Algebra & Number Theory

Volume 19
2025
No. 4

Efficient resolution of Thue–Mahler equations

Adela Gherga and Samir Siksek

msp

ALGEBRA AND NUMBER THEORY 19:4 (2025)
https://doi.org/10.2140/ant.2025.19.667

msp

Efficient resolution of Thue–Mahler equations

Adela Gherga and Samir Siksek

A Thue–Mahler equation is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}, \quad \gcd(X, Y) = 1$$

where F is an irreducible binary form of degree at least 3 with integer coefficients, a is a nonzero integer and $p_1, \ldots, p_v$ are rational primes. Existing algorithms for resolving such equations require computations in the field $L = \mathbb{Q}(\theta, \theta', \theta'')$, where $\theta, \theta', \theta''$ are distinct roots of $F(X, 1) = 0$. We give a new algorithm that requires computations only in $K = \mathbb{Q}(\theta)$ making it far more suited for higher degree examples. We also introduce a lattice sieving technique reminiscent of the Mordell–Weil sieve that makes it practical to tackle Thue–Mahler equations of higher degree and with larger sets of primes than was previously possible. We give several examples including one of degree 11.

Let $P(m)$ denote the largest prime divisor of an integer $m \geq 2$. As an application of our algorithm we determine all pairs (X, Y) of coprime nonnegative integers such that $P(X^4 - 2Y^4) \leq 100$, finding that there are precisely 49 such pairs.

1. Introduction

Let

$$F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d \tag{1}$$

be a binary form of degree $d \geq 3$ with coefficients $a_i \in \mathbb{Z}$. Suppose F is irreducible over $\mathbb{Q}$. Let a be a nonzero integer and let $p_1, \ldots, p_v$ be distinct primes such that $p_i \nmid a$. The purpose of this paper is to give an efficient algorithm to solve the Thue–Mahler equation

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}, \quad X, Y \in \mathbb{Z}, \gcd(X, Y) = 1, \tag{2}$$

for unknown integers X, Y, and unknown nonnegative integers $z_1, \ldots, z_v$. The set of solutions is known to be finite by a famous result of Mahler [1933] which extends classical work of Thue [1909]. Mahler's theorem is ineffective. The first effective bounds on the size of the solutions are due to Vinogradov and Sprindzhuk [1968] and to Coates [1970]. Vastly improved effective bounds have since been given by Bugeaud and Győry [1996a]. Evertse [1984, Corollary 2] showed that the number of solutions to (2) is at most $2 \times 7^{d^3(2v+3)}$. For $d \geq 6$, this has been improved by Bombieri [1987, Main Theorem] who showed that the number of solutions is at most $16(v+1)^2 \cdot (4d)^{26(v+1)}$.

The authors are supported by the EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).
MSC2020: primary 11D59; secondary 11D61.
Keywords: Thue equation, Thue–Mahler equation, LLL, linear form in logarithms.

Besides being of independent interest, Thue–Mahler equations frequently arise in a number of contexts:

• The problem of determining all elliptic curves over $\mathbb{Q}$ with good reduction outside a given set of primes algorithmically reduces to the problem of solving certain cubic Thue–Mahler equations (here cubic means $d = 3$). The earliest example appears to be due to Agrawal, Coates, Hunt, and van der Poorten [Agrawal et al. 1980] who used it to determine all elliptic curves over $\mathbb{Q}$ of conductor 11. The recent paper of Bennett, Gherga and Rechnitzer [Bennett et al. 2019] gives a systematic and general treatment of this approach. In fact, the link between cubic Thue–Mahler equations and elliptic curves can be used in conjunction with modularity of elliptic curves to give an algorithm for solving cubic Thue–Mahler equations as in the work of von Känel and Matschke [2023, Section 5] and of Kim [2017].

• Many Diophantine problems naturally reduce to the resolution of Thue–Mahler equations. These include the Lebesgue–Nagell equations (e.g., [Cangül et al. 2010; Soydan and Tzanakis 2016]), and Goormaghtigh's equation (e.g., [Bennett et al. 2020]). The most striking of such applications is the reduction, due to Bennett and Dahmen [2013], of asymptotic cubic superelliptic equations to cubic Thue–Mahler equations, via the modularity of Galois representation attached to elliptic curves.

Before the current paper, the only general algorithm for solving Thue–Mahler equations was the one due to Tzanakis and de Weger [1989]. A modern implementation of this algorithm, due Hambrook [2011], has been profitably used to solve a number of low degree Thue–Mahler equations, for example in [Cangül et al. 2010; Soydan and Tzanakis 2016].

Instead of (2), we consider the equation

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}, \quad X, Y \in \mathbb{Z}, \gcd(X, Y) = \gcd(a_0, Y) = 1. \tag{3}$$

Thus we have added the assumption $\gcd(a_0, Y) = 1$, where a_0 is the leading coefficient of F as in (1). This is a standard computational simplification in the subject, and is also applied by Tzanakis and de Weger. There is no loss of generality in adding this assumption in the following sense: an algorithm for solving (3) yields an algorithm for solving (2). To see this, let (X, Y) be a solution to (2) and let $b = \gcd(a_0, Y)$. Write $Y = bY'$ with $Y' \in \mathbb{Z}$. The possible values for b are the divisors of a_0; for each divisor b we need to solve $F(X, bY') = a \cdot p_1^{z_1} \cdots p_v^{z_v}$. Note that $F(X, bY') = bG(X, Y')$ where G has integral coefficients and leading coefficient $a_0' = a_0/b$, which satisfies $\gcd(a_0', Y') = 1$. The equation $bG(X, Y') = a \cdot p_1^{z_1} \cdots p_v^{z_v}$ is impossible unless $b/\gcd(a, b) = p_1^{w_1} \cdots p_v^{w_v}$ where $w_i \geq 0$, in which case

$$G(X, Y') = (a/\gcd(a, b)) \cdot p_1^{z_1 - w_1} \cdots p_v^{z_v - w_v},$$

which is now a Thue–Mahler equation of the form (3).

The approach of Tzanakis and de Weger can be summarized as follows:

(I) First (3) is reduced to a number of ideal equations

$$(a_0 X - \theta Y)\mathcal{O}_K = \mathfrak{a} \cdot \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}. \tag{4}$$

Here θ is a root of the monic polynomial $a_0^{d-1}F(X/a_0, 1)$, and $K = \mathbb{Q}(\theta)$. Moreover, $\mathfrak{a}$ is a fixed ideal of the ring of integers $\mathcal{O}_K$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are fixed prime ideals of $\mathcal{O}_K$. The variables X, Y, $n_1, \ldots, n_s$ represent the unknowns.

(II) Next, each ideal equation (4) is reduced to a number of equations of the form

$$a_0X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \tag{5}$$

where $\tau, \delta_1, \ldots, \delta_r \in K^\times$ are fixed and X, Y, $b_1, \ldots, b_r$ are unknowns.

(III) The next step generates a very large upper bound for the exponents $b_1, \ldots, b_r$ using the theory of real, complex, and p-adic linear forms in logarithms. This bound is then considerably reduced using the LLL algorithm [Lenstra et al. 1982] applied to approximation lattices associated to these linear forms, and finally, all solutions below this reduced bound are found using the algorithm of Fincke and Pohst [1985].

To compute these approximation lattices alluded to in step (III), the algorithm of Tzanakis and de Weger relies on extensive computations in the number field $K' = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$ where $\theta_1, \theta_2, \theta_3$ are distinct roots of $a_0^{d-1}F(X/a_0, 1)$, as well as $\mathfrak{p}$-adic completions of K'. The field K' typically has degree $d(d-1)(d-2)$, making their algorithm impractical if the degree d is large. Even if the degree d is small (say $d = 3$), we have found that the Tzanakis–de Weger algorithm runs into a combinatorial explosion of cases in step (I) if the number of primes v is large, and in step (II) if the class number h of K is large.

In this paper, we present an algorithm that builds on many of the powerful ideas in the paper of Tzanakis and de Weger but avoids computations in number fields other than the field $K = \mathbb{Q}(\theta)$ of degree d, and avoids all computations in p-adic fields or their extensions. The algorithm includes a number of refinements that circumvent the explosion of cases in steps (I) and (II). For example, to each ideal equation (4) we associate at most one equation (5); by contrast, the algorithm of Tzanakis and de Weger, typically associates h^{s-1} equations (5) to each ideal equation (4), where h is the class number of K. Moreover, inspired by the Mordell–Weil sieve (e.g., [Bruin and Stoll 2008; 2010; Bugeaud et al. 2008]), we introduce a powerful "Dirichlet sieve" that vastly improves the determination of the solutions to (5) after the LLL step, even if the remaining bound on the exponents b_i is large.

We have implemented the algorithm described in this paper in the computer algebra system `Magma` [Bosma et al. 1997].[1]

Below we give four examples of Thue–Mahler equations solved using our implementation. Our solutions will always be subject to the assumptions

$$\gcd(X, Y) = \gcd(a_0, Y) = 1.$$

They will be given in the form $[X, Y, z_1, z_2, \ldots, z_v]$. We will revisit these examples later on in the paper to illustrate the differences between our algorithm and that of Tzanakis and de Weger [1989]. We do point out that a number of recent papers also make use of our implementation, or the ideas in the present paper, to solve various Thue–Mahler equations where the degree d, or the number of primes v are large.

[1] Our implementation is available from https://github.com/adelagherga/ThueMahler/tree/master/Code/TMSolver.

For example in [Bennett et al. 2020; 2022; Bennett and Siksek 2023a; 2023b], our algorithm is used to solve Thue–Mahler equations of degrees 5, 20, 7 and 11 respectively.

