\text{fin}}| = 1$.

8. Applications

A major application of solving $S$-unit equations is in enumerating solutions to Shafarevich-type problems, for example finding complete
lists of curves of a given type with particular reduction properties. The blueprint for this implementation came from Smart’s 1997 enumeration of all genus 2 curves over $\mathbb{Q}$ with good reduction away from $p = 2$ [36], building off earlier work with Merriman [26]. In 2017, Malmskog and Rasmussen used these methods to determine all Picard curves defined over $\mathbb{Q}$ with good reduction away from $p = 3$ [25]. The same year, Koutsianas produced a new algorithm that uses solutions to the $S$-unit equation to find all elliptic curves over an arbitrary number field having good reduction outside $S$ [22].

In the remainder of this article, we provide some new applications of the implementation.

8.1. **Asymptotic Fermat.** Let $K/\mathbb{Q}$ be a number field. We consider the nontrivial solutions (over $K$) to the Fermat equation:

$$C_p : a^p + b^p + c^p = 0, \quad abc \neq 0, \quad p > 3 \text{ a prime.}$$

For fixed $p$, it follows from the work of Faltings that $C_p(K)$ is finite, but it is reasonable to ask whether $\cup_p C_p(K)$ is finite or infinite. Finiteness is equivalent to the condition that $C_p(K) = \emptyset$ for sufficiently large $p$. 

**Figure 2.** $R(K)$ versus $\Delta^{1/dK}_K$ for $K \in \mathcal{X}$, $S = S_{K,2}$, and $|S|_{\text{fin}} = 1$. 
We say $K$ satisfies *asymptotic Fermat* if there exists a bound $B_K$ such that $p > B_K$ implies $C_p(K) = \emptyset$.

There are several number fields $K$ for which it is known that $K$ satisfies asymptotic Fermat: Jarvis-Meekin [21] demonstrate that $K = \mathbb{Q}(\sqrt{2})$ satisfies asymptotic Fermat with $B_K = 4$. Freitas-Siksek give an explicit family of real quadratic fields of density $\geq \frac{5}{6}$ which satisfy asymptotic Fermat. They also report that the real quartic field, $K = \mathbb{Q}(\sqrt{2} + \sqrt{2})$ satisfies asymptotic Fermat.

In [15], Freitas and Siksek find a condition on a totally real field $K$ which guarantees that $K$ satisfies asymptotic Fermat. For the remainder, suppose $K$ is totally real. Define

$$S = \{p : p \text{ a nonzero prime ideal of } \mathcal{O}_K \text{ which divides } 2\},$$

$$T = \{p \in S : f_p = 1\}.$$ 

**Theorem 8.1** (Freitas-Siksek). Let $K/\mathbb{Q}$ be a totally real number field, with either $[K : \mathbb{Q}]$ odd or $T$ nonempty. Suppose that for every solution $(\lambda, \mu)$ to the $S$-unit equation, there is some $p \in T$ such that

$$\max\{\nu_p(\lambda), \nu_p(\mu)\} \leq 4\nu_p(2).$$

Then $K$ satisfies asymptotic Fermat.

**Remark 8.1.** We note that Freitas-Siksek’s result is actually stronger, and they provide additional conditions under which $K$ must satisfy asymptotic Fermat. Also, more recent work of Şengün-Siksek [33] provides similar criteria for arbitrary number fields. However, the above formulation is sufficient for our application.

The reader may recall that Wiles’s classic proof of Fermat’s Last Theorem proceeds by taking a hypothetical solution $(a, b, c)$ and noting that the associated Frey elliptic curve is forced to satisfy an impossible set of constraints (that the curve is not modular). Freitas and Siksek’s approach is similar. Given a solution to $C_p$ over $K$, they produce an elliptic curve $E/K$ (related to, but distinct from, the Frey curve) whose $j$-invariant is arithmetically constrained. However, the $j$-invariant is determined by the $\lambda$-invariants of $E$; these $\lambda$ are guaranteed to arise as solutions to the $S$-unit equation over $K$. The result above follows from a delicate analysis of how these constraints interact.

We report a new list of cubic number fields $K/\mathbb{Q}$ which satisfy asymptotic Fermat. Using the implementation of the algorithm described in this paper, we find all solutions to the $S$-unit equation ($S$ as above), and verify the condition of Freitas-Siksek (this last step is trivial once all solutions have been determined).