Example 1.1. An ongoing large-scale computational project, led by Bennett, Cremona, Gherga and Sutherland, aims to provably compute all elliptic curves of conductor at most 10^6. The method combines the approach in [Bennett et al. 2019] with our Thue–Mahler solver described in the current paper. We give an example to illustrate this application. Consider the problem of computing all elliptic curves $E/\mathbb{Q}$ with trivial 2-torsion and conductor

$$771456 = 2^7 \cdot 3 \cdot 7^2 \cdot 41.$$

Applying Theorem 1 of [Bennett et al. 2019] results in 13 cubic Thue–Mahler equations of the form

$$a_0X^3 + a_1X^2Y + a_2XY^2 + a_3Y^3 = 3^{z_1} \cdot 7^{z_2} \cdot 41^{z_3}, \quad \gcd(X, Y) = 1,$$

whose resolution algorithmically yields the desired set of elliptic curves. The coefficients (a_0, a_1, a_2, a_3) for these 13 forms are:

$$(1, 7, 2, -2), \quad (2, 1, 0, 3), \quad (1, 4, 3, 6), \quad (3, 4, 4, 4), \quad (4, 4, 6, 3), \quad (2, 5, 0, 6), \quad (1, 7, 4, 12),$$
$$(3, 3, -1, 7), \quad (3, 7, 14, 14), \quad (1, 3, 17, 43), \quad (8, 12, 13, 8), \quad (4, 1, 12, -6), \quad (3, 9, 5, 19)$$

Our implementation solved all 13 of these Thue–Mahler equations and computed the corresponding elliptic curves in a total of 5.4 minutes on a single core.[2]

For illustration, we consider one of these 13 Thue–Mahler equations:

$$4X^3 + X^2Y + 12XY^2 - 6Y^3 = 3^{z_1} \cdot 7^{z_2} \cdot 41^{z_3}, \quad \gcd(X, Y) = 1.$$

Our implementation solved this in 41 seconds. The solutions are

$$[-3, -7, 1, 0, 1], \quad [-1, -5, 2, 2, 0], \quad [1, -1, 1, 1, 0],$$
$$[3, 1, 1, 2, 0], \quad [5, 11, 0, 2, 0], \quad [9, 17, 1, 2, 1], \quad [19, 23, 5, 3, 0].$$

Of the seven solutions, only $(X, Y) = (1, -1)$ gives rise to elliptic curves of conductor 771456:

$$E_1 : y^2 = x^3 - x^2 + 13655x + 2351833,$$
$$E_2 : y^2 = x^3 - x^2 + 3414x - 295686.$$

Example 1.2. Consider the Thue–Mahler equation

$$7X^3 + X^2Y + 29XY^2 - 25Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}. \tag{6}$$

This in fact is one of the Thue–Mahler equations whose resolution, via the method of [Bennett et al. 2019], is needed to determine all elliptic curves of conductor

$$2^\alpha \cdot 3^\beta \cdot 17 \cdot 37 \cdot 53, \quad \text{where } \alpha \in \{2, 3, 4, 6, 7\} \text{ and } \beta \in \{1, 2\}.$$

[2] See https://github.com/adelagherga/ThueMahler/tree/master/GhSiData/Example1 for full computational details, as well as a list of all corresponding elliptic curves.

The class number of the cubic field associated to the cubic form in (6) is 33. As we shall see later (at the end of Section 4), our approach to dealing with the class group requires us to solve only 30 equations of the form (5), whereas in comparison the method of Tzanakis and de Weger requires the resolution of approximately 80990 equations of the form (5). For now, we merely point out that our implementation solved (6) in 2 minutes. The solutions are

$$[19, -23, 2, 4, 0, 1, 1], \quad [13, -6, 0, 0, 1, 1, 1], \quad [-343, -463, 2, 11, 1, 0, 0],$$
$$[79, -8, 0, 2, 2, 2, 0], \quad [37, -13, 2, 1, 1, 0, 2], \quad [1, 1, 2, 1, 0, 0, 0], \quad [3, 4, 0, 0, 1, 0, 0].$$

Example 1.3. Most explicit examples of the resolution of Thue–Mahler equations (3) found in the literature involve a relatively small set of primes $\{p_1, \ldots, p_v\}$. The following example, aside from being an interesting Diophantine application in its own right, is intended to illustrate that our algorithm can cope with a relatively large set of primes.

For a nonzero integer m, let $P(m)$ denote the maximum prime divisor of m (where we take $P(1) = P(-1) = 0$). In this example, we solve the inequality

$$P(X^4 - 2Y^4) \leq 100, \quad \gcd(X, Y) = 1.$$

Let

$$F(X, Y) = X^4 - 2Y^4.$$

We therefore would like to solve (3) with $a = \pm 1$ and with $p_1, \ldots, p_v$ being the set of primes ≤ 100 (of which there are 25). However, it is clear that if 2 is not a fourth power modulo p, then $p \nmid (X^4 - 2Y^4)$. Thus we reduce to the much smaller set of primes $p \leq 100$ for which 2 is a fourth power. This is the set

$$\{2, 7, 23, 31, 47, 71, 73, 79, 89\}.$$

Therefore the Thue–Mahler equation we shall consider is

$$X^4 - 2Y^4 = \pm 2^{z_1} \cdot 7^{z_2} \cdot 23^{z_3} \cdot 31^{z_4} \cdot 47^{z_5} \cdot 71^{z_6} \cdot 73^{z_7} \cdot 79^{z_8} \cdot 89^{z_9}, \quad \gcd(X, Y) = 1.$$

Our implementation took roughly 3.5 days to solve this Thue–Mahler equation. There are 49 solutions (up to changing the signs of X, Y):

[0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0],	[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
[1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0],	[1, 2, 0, 0, 0, 1, 0, 0, 0, 0, 0],
[1, 3, 0, 1, 1, 0, 0, 0, 0, 0, 0],	[1, 4, 0, 1, 0, 0, 0, 0, 1, 0, 0],
[1, 11, 0, 1, 0, 0, 1, 0, 0, 0, 1],	[2, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0],
[2, 3, 1, 0, 0, 0, 0, 0, 1, 0, 0],	[2, 27, 1, 1, 0, 2, 0, 0, 0, 1, 0],
[3, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0],	[3, 2, 0, 2, 0, 0, 0, 0, 0, 0, 0],
[3, 14, 0, 0, 1, 0, 1, 1, 0, 0, 0],	[4, 3, 1, 0, 0, 0, 1, 0, 0, 0, 0],
[4, 5, 1, 1, 0, 0, 0, 1, 0, 0, 0],	[5, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1],

[5, 8, 0, 1, 1, 0, 1, 0, 0, 0, 0], [6, 5, 1, 0, 1, 0, 0, 0, 0, 0, 0],
[6, 19, 1, 0, 0, 1, 1, 0, 0, 0, 1], [8, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1],
[10, 23, 1, 2, 0, 0, 0, 1, 0, 1, 0], [11, 9, 0, 2, 0, 1, 0, 0, 0, 0, 0],
[11, 20, 0, 0, 0, 0, 1, 0, 1, 0, 1], [15, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0],
[15, 13, 0, 0, 0, 0, 0, 0, 1, 0, 1], [16, 21, 1, 0, 1, 0, 0, 0, 0, 1, 1],
[17, 5, 0, 2, 1, 0, 0, 0, 1, 0, 0], [19, 20, 0, 4, 0, 0, 0, 0, 0, 1, 0],
[21, 11, 0, 0, 0, 1, 0, 0, 2, 0, 0], [22, 49, 1, 0, 1, 1, 0, 0, 0, 0, 2],
[33, 13, 0, 1, 0, 0, 2, 0, 1, 0, 0], [37, 19, 0, 0, 1, 2, 0, 0, 1, 0, 0],
[40, 13, 1, 1, 0, 1, 0, 0, 1, 1, 0], [52, 51, 1, 2, 1, 1, 0, 0, 0, 0, 1],
[53, 44, 0, 1, 1, 1, 0, 0, 0, 1, 0], [59, 56, 0, 0, 0, 1, 1, 1, 1, 0, 0],
[61, 48, 0, 1, 0, 0, 0, 1, 1, 0, 1], [66, 101, 1, 0, 2, 1, 0, 0, 1, 1, 0],
[68, 43, 1, 1, 1, 2, 1, 0, 0, 0, 0], [95, 58, 0, 1, 0, 1, 1, 0, 1, 1, 0],
[118, 101, 1, 2, 1, 0, 0, 1, 0, 0, 1], [142, 57, 1, 1, 3, 1, 0, 0, 1, 0, 0],
[162, 137, 1, 2, 0, 0, 2, 0, 1, 0, 0], [181, 124, 0, 0, 1, 0, 1, 0, 0, 2, 1],
[221, 295, 0, 0, 2, 0, 1, 0, 1, 1, 1], [281, 199, 0, 1, 1, 0, 1, 1, 1, 1, 0],
[286, 283, 1, 3, 1, 0, 0, 0, 3, 0, 0], [389, 96, 0, 4, 0, 1, 1, 0, 1, 0, 1],
[420, 437, 1, 0, 0, 1, 3, 0, 1, 0, 1].

Example 1.4. All examples found in the literature are of Thue–Mahler equations where the form F has the property that the field $K' = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$ (defined above) have small degree. As indicated above, a distinguishing feature of our algorithm is that the computations are carried out in the much smaller extension $K = \mathbb{Q}(\theta)$ (also defined above). Our last example is intended to illustrate this difference. Consider the Thue–Mahler equation,

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}.$$

As usual, we let F denote the form on the left-hand side. The Galois group of F is S_{11}, therefore the field K has degree 11, whereas the field K' has degree $11 \times 10 \times 9 = 990$. Our program solved this Thue–Mahler equation in around 6.8 hours. However this time was almost entirely taken up with the computation of the class group and the units of K. Once the class group and unit computations were complete, it took only 3.6 minutes to provably determine the solutions. These are

$$[0, -1, 1, 0, 0, 0, 0], \quad [1, -1, 1, 1, 1, 0, 0], \quad [1, 1, 5, 0, 0, 0, 0], \quad [1, 2, 0, 3, 0, 1, 1].$$

1.1. ***Notation and organization of the paper.*** As before $F \in \mathbb{Z}[X, Y]$ will be a binary form of degree $d \geq 3$, irreducible in $\mathbb{Q}[X, Y]$, and with coefficients $a_0, \ldots, a_d$ as in (1). Let a be a nonzero integer and $p_1, \ldots, p_v$

be distinct primes satisfying $p_i \nmid a$. Let

$$f(x) = a_0^{d-1} \cdot F(x/a_0, 1) = x^d + a_1 x^{d-1} + a_0 a_2 x^{d-2} + \cdots + a_0^{d-1} a_d.$$

This is an irreducible monic polynomial with coefficients in $\mathbb{Z}$. Let θ be a root of f and let $K = \mathbb{Q}(\theta)$. Note that K is a number field of degree d. Write $\mathcal{O}_K$ for the ring of integers of K. We can rewrite our Thue–Mahler equation (3) as

$$\text{Norm}(a_0 X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}. \tag{7}$$

Note that we do not assume that $(a_0, p_i) = 1$.

The paper is organized as follows:

(a) In Section 2 we consider the decomposition of the ideal $(a_0 X - \theta Y)\mathcal{O}_K$ as a product of prime ideals. In particular, we introduce an algorithm to compare and restrict the possible valuations of all prime ideals above each of $p_1, \ldots, p_v$.

(b) We summarize the results of applying this algorithm in Section 3, wherein we reduce solving (7) to solving a family of ideal equations of the form (4).

(c) In Section 4, we show that such ideal equations are either impossible due to a class group obstruction, or reduce to a single equation of the form (5). The remainder of the paper is devoted to solving equations of the form (5) where the unknowns are coprime integers X, Y and nonnegative integers $b_1, \ldots, b_r$.

(d) In Section 5, we recall key theorems from the theory of lower bounds for linear forms in complex and p-adic logarithms due to Matveev and to Yu.

(e) In Section 6, with the help of these theorems, we obtain a very large upper bound on the exponents $b_1, \ldots, b_r$ in (5).

(f) In Section 7 we show how an application of close vector algorithms allows us to obtain a substantially improved bound on the $\mathfrak{p}$-adic valuation of $a_0 X - \theta Y$ for any prime $\mathfrak{p}$. This step avoids the $\mathfrak{p}$-adic logarithms of earlier approaches.

(g) Section 8 uses the real and complex embeddings of K applied to (5) to obtain $d-2$ approximate relations involving the exponents b_i. In Section 9, we set up an "approximation lattice" using these $d-2$ approximate relations. We explain how close vector algorithms can be used to substantially reduce our bound for the exponents $b_1, \ldots, b_r$ in (5). Earlier approaches used just one of the $d-2$ relations to construct the approximation lattice, but we explain why using just one approximate relation can fail in certain situations.

(h) Steps (f) and (g) are applied repeatedly until no further improvements in the bounds are possible. In Section 10 we introduce an analogue of the Mordell–Weil sieve, which we call the "Dirichlet sieve" which is capable of efficiently sieving for the solutions up to the remaining bounds, thereby finally resolving the Thue–Mahler equation (3).

2. The p-part of $(a_0X - \theta Y)\mathcal{O}_K$

If $\mathfrak{c}$ is a fractional ideal of $\mathcal{O}_K$, and p is a rational prime, we define the *p-part of* $\mathfrak{c}$ to be the fractional ideal

$$\prod_{\mathfrak{p} \mid p} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{c})}.$$

For each rational prime $p \in \{p_1, \ldots, p_v\}$ of (7), we want to study the p-part of $(a_0X - \theta Y)\mathcal{O}_K$ coming from the prime ideals above p. The so-called prime ideal removal lemma in Tzanakis and de Weger compares the possible valuations of $(a_0X - \theta Y)\mathcal{O}_K$ at two prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \mid p$ to help cut down the possibilities for the p-part of $(a_0X - \theta Y)\mathcal{O}_K$. However if $\mathfrak{p}_1 \mid (a_0X - \theta Y)\mathcal{O}_K$ then this restricts the values of X and Y modulo p. Indeed, any choice of X and Y modulo p affects the valuations of $(a_0X - \theta Y)\mathcal{O}_K$ at all primes $\mathfrak{p} \mid p$. So we study all valuations at the same time, not just two of them. This enables us to give a much smaller list of possibilities for the p-part of $(a_0X - \theta Y)\mathcal{O}_K$ than in Tzanakis and de Weger, as we will see in Section 4.

Definition 2.1. Let p be a rational prime. Let L_p be a subset of the ideals $\mathfrak{b}$ supported at the prime ideals above p. Let M_p be a subset of the set of pairs $(\mathfrak{b}, \mathfrak{p})$ where $\mathfrak{b}$ is supported at the prime ideals above p, and $\mathfrak{p} \mid p$ is a prime ideal satisfying $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$, where $e(\mathfrak{p} \mid p)$ and $f(\mathfrak{p} \mid p)$ are, respectively, the ramification index and inertial degree of $\mathfrak{p}$ over p. We call the pair L_p, M_p *satisfactory* if for every solution (X, Y) to (3),

(i) either the p-part of $(a_0X - \theta Y)\mathcal{O}_K$ is in L_p, or

(ii) there is a pair $(\mathfrak{b}, \mathfrak{p}) \in M_p$ and a nonnegative integer l such that the p-part of $(a_0X - \theta Y)\mathcal{O}_K$ is equal to $\mathfrak{b}\mathfrak{p}^l$.

At this point the definition is perhaps mysterious. Lemma 2.4 and the following remark give an explanation for the definition and for the existence of finite satisfactory sets L_p, M_p. We will give an algorithm to produce (hopefully small) satisfactory sets L_p and M_p. Before that we embark on a simplification. The expression $a_0X - \theta Y$ is a linear form in two variables X, Y. It is easier to scale so that we are dealing with a linear expression in just one variable.

For a rational prime p, let

$$\mathbb{Z}_{(p)} = \{U \in \mathbb{Q} : \mathrm{ord}_p(U) \geq 0\}.$$

Definition 2.2. Let p be a rational prime. Let $\alpha \in K$ and $\beta \in K^\times$. Let L be a subset of the ideals $\mathfrak{b}$ supported on the prime ideals of $\mathcal{O}_K$ above p. Let M be a subset of the set of pairs $(\mathfrak{b}, \mathfrak{p})$ where $\mathfrak{b}$ is supported on the prime ideals above p, and where $\mathfrak{p}$ is a prime ideal above p satisfying $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$. We call L, M *adequate for* (α, β) if for every $U \in \mathbb{Z}_{(p)}$,

(i) either the p-part of $\beta \cdot (U + \alpha)\mathcal{O}_K$ is in L, or

(ii) there is a pair $(\mathfrak{b}, \mathfrak{p}) \in M$ and a nonnegative integer l such that the p-part of $\beta \cdot (U + \alpha)\mathcal{O}_K$ equals $\mathfrak{b}\mathfrak{p}^l$.

Lemma 2.3. *Let L, M be adequate for $(-\theta/a_0, a_0)$ and let $L_p = L \cup \{1 \cdot \mathcal{O}_K\}$ and $M_p = M$. Then the pair L_p, M_p is satisfactory.*

Proof. Recall that $\gcd(X, Y) = \gcd(a_0, Y) = 1$.

If $p \mid Y$ then $\mathrm{ord}_{\mathfrak{p}}(Y) > 0$ for any $\mathfrak{p}$ above p, and thus

$$\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) = 0.$$

If $p \nmid Y$, we write

$$U = \frac{X}{Y}, \quad \alpha = \frac{-\theta}{a_0}, \quad \beta = a_0.$$

Then $U \in \mathbb{Z}_{(p)}$ and $\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) = \mathrm{ord}_{\mathfrak{p}}(\beta \cdot (U + \alpha))$ for all prime ideals $\mathfrak{p}$ above p. Thus the p-part of $\beta \cdot (U + \alpha)$ is equal to the p-part of $\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y)$.

The lemma follows. □

We now demystify Definitions 2.1 and 2.2.

Lemma 2.4. *Let p be a rational prime and γ a generator of K. Then there is a bound B depending only on p and γ such that the following hold*:

(a) *For any $U \in \mathbb{Z}_{(p)}$ and any pair of distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ lying over p,*

$$\mathrm{ord}_{\mathfrak{p}_1}(U + \gamma) \le B \quad \text{or} \quad \mathrm{ord}_{\mathfrak{p}_2}(U + \gamma) \le B.$$

(b) *For any $U \in \mathbb{Z}_{(p)}$ and any prime ideal $\mathfrak{p}$ over p with $e(\mathfrak{p} \mid p) \ne 1$ or $f(\mathfrak{p} \mid p) \ne 1$,*

$$\mathrm{ord}_{\mathfrak{p}}(U + \gamma) \le B.$$

Proof. Let $\mathfrak{p}$ be a prime ideal above p, and suppose that $\mathrm{ord}_{\mathfrak{p}}(U + \gamma)$ is unbounded for $U \in \mathbb{Z}_{(p)}$. Thus there is an infinite sequence $\{U_i\} \subset \mathbb{Z}_{(p)}$ such that

$$\lim_{i \to \infty} \mathrm{ord}_{\mathfrak{p}}(U_i + \gamma) = \infty.$$

However, $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$, where the latter is compact. Thus $\{U_i\}$ contains an infinite subsequence $\{U_{n_i}\}$ converging to, say, $U \in \mathbb{Z}_p$. Write $\phi_{\mathfrak{p}} : K \hookrightarrow \mathbb{C}_p$ for the embedding of K corresponding to the prime ideal $\mathfrak{p}$. It follows that $\phi_{\mathfrak{p}}(\gamma) = -U \in \mathbb{Z}_p$. Recall the assumption that $K = \mathbb{Q}(\gamma)$. Thus $K_{\mathfrak{p}}$, the topological closure of $\phi_{\mathfrak{p}}(K)$ in $\mathbb{C}_p$, is in fact $\mathbb{Q}_p$. Thus $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$. This proves (b).