Let $\mathcal{S}_K$ denote the set of totally real cubic number fields in which 2 is totally ramified and which have absolute discriminant $\Delta_K$ satisfying
| $f_K$ | $\Delta_K$ | $C_0$ | $N(S,K)$ |
|-------|-----------|-------|----------|
| $x^3 - x^2 - 3x + 1$ | $2^2 \cdot 37$ | 198 | 53 |
| $x^3 - x^2 - 5x - 1$ | $2^2 \cdot 101$ | 154 | 11 |
| $x^3 - x^2 - 5x + 3$ | $2^2 \cdot 3 \cdot 47$ | 143 | 5 |
| $x^3 - 6x - 2$ | $2^2 \cdot 3^3 \cdot 7$ | 147 | 5 |
| $x^3 - x^2 - 7x - 3$ | $2^2 \cdot 197$ | 147 | 8 |
| $x^3 - 8x - 6$ | $2^2 \cdot 269$ | 175 | 8 |
| $x^3 - 10x - 10$ | $2^2 \cdot 5^2 \cdot 13$ | 147 | 8 |
| $x^3 - x^2 - 7x + 5$ | $2^2 \cdot 349$ | 164 | 8 |
| $x^3 - x^2 - 9x - 5$ | $2^2 \cdot 373$ | 149 | 8 |
| $x^3 - x^2 - 7x + 1$ | $2^2 \cdot 3 \cdot 127$ | 160 | 2 |
| $x^3 - x^2 - 9x + 11$ | $2^2 \cdot 389$ | 169 | 8 |
| $x^3 - 12x - 14$ | $2^2 \cdot 3^4 \cdot 5$ | 139 | 2 |
| $x^3 - 8x - 2$ | $2^2 \cdot 5 \cdot 97$ | 130 | 5 |

Table 2. Fields in $\mathcal{X}_{2000}$ and number of $S$-unit equation solutions

$|\Delta_K| \leq X$. Table 8.1 lists all the fields of $\mathcal{X}$ for $X = 2000$. For each $K \in \mathcal{X}$, we solved the appropriate $S$-unit equation, and by applying Theorem 8.1, verified that $K$ satisfies asymptotic Fermat. Our results are not effective, as Theorem 8.1 does not provide the bound $B_K$.

For each $K \in \mathcal{X}_{2000}$, $f_K$ denotes a minimal polynomial for $K/\mathbb{Q}$; $\Delta_K$ is the absolute discriminant of $K$. The constant $C_0$ is the explicit bound for the absolute value of entries appearing in the exponent vectors associated to a solution $(\lambda, \mu)$ of the $S$-unit equation: if $\lambda, \mu \in \mathcal{O}_{K,S}^\times$ are given by $\lambda = \rho^a$ and $\mu = \rho^b$, then $|a|, |b| \leq C_0$. Finally, $N(S,K)$ indicates the number of distinct solutions $(\lambda, \mu)$ to the $S$-unit equation found. (These are unordered solutions, so that $(\lambda, \mu)$ and $(\mu, \lambda)$ are not considered distinct.) The reader should note that the two trivial solutions over $\mathbb{Q}$, $(-1, 2)$ and $(\frac{1}{2}, \frac{1}{2})$, are counted in each field $K$.

8.2. Genus 2 Curves. Let $\mathcal{M}$ denote the set of $\mathbb{Q}$-isomorphism classes of smooth genus 2 curves $C$ over $\mathbb{Q}$, where $C$ has good reduction away from 3. Within $\mathcal{M}$, let $\mathcal{W}$ denote the subset of classes for which $C$ has
all Weierstrass points defined over a number field $K$ unramified away from $\{3, \infty\}$.