For (a), suppose that there is a pair of distinct primes $\mathfrak{p}_1, \mathfrak{p}_2$ above p and an infinite sequence $\{U_i\} \subset \mathbb{Z}_{(p)}$ such that

$$\lim_{i \to \infty} \mathrm{ord}_{\mathfrak{p}_1}(U_i + \gamma) = \lim_{i \to \infty} \mathrm{ord}_{\mathfrak{p}_2}(U_i + \gamma) = \infty. \tag{8}$$

Again, let $\{U_{n_i}\}$ be an infinite subsequence of $\{U_i\}$ converging to, say, $U \in \mathbb{Z}_p$. Then $\phi_{\mathfrak{p}_1}(\gamma) = -U = \phi_{\mathfrak{p}_2}(\gamma)$. As $K = \mathbb{Q}(\gamma)$, the embeddings $\phi_{\mathfrak{p}_1}, \phi_{\mathfrak{p}_2}$ are equal, contradicting $\mathfrak{p}_1 \ne \mathfrak{p}_2$. □

Remark. We apply Lemma 2.4 with $\gamma = \alpha$ as in Lemma 2.3 in order to explain Definitions 2.1 and 2.2. The valuation of $\beta \cdot (U + \alpha)$ can be arbitrarily large only for those $\mathfrak{p}$ above p that satisfy $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$, and if it is sufficiently large for one such $\mathfrak{p}$ then it is bounded for all others. Thus there must exist finite adequate sets L, M. We now turn to the task of giving an algorithm to determine such adequate sets L, M.

Lemma 2.5. *Let $\alpha \in K$ and let p be a rational prime. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p. Suppose $U \in \mathbb{Z}_{(p)}$ and*

$$\mathrm{ord}_{\mathfrak{p}}(U+\alpha) > \min\{0, \mathrm{ord}_{\mathfrak{p}}(\alpha)\}. \tag{9}$$

Then the following hold:

(i) $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$.

(ii) *The image of α in $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ belongs to the prime subfield $\mathbb{F}_p$. In particular, there is a unique $u \in \{0, \ldots, p-1\}$ such that $u \equiv -\alpha \pmod{\mathfrak{p}}$.*

(iii) *With u as in* (ii), *$U = pU' + u$ where $U' \in \mathbb{Z}_{(p)}$.*

Proof. Since $U \in \mathbb{Z}_{(p)}$, we have $\mathrm{ord}_{\mathfrak{p}}(U) \geq 0$. If $\mathrm{ord}_{\mathfrak{p}}(\alpha) < 0$, it follows that $\mathrm{ord}_{\mathfrak{p}}(U+\alpha) = \mathrm{ord}_{\mathfrak{p}}(\alpha)$, contradicting (9). Thus $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$, proving (i).

Write $\bar{\alpha}$ for the image of α in $\mathbb{F}_{\mathfrak{p}}$, and suppose this does not belong to the prime subfield $\mathbb{F}_p$. In particular $\mathrm{ord}_{\mathfrak{p}}(\alpha) = 0$. However, the image $\overline{U}$ of U in $\mathbb{F}_{\mathfrak{p}}$ does belong to $\mathbb{F}_p$. Thus $U \not\equiv -\alpha \pmod{\mathfrak{p}}$, or equivalently $\mathrm{ord}_{\mathfrak{p}}(U+\alpha) = 0$, contradicting (9). We deduce that $\bar{\alpha} \in \mathbb{F}_p$, and thus (ii) holds.

Now, let u be as in (ii). By (9), we have $\mathrm{ord}_{\mathfrak{p}}(U+\alpha) > 0$, and thus $\overline{U} = -\bar{\alpha} = \bar{u}$. But $\overline{U}, \bar{u} \in \mathbb{F}_p$. Therefore, $\mathrm{ord}_p(U-u) > 0$, and so $U = pU' + u$ for some $U' \in \mathbb{Z}_{(p)}$. □

Algorithm 2.6. *Given p a rational prime, $\alpha \in K$ satisfying $K = \mathbb{Q}(\alpha)$, and $\beta \in K^{\times}$, to compute L, M adequate for (α, β)*:

Step (a) *Let*

$$\mathcal{B} = \{\mathfrak{p} \mid p : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ and the image of } \alpha \text{ in } \mathbb{F}_{\mathfrak{p}} \text{ belongs to } \mathbb{F}_p\},$$

and

$$\mathfrak{b} = \prod_{\mathfrak{p} \mid p} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\beta) + \min\{0, \mathrm{ord}_{\mathfrak{p}}(\alpha)\}}.$$

Step (b) *If $\mathcal{B} = \varnothing$ then return $L = \{\mathfrak{b}\}$, $M = \varnothing$ and terminate the algorithm.*

Step (c) *If $\mathcal{B}$ consists of a single prime ideal $\mathfrak{p}'$ satisfying $e(\mathfrak{p}' \mid p) = f(\mathfrak{p}' \mid p) = 1$ then return $L = \varnothing$, $M = \{(\mathfrak{b}, \mathfrak{p}')\}$ and terminate the algorithm.*

Step (d) *Let*

$$\mathcal{U} = \{0 \leq u \leq p-1 : \text{there is some } \mathfrak{p} \in \mathcal{B} \text{ such that } \alpha \equiv -u \pmod{\mathfrak{p}}\}.$$

Loop through the elements $u \in \mathcal{U}$. For each u, use Algorithm 2.6 to compute adequate L_u, M_u for the pair $((u+\alpha)/p, p\beta)$.

Step (d1) *If $\mathcal{U} = \{0, 1, 2, \ldots, p-1\}$ then return*

$$L = \bigcup_{u \in \mathcal{U}} L_u, \quad M = \bigcup_{u \in \mathcal{U}} M_u, \tag{10}$$

and terminate the algorithm.

Step (d2) *Else, return*

$$L = \{\mathfrak{b}\} \cup \bigcup_{u \in \mathcal{U}} L_u, \quad M = \bigcup_{u \in \mathcal{U}} M_u, \tag{11}$$

and terminate the algorithm.

Remarks. • Algorithm 2.6 is recursive. If the hypotheses of (b) and (c) fail then the algorithm replaces the linear form $\beta \cdot (U + \alpha)$ with a number of linear forms

$$p\beta \cdot (U' + (u + \alpha)/p) = \beta \cdot (pU' + u + \alpha).$$

In essence we are replacing $\mathbb{Z}_{(p)}$ with a number of the cosets of $p\mathbb{Z}_{(p)}$. The algorithm is then applied to each of these linear forms individually.

- Note that the number of prime ideals $\mathfrak{p}$ above p is bounded by the degree $[K : \mathbb{Q}]$. In particular, $\#\mathcal{U} \leq [K : \mathbb{Q}]$. Therefore the number of branches at each iteration of the algorithm is bounded independently of p.

Proposition 2.7. *Suppose $\beta \in K^\times$, $\alpha \in K$ and moreover, $K = \mathbb{Q}(\alpha)$. Then Algorithm 2.6 terminates in finite time and produces adequate L, M for (α, β).*

Proof. Let $\mathcal{B}$ and $\mathfrak{b}$ be as in Step (a). Observe that, for any $\mathfrak{p}$ above p,

$$\mathrm{ord}_{\mathfrak{p}}(\beta \cdot (U + \alpha)) \geq \mathrm{ord}_{\mathfrak{p}}(\beta) + \min\{0, \mathrm{ord}_{\mathfrak{p}}(\alpha)\} = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}).$$

It follows that $\mathfrak{b}$ divides the p-part of $\beta \cdot (U + \alpha)$. Lemma 2.5 tells us that

$$\mathrm{ord}_{\mathfrak{p}}(\beta \cdot (U + \alpha)) = \mathrm{ord}_{\mathfrak{p}}(\beta) + \min\{0, \mathrm{ord}_{\mathfrak{p}}(\alpha)\} = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) \tag{12}$$

for all prime ideals $\mathfrak{p}$ lying above p, except possibly for $\mathfrak{p} \in \mathcal{B}$. If $\mathcal{B} = \varnothing$ (i.e., the hypothesis of (b) is satisfied), then the p-part of $\beta \cdot (U + \alpha)$ is $\mathfrak{b}$, and hence the pair $L = \{\mathfrak{b}\}$, $M = \varnothing$ is adequate for (α, β). If $\mathcal{B} = \{\mathfrak{p}'\}$ where $e(\mathfrak{p}' \mid p) = f(\mathfrak{p}' \mid p) = 1$ (i.e., the hypothesis of step (c) is satisfied) then the p-part of $\beta \cdot (U + \alpha)$ has the form $\mathfrak{b} \cdot \mathfrak{p}'^l$ for some $l \geq 0$. Hence $L = \varnothing$, $M = \{(\mathfrak{b}, \mathfrak{p}')\}$ are adequate for (α, β).

Suppose the hypotheses of steps (b) and (c) fail. Let $\mathcal{U}$ be as in step (d). If $U \equiv u \pmod{p}$ for some $u \in \mathcal{U}$, then $U = pU' + u$ for some $U' \in \mathbb{Z}_{(p)}$. Thus $\beta \cdot (U + \alpha) = p\beta \cdot (U' + (u + \alpha)/p)$, and so naturally the p-parts of $\beta \cdot (U + \alpha)$ and $p\beta \cdot (U' + (u + \alpha)/p)$ agree. In (d1), $\mathcal{U}$ represents all of the congruence classes modulo p, and this justifies (10). In (d2), $\mathcal{U}$ represents some of the congruence classes. If $u \notin \mathcal{U}$, then by Lemma 2.5, the equality (12) holds for all prime ideals $\mathfrak{p}$ above p, and hence $\mathfrak{b}$ is the p-part of $\beta \cdot (U + \alpha)$. This justifies (11).