In the project [31], Rowan (with supervision from Kadets and Sutherland) demonstrated that listing all classes of $W$ was possible, given a complete set of solutions to the $S$-unit equation over a set of six fields, where $S$ contained all the primes above 2 and 3. The fields in question are the splitting fields $K_1, \ldots, K_6$ of the polynomials

$$\begin{align*}
g_1(x) &= x^2 - x - 1 & g_4(x) &= x^6 - x^3 + 1 \\
g_2(x) &= x^3 - 3 & g_5(x) &= x^6 + 3 \\
g_3(x) &= x^3 - 3x - 1 & g_6(x) &= x^6 - 3x^3 + 3
\end{align*}$$

The fields $K_1, K_2, K_3$ are small degree and pose little difficulty. Rowan, using older code of Koutsianas, computed a reduced exponent bound for solutions in the field $K_5$ to be $B = 231345$, and concluded that an exhaustive search would not be possible. However, using our current implementation, we find the reduced exponent bounds:

$$B(K_4) = 1578, \quad B(K_5) = 2850, \quad B(K_6) = 7822.$$ 

Unfortunately, solving the equation when $S_Q = \{2, 3, \infty\}$ may still be computationally out of reach, even with this improvement. For example, $K_6$ is a degree 6 extension of $\mathbb{Q}$ with $S$-unit group of rank $t = 4$ and $w = 6$ roots of unity. Thus, the total space to be searched is size $6(15645)^4 \approx 3.60 \times 10^{17}$, which cannot be managed practically, even with the sieve. Still, the improved bounds move us closer to such an enumeration.

### 8.3. Cubic Ramanujan-Nagell equations

In 1913, Ramanujan conjectured that the only solutions of the Diophantine equation $x^2 + 7 = 2^n$ satisfy $|x| = 1, 3, 5, 11, 181$ [30]. This was settled in 1948 by Nagell [27]. The more general family of equations,

$$Ax^2 + B = C^n, \quad A, B, C \in \mathbb{Z}$$

are called Ramanujan-Nagell equations, and the literature for solving such equations is very rich (see for example [9, 8, 10, 6]). Very recently cubic Ramanujan-Nagell equations have attracted the attention of mathematicians [4]. These are equations where the left-hand side is a cubic polynomial. In this section, we study the equation

$$x^3 + 3^k = q^n, \quad q \text{ odd prime}. \tag{10}$$

Actually, we prove the following\footnote{Our method also works for the equation $x^3 + p^k = q^n$, where $p, q$ are different odd primes, and the proof is similar to the case $p = 3$.}
| (q, x, k, n) |
|---------------|
| (17, 2, 2, 1) |
| (67, 4, 1, 1) |
| (73, 4, 2, 1) |
| (89, 2, 4, 1) |
| (251, 2, 5, 1) |
| (307, 4, 5, 1) |

Table 3. Solutions of the cubic Ramanujan-Nagell equation.

**Theorem 8.2.** Let \( q \) be an odd prime with \( q \leq 10 \). Then, all solutions of the cubic Ramanujan-Nagell equation (10) with \( k, n \geq 0 \) are listed in Table 8.3.

We let \( L \) denote the splitting field of \( x^3 + 3 \), and let \( S_L \) be the set of prime ideals in \( L \) lying above 3 and \( q \). Let \( \rho \) be a set of generators for \( \mathcal{O}_L \times S_L \), where \( \rho_0 \) is the generator of the torsion part. Let \( B \) be an upper bound for the exponent vectors of solutions of the \( S \)-unit equation with respect to \( \mathcal{O}_L \times S_L \) and \( \rho \). Then, the main idea behind the proof of Theorem 8.2 is that we can bound \( k, n \) with respect to \( B \). In more detail, we have the following lemma.

**Lemma 8.3.** With the above notation there exist computable constants \( c_3 \) and \( c_q \) such that \( k \leq c_3 \cdot B \) and \( n \leq c_q \cdot B \).

**Proof.** Suppose \((x, y)\) is a solution of (10) and \( \zeta_3 \) is a primitive third root of unity. Then

\[
(x + \sqrt[3]{3}) (x + \zeta_3 \cdot \sqrt[3]{3}) (x + \zeta_2 \cdot \sqrt[3]{3}) = q^n.
\]

As \( q \neq 2, 3 \), the ideals \( \langle x + \sqrt[3]{3} \rangle \), \( \langle x + \zeta_3 \cdot \sqrt[3]{3} \rangle \) and \( \langle x + \zeta_2 \cdot \sqrt[3]{3} \rangle \) must be pairwise coprime. Moreover, the extension \( L/\mathbb{Q} \) is unramified outside 6, so if \( q \mid q \) and \( q \mid \langle x + \sqrt[3]{3} \rangle \) then \( \text{ord}_q(x + \sqrt[3]{3}) = n \). There are (positive) integers \( a_i \) and \( b_i \) such that

\[
(x + \sqrt[3]{3}) = \prod_{i=0}^{t} \rho_i^{a_i} \quad \text{and} \quad (x + \zeta_3 \cdot \sqrt[3]{3}) = \prod_{i=0}^{t} \rho_i^{b_i}.
\]