Next we show that the algorithm terminates in finitely many steps. Suppose otherwise. Then there will be an infinite sequence of $u_i \in \{0, 1, \ldots, p - 1\}$ and pairs (α_i, β_i) with

$$\alpha_0 = \alpha, \quad \beta_0 = \beta, \quad \alpha_{i+1} = \frac{u_i + \alpha_i}{p}, \quad \beta_{i+1} = p\beta_i.$$

Let us denote by $\mathcal{B}_i$ the set $\mathcal{B}$ for the pair (α_i, β_i). It is easy to see from the definition that $\mathcal{B}_{i+1} \subseteq \mathcal{B}_i$. Suppose $\mathfrak{p}$ belongs to infinitely many of the $\mathcal{B}_i$. Then, infinitely often, $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) \geq 0$. However,

$$\alpha = \alpha_0 = -u_0 - u_1 p - u_2 p^2 - \cdots - u_{i-1} p^{i-1} + p^i \alpha_i.$$

Let $\mu = -u_0 - u_1 p - \cdots \in \mathbb{Z}_p$. Let $\phi_{\mathfrak{p}} : K \hookrightarrow \mathbb{C}_p$ be the embedding corresponding to $\mathfrak{p}$. Then $\phi_{\mathfrak{p}}(\alpha) = \mu$. Since $K = \mathbb{Q}(\alpha)$, the embedding $\phi_{\mathfrak{p}}$ is determined by the image of α. Since $\phi_{\mathfrak{p}} \neq \phi_{\mathfrak{p}'}$ whenever $\mathfrak{p} \neq \mathfrak{p}'$, we see that $\mathcal{B}_i$ consists of at most one prime for i sufficiently large. For such a prime, we must have $\phi_{\mathfrak{p}}(K) = \mathbb{Q}_p$ so that $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$. Thus for sufficiently large i the algorithm must terminate at Step (b) or Step (c), giving a contradiction. □

Following Lemma 2.3, we thus let $L_p = L \cup \{1 \cdot \mathcal{O}_K\}$ and $M_p = M$, where we compute L and M using Algorithm 2.6 with $\alpha = -\theta/a_0$ and $\beta = a_0$.

Refinements. Let L_p, M_p be a satisfactory pair (for example, produced by Algorithm 2.6). We explain here some obvious refinements that will reduce or simplify these sets, whilst maintaining the satisfactory property:

- If some pair $(\mathfrak{b}, \mathfrak{p})$ is in M_p then we may replace this with the pair $(\mathfrak{b}', \mathfrak{p})$ where

$$\mathfrak{b}' = \frac{\mathfrak{b}}{\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})}}.$$

- If some $\mathfrak{b}$ is contained in L_p, and some $(\mathfrak{b}', \mathfrak{p})$ is contained in M_p with $\mathfrak{b}' \mid \mathfrak{b}$ and $\mathfrak{b}/\mathfrak{b}' = \mathfrak{p}^w$ for some $w \geq 0$, then we may delete $\mathfrak{b}$ from L_p.

- Suppose $p \mid a_0$. Observe that if $\mathfrak{b} \in L_p$ is the p-part of $(a_0 X - \theta Y)\mathcal{O}_K$ then $\mathrm{ord}_p(\mathrm{Norm}(a_0 X - \theta Y)) = \mathrm{ord}_p(\mathrm{Norm}(\mathfrak{b}))$. However, it is clear that $\mathrm{ord}_p(\mathrm{Norm}(a_0 X - \theta Y)) \geq (d-1)\,\mathrm{ord}_p(a_0)$. Thus, we may delete $\mathfrak{b}$ from L_p if $\mathrm{ord}_p(\mathrm{Norm}(\mathfrak{b})) < (d-1)\,\mathrm{ord}_p(a_0)$.

3. An equation in ideals

Let (X, Y) be a solution of (3). For every $p \in P := \{p_1, \ldots, p_v\}$ we let L_p, M_p be a corresponding satisfactory pair. From Definition 2.1, we see that there is some partition $P = P_1 \cup P_2$ such that for every $p \in P_1$, the p-part of $(a_0 X - \theta Y)\mathcal{O}_K$ equals $\mathfrak{b}\mathfrak{p}^l$ for some $(\mathfrak{b}, \mathfrak{p}) \in M_p$ and $l \geq 0$, and for every $p \in P_2$, it equals some $\mathfrak{b} \in L_p$. Let $P = P_1 \cup P_2$ be a partition of P and write

$$P_1 = \{q_1, \ldots, q_s\}, \quad P_2 = \{q_{s+1}, \ldots, q_v\}.$$

Let $\mathcal{Z}_{P_1, P_2}$ be the set of all pairs $(\mathfrak{a}, S)$ such that there are $(\mathfrak{b}_i, \mathfrak{p}_i) \in M_{q_i}$ for $1 \leq i \leq s$, and $\mathfrak{b}_j \in L_{q_j}$ for $s+1 \leq j \leq v$ satisfying

$$\mathfrak{a} = \mathfrak{b}_0 \cdot \mathfrak{b}_1 \mathfrak{b}_2 \cdots \mathfrak{b}_s \cdot \mathfrak{b}_{s+1} \cdots \mathfrak{b}_v, \quad S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\},$$

where $\mathfrak{b}_0$ denotes an ideal of $\mathcal{O}_K$ of norm

$$R = \left| \frac{a \cdot a_0^{d-1}}{\gcd(\mathrm{Norm}(\mathfrak{b}_1 \cdots \mathfrak{b}_v), a \cdot a_0^{d-1})} \right|.$$

Let

$$\mathcal{Z} := \bigcup_{P_1 \subseteq P} \mathcal{Z}_{P_1, P-P_1}.$$

Proposition 3.1. *Let (X, Y) be a solution to* (3). *Then there is some $(\mathfrak{a}, S) \in \mathcal{Z}$ such that*

$$(a_0 X - \theta Y)\mathcal{O}_K = \mathfrak{a} \cdot \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \tag{13}$$

where $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, and $n_1, \ldots, n_s$ are nonnegative integers. Moreover, the set S has the following properties:

(i) $e(\mathfrak{p}_i \mid q_i) = f(\mathfrak{p}_i \mid q_i) = 1$ *for* $1 \le i \le s$.

(ii) *Let* $1 \le i \le s$. *Let p be the unique rational prime below $\mathfrak{p}_i$. Then $\mathfrak{p}_j \nmid p$ for all* $1 \le j \le s$ *with* $j \ne i$.

Proof. The claims follow from the definitions of $\mathcal{Z}$ and M_p. □

To solve (3), we will solve (13) for every possible choice of $(\mathfrak{a}, S) \in \mathcal{Z}$.

Remark. Observe that for any $(\mathfrak{a}, S) \in \mathcal{Z}$, there may be several possibilities for $\mathfrak{b}_0$. Let $\mathcal{R}$ denote the set of all ideals $\mathfrak{b}_0$ having norm R for some $(\mathfrak{a}, S) \in \mathcal{Z}$. Here, we provide a simple refinement to cut down the number of ideals in $\mathcal{R}$. In particular, we apply Algorithm 2.6 and Lemma 2.3 to each rational prime p dividing R, generating the corresponding sets M_p and L_p. For each $\mathfrak{b}_0 \in \mathcal{R}$, if the p-part of $\mathfrak{b}_0$ cannot be made up of any of the elements of M_p or L_p, we may remove $\mathfrak{b}_0$ from $\mathcal{R}$. Moreover, if this process yields $\mathcal{R} = \varnothing$, we may remove $(\mathfrak{a}, S)$ from $\mathcal{Z}$.

4. Making the ideals principal

From now on we fix $(\mathfrak{a}, S) \in \mathcal{Z}$ and we focus on a solution of (13). The method of Tzanakis and de Weger [1989] reduces (13) to at most $(m/2) \cdot h^s$ S-unit equations, where m is the number of roots of unity and h is the class number of K. Our method, explained below, gives at most only $m/2$ S-unit equations.

Given an ideal $\mathfrak{b}$ of $\mathcal{O}_K$, we denote its class in the class group $\mathrm{Cl}(K)$ by $[\mathfrak{b}]$.

Lemma 4.1. *Let*

$$\phi : \mathbb{Z}^s \to \mathrm{Cl}(K), \quad (m_1, \ldots, m_s) \mapsto [\mathfrak{p}_1]^{m_1} \cdots [\mathfrak{p}_s]^{m_s} :$$

(a) *If $[\mathfrak{a}]^{-1}$ is not in the image of ϕ then* (13) *has no solutions.*

(b) *Suppose $[\mathfrak{a}]^{-1} = \phi(\boldsymbol{r})$, where $\boldsymbol{r} = (r_1, \ldots, r_s)$. Let ζ be a generator of the roots of unity in K, and suppose it has order m. Let $\delta_1, \ldots, \delta_r$ be a basis for the group of S-units $\mathcal{O}_S^\times$ modulo the torsion*

subgroup $\langle\zeta\rangle$. *Let* α *be a generator of the principal ideal* $\mathfrak{a}\cdot\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s}$. *Let* (X, Y) *satisfy* (13). *Then, after possibly replacing* (X, Y) *by* $(-X, -Y)$, *we have*

$$a_0X-\theta Y=\tau\cdot\delta_1^{b_1}\cdots\delta_r^{b_r}, \tag{14}$$

where $\tau=\zeta^a\cdot\alpha$ *with* $0\le a\le\frac{m}{2}-1$, *and* $b_1,\dots,b_r\in\mathbb{Z}$.

Proof. Note that if (13) has a solution $\boldsymbol{n}=(n_1,\dots,n_s)$ then

$$\phi(\boldsymbol{n})=[\mathfrak{a}]^{-1}.$$

This proves (a). For (b), suppose $[\mathfrak{a}]^{-1}=\phi(r_1,\dots,r_s)$. Thus $\mathfrak{a}\cdot\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s}$ is principal and we let α be a generator. Then the fractional ideal $((a_0X-\theta Y)/\alpha)\mathcal{O}_K$ is supported on $S=\{\mathfrak{p}_1,\dots,\mathfrak{p}_s\}$. Hence $(a_0X-\theta Y)/\alpha\in\mathcal{O}_S^\times$. Now $\zeta,\delta_1,\dots,\delta_r$ is a set of generators for the S-unit group, where $\delta_1,\dots,\delta_r$ is in fact a basis for $\mathcal{O}_S^\times/\langle\zeta\rangle$. Thus (14) holds for some $0\le a\le m-1$, and $b_1,\dots,b_r\in\mathbb{Z}$. However $\zeta^{m/2}=-1$. Thus we can suppose $0\le a\le m/2-1$ by replacing (X, Y) by $(-X, -Y)$ if necessary. □

Lemma 4.2. *The denominator of the fractional ideal* $\tau\mathcal{O}_K$ *is supported on the set of prime ideals* $S=\{\mathfrak{p}_1,\dots,\mathfrak{p}_s\}$.

Proof. This follows immediately from (14) since $\delta_1,\dots,\delta_r$ are S-units. □

We have reduced the task of solving our original Thue–Mahler equation (3) to solving equations of the form

$$a_0X-\theta Y=\tau\cdot\delta_1^{b_1}\cdots\delta_r^{b_r}, \tag{15}$$

subject to the conditions

$$X,Y\in\mathbb{Z},\quad \gcd(X,Y)=1,\quad \gcd(a_0,Y)=1,\quad b_i\in\mathbb{Z}. \tag{16}$$

For technical reasons we would like to exclude the case $b_1=b_2=\cdots=b_r=0$; of course we can trivially test if this case leads to a solution. Hence we shall henceforth suppose in addition to (16) that

$$\max\{|b_1|,\dots,|b_r|\}\ge 1. \tag{17}$$

We will tackle each of these equations (15) separately. In [Tzanakis and de Weger 1989], the authors work in the field generated by three conjugates of θ and its completions. This is fine theoretically but difficult computationally. We will work with that extension theoretically simply to obtain a bound for

$$B:=\max\{|b_1|,\dots,|b_r|\}. \tag{18}$$

(The reason for restriction (17) is that in Section 6 we work with $\log B$). To reduce the bound, we will need to carry out certain computations; these will take place only in K, $\mathbb{R}$, $\mathbb{C}$, but not in extensions of K, and certainly not in extensions of $\mathbb{Q}_p$.

To obtain our initial bound for B we shall mostly follow ideas found in [Bugeaud and Győry 1996b; Bugeaud et al. 2008; Gallegos-Ruiz 2011]. However, we have a key advantage that will allow us to obtain

	$\#\mathcal{Z}$	number of $(\tau, \delta_1, \ldots, \delta_r)$	rank frequencies
Example 1.1	16	16	(1, 2), (2, 6), (3, 6), (4, 2)
Example 1.2	32	30	(2, 8), (3, 12), (4, 8), (5, 2)
Example 1.3	4096	4096	(10, 4096)
Example 1.4	2	2	(9, 1), (10, 1)

Table 1. This table gives the sizes of the set $\mathcal{Z}$ and the number of resulting $(\tau, \delta_1, \ldots, \delta_r)$ for Examples 1.1–1.4. The last column is a list of pairs (r, t) meaning there are t cases where the S-unit rank is r.

sharper bounds: namely we assume knowledge of the S-unit basis $\delta_1, \ldots, \delta_r$ rather than working with estimates for the size of a basis.

4.1. ***Convention on the choice of S-unit basis.*** As before let ζ be a generator for the roots of unity in $\mathcal{O}_K^\times$. We note that the unit group $\mathcal{O}_K^\times$ is a subgroup of the S-unit group $\mathcal{O}_S^\times$. Moreover, it is saturated in the sense that the quotient $\mathcal{O}_S^\times/\mathcal{O}_K^\times$ is torsion-free. Hence there is a basis $\delta_1, \ldots, \delta_r$ for $\mathcal{O}_S^\times/\langle\zeta\rangle$ such that $\delta_1, \ldots, \delta_{u+v-1}$ is a basis for $\mathcal{O}_K^\times/\langle\zeta\rangle$, where (u, v) is the signature of K. We shall in fact work with such a basis.

4.2. ***Examples continued.*** Table 1 gives some data for Examples 1.1–1.4. At this stage of the algorithm, we would like to stress the main difference between our approach and that of Tzanakis and de Weger [1989]. When dealing with

$$(a_0X - \theta Y)\mathcal{O}_K = \mathfrak{a} \cdot \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s},$$

they write each exponent n_i as $n_i = k_i h_i + m_i$, where h_i is the order of $\mathfrak{p}_i$ in the class group of $\mathcal{O}_K$ and $0 \le m_i \le h_i - 1$. Now $\mathfrak{p}_i^{h_i}$ is principal and we may write it as $(\beta_i)\mathcal{O}_K$. It follows from (13) that $\mathfrak{a} \cdot \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_s^{m_s}$ is principal. Clearly $h_i \mid h$ and there are at most h^s possibilities for this ideal. In the worst case, we expect around h^{s-1} ideals to be principal, and so of the form $(\tau)\mathcal{O}_K$. This results in a huge explosion of cases when h is nontrivial, as it is often the case that $h_i = h$. For instance, in our Example 1.2, the class number is 33. There are 32 possibilities for $(\mathfrak{a}, S)$ in $\mathcal{Z}$. The 32 possible values for $s = \#S$ are

$$0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 3,\ 3,\ 3,\ 3,\ 3,\ 3,\ 3,\ 3,\ 4,\ 4,$$

where all possible ideals in S have order 33 in $\mathcal{O}_K$. Following the method of Tzanakis and de Weger, we would need to check 2672672 ideals if they are principal, and this approach leads to approximately 80990 equations of the form (15). With our approach, as we need only to deal with 32 ideal equations, we expect to deal with at most 32 equations of the form (15). Indeed, in doing so, we obtain merely 30 equations of the form (15).

5. Lower bounds for linear forms in logarithms

In this section, we state theorems of Matveev [2000] and of Yu [2007] for lower bounds for linear forms in complex and p-adic logarithms. In the next section, we will use these results to obtain bounds for

$b_1, \dots, b_r$. We begin by establishing some notation, as well as some key results which we will need for the lower bound:

- L a number field.
- D the degree $[L : \mathbb{Q}]$.
- M_L the set of all places of L.
- M_L^∞ the subset of infinite places.
- M_L^0 the subset of finite places.
- ν a place of L.
- D_ν the local degree $[L_\nu : \mathbb{Q}_\nu]$.
- $|\cdot|_\nu$ the usual normalized absolute value associated to ν:
  - If ν is infinite and associated to a real or complex embedding σ of L, then $|\alpha|_\nu = |\sigma(\alpha)|$.
  - If ν is finite and above the rational prime p, then $|p|_\nu = p^{-1}$.
- $\|\cdot\|_\nu$ $= |\cdot|_\nu^{D_\nu}$.
- $h(\cdot)$ the absolute logarithmic height, defined in (22).

In the above notation, the product formula may be stated as

$$\prod_{\nu \in M_L} \|\alpha\|_\nu = 1 \tag{19}$$

for all $\alpha \in L^\times$. In particular, if ν is infinite, corresponding to a real or complex embedding σ of L, then

$$\|\alpha\|_\nu = \begin{cases} |\sigma(\alpha)| & \text{if } \sigma \text{ is real,} \\ |\sigma(\alpha)|^2 & \text{if } \sigma \text{ is complex.} \end{cases} \tag{20}$$

If ν is finite, and $\mathfrak{P}$ is the prime ideal corresponding to ν, then for $\alpha \in L^\times$ we have

$$\|\alpha\|_\nu = \mathrm{Norm}(\mathfrak{P})^{-\,\mathrm{ord}_{\mathfrak{P}}(\alpha)}; \tag{21}$$

this easily follows from $D_\nu = e(\mathfrak{P} \mid p) f(\mathfrak{P} \mid p)$, where $e(\mathfrak{P} \mid p)$ and $f(\mathfrak{P} \mid p)$ are respectively the ramification index and the inertial degree of $\mathfrak{P}$.

For $\alpha \in L$, we define the absolute logarithmic height $h(\alpha)$ by

$$h(\alpha) = \frac{1}{[L : \mathbb{Q}]} \sum_{\nu \in M_L} D_\nu \log \max\{1, |\alpha|_\nu\} = \frac{1}{[L : \mathbb{Q}]} \sum_{\nu \in M_L} \log \max\{1, \|\alpha\|_\nu\}. \tag{22}$$

Lemma 5.1. *The absolute logarithmic height of an algebraic number α is independent of the number field L containing α. Moreover, if α and β are Galois conjugates, then $h(\alpha) = h(\beta)$.*

For proofs of the following two lemmata, see [Bugeaud et al. 2008, Lemma 4.1] and [Gallegos-Ruiz 2011, Lemma 3.2].