Because \( q \neq 3 \), we have for any prime \( p \) of \( L \) above 3 that

\[
\text{ord}_p \prod_{i=0}^{t} \rho_i^{a_i} = \text{ord}_p \prod_{i=0}^{t} \rho_i^{b_i} = 0,
\]
Subtracting the above two equations we have

\[(1 - \zeta_3) \sqrt{p^k} = \prod_{i=0}^{t} \rho_i^{a_i} - \prod_{i=0}^{t} \rho_i^{b_i}.\]

Because \(1 - \zeta_3\) is a root of unity, the above equation is a \(S\)-unit equation and we rewrite it in the usual form

\[1 = \frac{\prod_{i=0}^{t} \rho_i^{a_i}}{(1 - \zeta_3) \sqrt{p^k}} - \frac{\prod_{i=0}^{t} \rho_i^{b_i}}{(1 - \zeta_3) \sqrt{p^k}}.\]

If \(e_3\) is the ramification index with respect to 3 then we have that \(n \leq c_q \cdot B\) and \(k \leq c_3 \cdot B\) where

\[c_q := \max_{q \mid q} \sum_{i=1}^{t} \left| \text{ord}_q(\rho_i) \right|,\]

\[c_3 := \frac{3}{e_3} \max_{p \mid 3} \sum_{i=1}^{t} \left| \text{ord}_p(\rho_i) \right|.\]

\[\square\]

**References**

[1] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13* (1966), 204-216; *ibid. 14* (1967), 102-107; *ibid., 14:220–228, 1967.

[2] A. Baker and G. Wüstholz. Logarithmic forms and group varieties. *J. Reine Angew. Math.*, 442:19–62, 1993.

[3] A. Baker and G. Wüstholz. *Logarithmic forms and Diophantine geometry*, volume 9 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2007.

[4] M. Bauer and M. A. Bennett. Ramanujan-Nagell cubics. *Rocky Mountain J. Math.*, 48(2):385–412, 2018.

[5] M. A. Bennett, A. Gherga, and A. Rechnitzer. Computing elliptic curves over \(Q\). *Math. Comp.*, 88(317):1341–1390, 2019.

[6] M. A. Bennett and C. M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[7] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[8] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[9] Y. Bugeaud and T. N. Shorey. On the number of solutions of the generalized Ramanujan-Nagell equation. *J. Reine Angew. Math.*, 539:55–74, 2001.

[10] J. H. E. Cohn. The Diophantine equation \(x^2 + C = y^n\). *Acta Arith.*, 65(4):367–381, 1993.

[11] B. M. M. de Weger. Solving exponential Diophantine equations using lattice basis reduction algorithms. *J. Number Theory*, 26(3):325–367, 1987.

[12] B. M. M. de Weger. *Algorithms for Diophantine Equations*. PhD thesis, Universiteit Leiden, 1988.
[13] B. M. M. de Weger. *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*. Stichting Mathematicisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[14] J.-H. Evertse and K. Győry. *Unit equations in Diophantine number theory*, volume 146 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2015.

[15] N. Freitas and S. Siksek. The asymptotic Fermat’s last theorem for five-sixths of real quadratic fields. *Compos. Math.*, 151(8):1395–1415, 2015.

[16] C. Fuchs. *On some applications of Diophantine approximations*, volume 2 of *Quaderni/Monographs*. Edizioni della Normale, Pisa, 2014. A translation of Carl Ludwig Siegel’s “Über einige Anwendungen diophantischer Approximationen” by Clemens Fuchs, With a commentary and the article “Integral points on curves: Siegel’s theorem after Siegel’s proof” by Fuchs and Umberto Zannier, Edited by Zannier.

[17] K. Győry. On the number of solutions of linear equations in units of an algebraic number field. *Comment. Math. Helv.*, 54(4):583–600, 1979.

[18] K. Győry. Bounds for the solutions of $S$-unit equations and decomposable form equations II. [arXiv:1901.11289] January 2019.

[19] K. Győry and K. Yu. Bounds for the solutions of $S$-unit equations and decomposable form equations. *Acta Arithmetica*, 123(1):9–41, 2006.