Lemma 5.2. *For $\alpha_1, \dots, \alpha_n \in L$ we have*

$$h(\alpha_1 \cdots \alpha_n) \le h(\alpha_1) + \cdots + h(\alpha_n), \quad h(\alpha_1 + \cdots + \alpha_n) \le \log n + h(\alpha_1) + \cdots + h(\alpha_n).$$

For any $\alpha \in L^\times$, we have $h(\alpha) = h(\alpha^{-1})$. Moreover, for any place $v \in M_L$,

$$\log \|\alpha\|_v \le [L : \mathbb{Q}] \cdot h(\alpha). \tag{23}$$

Lemma 5.3. *Let L be a number field of degree D. Let $\mathfrak{S}$ be a finite set of finite places of L. Let $\varepsilon \in \mathcal{O}_{\mathfrak{S}}^\times$. Let $\eta \in M_L$ be a place of L chosen so that $\|\varepsilon\|_\eta$ is minimal. Then $\|\varepsilon\|_\eta \le 1$ and*

$$h(\varepsilon) \le \frac{(\#M_L^\infty + \#\mathfrak{S})}{D} \cdot \log(\|\varepsilon^{-1}\|_\eta).$$

5.1. ***Lower bounds for linear forms in $\mathfrak{P}$-adic logarithms.*** Let L be a number field of degree D. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ and let p be the rational prime below $\mathfrak{P}$. Let $v \in M_L^0$ correspond to $\mathfrak{P}$. Let $\alpha_1, \dots, \alpha_n \in L^\times$. Write $e = \exp(1)$.

Let

$$\begin{aligned} h_j &:= \max\left\{h(\alpha_j), \frac{1}{16e^2D^2}\right\}, \quad j = 1, \dots, n; \\ c_1(n, D) &:= (16eD)^{2n+2} \cdot n^{5/2} \cdot \log(2nD) \cdot \log(2D), \\ c_2(n, \mathfrak{P}) &:= e(\mathfrak{P} \mid p)^n \cdot \frac{p^{f(\mathfrak{P} \mid p)}}{f(\mathfrak{P} \mid p) \cdot \log p}, \\ c_3(n, D, \mathfrak{P}, \alpha_1, \dots, \alpha_n) &:= c_1(n, D) \cdot c_2(n, \mathfrak{P}) \cdot h_1 \cdots h_n. \end{aligned} \tag{24}$$

We shall make use of the following theorem of Yu [2007].

Theorem 5.4 (K. Yu). *Let $b_1, \dots, b_n$ be rational integers and let*

$$B = \max\{|b_1|, \dots, |b_n|\},$$

and suppose $B \ge 3$. Let

$$\Lambda = \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1,$$

and suppose $\Lambda \ne 0$. Then

$$\log \|\Lambda^{-1}\|_v < c_3(n, D, \mathfrak{P}, \alpha_1, \dots, \alpha_n) \cdot \log B.$$

Proof. Let

$$c_4(n, D, \mathfrak{P}) := \frac{c_1(n, D) \cdot c_2(n, \mathfrak{P})}{n \cdot f(\mathfrak{P} \mid p) \cdot \log p}.$$

As stated in [Yu 2007, page 190], a consequence of Yu's Main Theorem is

$$\operatorname{ord}_{\mathfrak{P}}(\Lambda) < n \cdot c_4(n, D, \mathfrak{P}) \cdot h_1 \cdots h_n \cdot \log B.$$

By (21) we have

$$\log \|\Lambda^{-1}\|_v = \log(\operatorname{Norm}(\mathfrak{P})) \cdot \operatorname{ord}_{\mathfrak{P}}(\Lambda) = f(\mathfrak{P} \mid p) \cdot \log p \cdot \operatorname{ord}_{\mathfrak{P}}(\Lambda).$$

The theorem follows. □

5.2. ***Lower bounds for linear forms in real or complex logarithms.*** We continue with the above notation. Let

$$h'_j = \sqrt{h(\alpha_j)^2 + \frac{\pi^2}{D^2}}, \quad j = 1, \ldots, n. \tag{25}$$

The following theorem is a version of Matveev's bound [2000] for linear forms in logarithms.

Theorem 5.5 (Matveev). *Let v be an infinite place of L. Suppose $\Lambda \neq 0$. Let*

$$c_5(n, D, \alpha_1, \ldots, \alpha_n) = 6 \cdot 30^{n+4} \cdot (n+1)^{5.5} \cdot D^{n+2} \cdot \log(eD) \cdot h'_1 \cdots h'_n.$$

Then

$$\log \|\Lambda^{-1}\|_v \leq c_5(n, D, \alpha_1, \ldots, \alpha_n) \cdot (\log(en) + \log B).$$

Proof. This in fact follows from a version of Matveev's theorem derived in [Bugeaud et al. 2006]. Let σ be a real or complex embedding of L corresponding to v. Let

$$h''_j = \max\{Dh(\alpha_j), |\log(\sigma(\alpha_j))|, 0.16\},$$

where $\log(\sigma(\alpha_j))$ is the principal determination of the logarithm (i.e., the imaginary part of log lies in $(-\pi, \pi]$). Let

$$c_6(n, D) = 3 \cdot 30^{n+4} \cdot (n+1)^{5.5} \cdot D^2 \cdot \log(eD).$$

Then Theorem 9.4 of [Bugeaud et al. 2006] asserts that

$$\log |\Lambda|_v \geq -c_6(n, D) \cdot h''_1 \cdots h''_n \cdot (\log(en) + \log B).$$

Since $\|\Lambda\| = |\Lambda|^{D_v}$, where D_v is either 1 or 2, we have

$$\log \|\Lambda^{-1}\| \leq 2 \cdot c_6(n, D) \cdot h''_1 \cdots h''_n \cdot (\log(en) + \log B).$$

Thus it is sufficient to show that $h''_j \leq Dh'_j$. However,

$$\log(\sigma(\alpha_j)) = \log|\sigma(\alpha_j)| + i\theta$$

where $-\pi < \theta \leq \pi$. But by (23) and $\|\cdot\|_v = |\cdot|_v^{D_v}$, we have

$$\log|\sigma(\alpha_j)| = \frac{1}{D_v} \log\|\alpha_j\|_v \leq \log\|\alpha_j\|_v \leq D \cdot h(\alpha_j).$$

Thus

$$|\log(\sigma(\alpha_j))| \leq \sqrt{D^2 \cdot h(\alpha_j)^2 + \pi^2} = D \cdot h'_j.$$

It is now clear that $h''_j \leq D \cdot h'_j$. □

6. The S-unit equation

We now return to the task of studying the solutions of (15) satisfying (16), (17). Here, we use the theorems of Matveev and Yu (recalled in the previous section) to establish bounds for $b_1, \ldots, b_r$, following the ideas of [Bugeaud and Győry 1996b; Bugeaud et al. 2008; Gallegos-Ruiz 2011], and taking care to keep our constants completely explicit and as small as possible.

We begin by establishing the following notation:

θ, K	as defined in Section 1.
d	the degree $[K:\mathbb{Q}] \geq 3$.
S	a set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ of prime ideals of K satisfying conditions (a), (b) of Proposition 3.1.
s	the cardinality $\#S$ of the set S.
$\delta_1, \ldots, \delta_r$	a basis for the S-unit group $\mathcal{O}_S^\times$ modulo torsion, also appearing in (15).
τ	a nonzero element of K, appearing in (15).
$X, Y, b_1, \ldots, b_r$	a solution to (15) satisfying (16), (17).
ε	$= \delta_1^{b_1} \cdots \delta_r^{b_r}$. Thus (15) can be rewritten as $a_0 X - \theta Y = \tau \cdot \varepsilon$.
μ	$= \tau \cdot \varepsilon = a_0 X - \theta Y$.
B	$= \max\{\lvert b_1\rvert, \ldots, \lvert b_r\rvert\}$.
$\theta_1, \theta_2, \theta_3$	three conjugates of θ chosen below, with $\theta = \theta_1$.
L	the extension $\mathbb{Q}(\theta_1, \theta_2, \theta_3) \supseteq K$.
D	the degree $[L:\mathbb{Q}]$.
σ_i	the embedding $K \hookrightarrow L$, $\theta \mapsto \theta_i$.
$\mu_i, \varepsilon_i, \tau_i, \delta_{j,i}$	the images of $\mu, \varepsilon, \tau, \delta_j$ under the embedding σ_i.
ξ_1, ξ_2, ξ_3	defined in (26).

We want to write down an S-unit equation starting with (15). For this we will need to work with three conjugates of θ. Let $d = [K:\mathbb{Q}]$, and let $\theta_1, \ldots, \theta_d$ be the conjugates of θ in some splitting field $M \supseteq K$. We shall not need M explicitly, but we assume that we are able to compute the Galois group G of $M/\mathbb{Q}$ as a transitive permutation group on the conjugates θ_i. From this we are able to list all subgroups (up to conjugacy), and for each subgroup determine if it fixes at least three conjugates of θ. Let H be a subgroup of G fixing at least three conjugates of θ with index $[G:H]$ as small as possible. Let $L = M^H$ be the fixed field of H. Then $L = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$ for some three conjugates of θ (after a possible reordering of conjugates) and it has the property that its degree is minimal amongst all extensions generated by three conjugates. Write

$$D := [G:H] = [L:\mathbb{Q}].$$

Again we shall not need the field L explicitly, but only its degree D, which we can deduce from the Galois group. We identify $\theta = \theta_1$, and so can think of $K \subseteq L$.