[20] H. Hasse. *Number theory*. Classics in Mathematics. Springer-Verlag, Berlin, german edition, 2002. Reprint of the 1980 English edition [Springer, Berlin; MR0562104 (81c:12001b)], Edited and with a preface by Horst Günter Zimmer.

[21] F. Jarvis and P. Meekin. The Fermat equation over $\mathbb{Q}(\sqrt{2})$. *J. Number Theory*, 109(1):182–196, 2004.

[22] A. Koutsianas. Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction. *Experimental Mathematics*, 2017.

[23] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[24] K. Mahler. Zur Approximation algebraischer Zahlen. I. *Math. Ann.*, 107(1):691–730, 1933.

[25] B. Malmskog and C. Rasmussen. Picard curves over $\mathbb{Q}$ with good reduction away from 3. *LMS J. Comput. Math.*, 19(2):382–408, 2016.

[26] J. R. Merriman and N. P. Smart. Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point. *Math. Proc. Cambridge Philos. Soc.*, 114(2):203–214, 1993.

[27] T. Nagell. The Diophantine equation $x^2 + 7 = 2^n$. *Ark. Mat.*, 4:185–187, 1961.

[28] A. Pethő and B. M. M. de Weger. Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation. *Math. Comp.*, 47(176):713–727, 1986.

[29] B. M. R. von Känel. Solving $S$-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture. preprint, [arXiv:1605.06079] 2016.

[30] S. Ramanujan. Question #464. *J. Indian Math. Soc.*, 5:120, 1913.

[31] J. Rowan. $S$-unit equations and curves of genus 2 with good reduction away from 3, 2016.

[32] Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.4)*, 2018.
[33] M. H. Şengün and S. Siksek. On the asymptotic Fermat’s last theorem over number fields. *Comment. Math. Helv.*, 93(2):359–375, 2018.

[34] C. L. Siegel. Über einige anwendungen diophantischer approximationen. *Abh. der Preuss. Akad. der Wissenschaften Phys. Math. Kl.*, 1:209–266, 1929.

[35] N. P. Smart. The solution of triangularly connected decomposable form equations. *Math. Comp.*, 64(210):819–840, 1995.

[36] N. P. Smart. S-unit equations, binary forms and curves of genus 2. *Proc. London Math. Soc. (3)*, 75(2):271–307, 1997.

[37] N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[38] N. P. Smart. Determining the small solutions to S-unit equations. *Math. Comp.*, 68(228):1687–1699, 1999.

[39] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135:284–305, 1909.

[40] N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *J. Number Theory*, 31(2):99–132, 1989.

[41] N. Tzanakis and B. M. M. de Weger. Solving a specific Thue-Mahler equation. *Math. Comp.*, 57(196):799–815, 1991.

[42] N. Tzanakis and B. M. M. de Weger. How to explicitly solve a Thue-Mahler equation. *Compositio Math.*, 84(3):223–288, 1992.

[43] K. Wildanger. Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. *J. Number Theory*, 82(2):188–224, 2000.

[44] K. Yu. Linear forms in p-adic logarithms. *Acta Arith.*, 53(2):107–186, 1989.

[45] K. Yu. Linear forms in p-adic logarithms. II. *Compositio Math.*, 74(1):15–113, 1990.

[46] K. Yu. Linear forms in p-adic logarithms. III. *Compositio Math.*, 91(3):241–276, 1994.

[47] K. Yu. p-adic logarithmic forms and group varieties. III. *Forum Math.*, 19(2):187–280, 2007.
Alejandra Alvarado, Department of Mathematics and Computer Science, Eastern Illinois University
E-mail address: aalvarado2@eiu.edu

Angelos Koutisanas, Department of Mathematics, University of British Columbia
E-mail address: koutsis.jr@gmail.com

Beth Malmskog, Department of Mathematics and Computer Science, Colorado College
E-mail address: beth.malmskog@gmail.com

Christopher Rasmussen, Department of Mathematics and Computer Science, Wesleyan University
E-mail address: crasmussen@wesleyan.edu

Christelle Vincent, Department of Mathematics and Statistics, University of Vermont
E-mail address: christelle.vincent@uvm.edu

Mckenzie West, Department of Mathematics, University of Wisconsin Eau Claire
E-mail address: WestMR@uwec.edu