Write $\mu = a_0 X - \theta Y$. Let $\varepsilon = \delta_1^{b_1} \cdots \delta_r^{b_r}$. Then $\mu = \tau \cdot \varepsilon$. Let $\mu_i, \varepsilon_i, \tau_i, \delta_{j,i}$ be the images of $\mu, \varepsilon, \tau, \delta_j$ under the embeddings $\sigma_i : K \hookrightarrow L$, $\theta \mapsto \theta_i$. We observe the following Siegel identity:

$$(\theta_3 - \theta_2)\mu_1 + (\theta_1 - \theta_3)\mu_2 + (\theta_2 - \theta_1)\mu_3 = 0.$$

Let

$$\xi_1 = (\theta_3 - \theta_2) \cdot \tau_1, \quad \xi_2 = (\theta_1 - \theta_3) \cdot \tau_2, \quad \xi_3 = (\theta_2 - \theta_1) \cdot \tau_3. \tag{26}$$

Then

$$\xi_1\varepsilon_1 + \xi_2\varepsilon_2 + \xi_3\varepsilon_3 = 0. \tag{27}$$

Note that ε_1 is an S-unit in K and ε_2, ε_3 are Galois conjugates of ε. This equation will serve as our S-unit equation. We would like to rewrite (27) in a manner that makes it convenient to apply Theorems 5.4 and 5.5. Observe that (27) can be rewritten as

$$\frac{\xi_3\varepsilon_3}{\xi_1\varepsilon_1} = \left(\frac{-\xi_2}{\xi_1}\right)\left(\frac{\varepsilon_2}{\varepsilon_1}\right) - 1. \tag{28}$$

Let

$$\alpha_j := \frac{\delta_{j,2}}{\delta_{j,1}} \quad (j = 1, \ldots, r), \quad \alpha_{r+1} := \frac{-\xi_2}{\xi_1}, \quad b_{r+1} = 1.$$

Then

$$\frac{\xi_3\varepsilon_3}{\xi_1\varepsilon_1} = \Lambda \tag{29}$$

where Λ is the "linear form"

$$\Lambda := \alpha_1^{b_1} \cdots \alpha_{r+1}^{b_{r+1}} - 1.$$

We assume that we know θ, τ and $\delta_1, \ldots, \delta_r$ explicitly and can therefore compute their absolute logarithmic heights. We will use this to estimate the heights of other algebraic numbers, such as ξ_i, α_j, without computing their minimal polynomials. By Lemmas 5.1 and 5.2,

$$h(\xi_i) \le c_7, \quad c_7 := \log 2 + 2h(\theta) + h(\tau).$$

Lemma 6.1. *Let*

$$c_8 := 2Dc_7.$$

Let v be any place of L. Then

$$\log \|(\varepsilon_3/\varepsilon_1)^{-1}\|_v \le \log \|\Lambda^{-1}\|_v + c_8.$$

Proof. Note that

$$\log \|(\varepsilon_3/\varepsilon_1)^{-1}\|_v = \log \|\Lambda^{-1}\|_v + \log \|\xi_3/\xi_1\|_v.$$

By Lemma 5.2

$$\log \|\xi_3/\xi_1\|_v \le D \cdot h(\xi_3/\xi_1) \le D \cdot (h(\xi_3) + h(\xi_1)).$$ □

By definition $B = \max\{|b_1|, \ldots, |b_r|\}$. However, by (17), and since $b_{r+1} = 1$, we have

$$B = \max\{|b_1|, \ldots, |b_r|, |b_{r+1}|\}.$$

We now apply Matveev's theorem in order to obtain a bound for B.

Lemma 6.2. *Let*

$$h_j^* := \sqrt{4h(\delta_j)^2 + \frac{\pi^2}{D^2}} \quad \textit{for } j = 1, \ldots, r \textit{ and } h_{r+1}^* := \sqrt{4c_7^2 + \frac{\pi^2}{D^2}}.$$

Let

$$c_9 = 6 \cdot 30^{r+5} \cdot (r+2)^{5.5} \cdot D^{r+3} \cdot \log(eD) \cdot h_1^* \cdots h_{r+1}^* \quad \textit{and} \quad c_{10} = c_8 + c_9 \cdot \log(e(r+1)).$$

Let v be an infinite place of L. Then

$$\log \|(\varepsilon_3/\varepsilon_1)^{-1}\|_v \le c_{10} + c_9 \cdot \log B.$$

Proof. We will apply Theorem 5.5 with $n = r+1$. Observe that

$$h(\alpha_j) \le 2h(\delta_j) \quad \text{for } j = 1, \ldots, r \text{ and } h(\alpha_{r+1}) \le 2c_7.$$

Thus $h'_j \le h_j^*$, where h'_j is defined in (25). By Theorem 5.5,

$$\log \|\Lambda^{-1}\|_v \le c_9 \cdot (\log(e(r+1)) + \log B).$$

Lemma 6.1 completes the proof. □

We also apply Yu's theorem.

Lemma 6.3. *Let*

$$h_j^\dagger := \max\left\{2h(\delta_j), \frac{1}{16e^2D^2}\right\} \quad \textit{for } j = 1, \ldots, r,$$

and

$$h_{r+1}^\dagger := \max\left\{2c_7, \frac{1}{16e^2D^2}\right\}.$$

Let T be the set of rational primes p below the primes $\mathfrak{p} \in S$. Let

$$c_{11} := \max_{p \in T} \max\left\{\frac{u^{r+1} \cdot p^v}{v \cdot \log p} : u, v \textit{ are positive integers and } uv \le D/d\right\}$$

and

$$c_{12} := c_1(r+1, D) \cdot c_{11} \cdot h_1^\dagger \cdots h_{r+1}^\dagger.$$

Let v be a finite place of L. Then

$$\log \|(\varepsilon_3/\varepsilon_1)^{-1}\|_v \le c_8 + c_{12} \log B.$$

Proof. Of course we may suppose that $\|(\varepsilon_3/\varepsilon_1)^{-1}\|_v \ne 1$. Let $\mathfrak{P}$ be the prime ideal of $\mathcal{O}_L$ corresponding to v. We will deduce the lemma from Theorem 5.4 combined with Lemma 6.1. For this, it suffices to show that $c_3(r+1, D, \mathfrak{P}, \alpha_1, \ldots, \alpha_{r+1}) \le c_{12}$. Observe that $h_j \le h_j^\dagger$ for $j = 1, \ldots, r+1$. Thus it is enough to show that $c_2(r+1, \mathfrak{P}) \le c_{11}$.

Let $K_i = \mathbb{Q}(\theta_i) \subseteq L$. Recall that ε is an S-unit and that ε_i is the image of ε under the map $\sigma_i : K \to K_i$, $\theta \mapsto \theta_i$. As $\|(\varepsilon_3/\varepsilon_1)^{-1}\|_v \ne 1$, we see that $\mathrm{ord}_{\mathfrak{P}}(\varepsilon_i) \ne 0$ for $i = 1$ or 3. Thus $\mathfrak{P}$ must be a prime above $\mathfrak{p}_i := \sigma_i(\mathfrak{p})$ of $\mathcal{O}_{K_i}$ for some $\mathfrak{p} \in S$, where $i = 1$ or 3. In particular $\mathfrak{P}$ is above some rational prime $p \in T$. However, $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$ for all $\mathfrak{p} \in S$. Thus $e(\mathfrak{P} \mid p) = e(\mathfrak{P} \mid \mathfrak{p}_i)$ and $f(\mathfrak{P} \mid p) = f(\mathfrak{P} \mid \mathfrak{p}_i)$ for $i = 1$ or 3. Let $u = e(\mathfrak{P} \mid p)$ and $v = f(\mathfrak{P} \mid p)$. We see that $uv = e(\mathfrak{P} \mid \mathfrak{p}_i) f(\mathfrak{P} \mid \mathfrak{p}_i) \le [L : K_i] = D/d$. Now $c_2(r+1, \mathfrak{P}) \le c_{11}$ follows from the definitions of c_2 and c_{11}. □

Lemma 6.4. *Let*

$$c_{13} := \frac{\#M_K^\infty + 2 \cdot \#S}{d},$$

and

$$c_{14} := 2h(\tau) + c_{13} \cdot \max(c_8, c_{10}), \quad c_{15} := c_{13} \cdot \max(c_9, c_{12}).$$

Then

$$h(\mu_3/\mu_1) \le c_{14} + c_{15} \cdot \log B.$$

Proof. Let $\mathfrak{S}$ be the prime ideals appearing in the support of $\varepsilon_3/\varepsilon_1$. We will show that $\#\mathfrak{S} \le (2D/d) \cdot \#S$. Indeed, ε_i belongs to $K_i = \mathbb{Q}(\theta_i)$ and its support in K_i is contained in $\sigma_i(S)$. Now a prime belonging to $\sigma_i(S)$ has at most $[L : K_i] = D/d$ primes above it in L. Thus

$$\#\mathfrak{S} \le (D/d) \cdot \#\sigma_1(S) + (D/d) \cdot \#\sigma_3(S) \le (2D/d) \cdot \#S$$

as required. Moreover, since $[L : K] = D/d$, we have $\#M_L^\infty \le (D/d) \cdot \#M_K^\infty$.

Let $\eta \in M_L$ be the place of L such that $\|\varepsilon_3/\varepsilon_1\|_\eta$ is minimal. By Lemma 5.3

$$h(\varepsilon_3/\varepsilon_1) \le \frac{\#M_L^\infty + \#\mathfrak{S}}{D} \cdot \|(\varepsilon_3/\varepsilon_1)^{-1}\|_\eta.$$

From the above inequalities for $\#M_L^\infty$ and $\#\mathfrak{S}$, we deduce that

$$h(\varepsilon_3/\varepsilon_1) \le c_{13} \cdot \|(\varepsilon_3/\varepsilon_1)^{-1}\|_\eta.$$

We now apply Lemmas 6.2 and 6.3 to obtain

$$h(\varepsilon_3/\varepsilon_1) \le c_{13} \cdot (\max(c_8, c_{10}) + \max(c_9, c_{12}) \cdot \log B).$$

Finally, observe that $\mu_3/\mu_1 = (\tau_3/\tau_1) \cdot (\varepsilon_3/\varepsilon_1)$ and thus

$$h(\mu_3/\mu_1) \le 2h(\tau) + h(\varepsilon_3/\varepsilon_1). \qquad \square$$

We shall henceforth suppose $(X, Y) \ne (\pm 1, 0)$. As $\gcd(X, Y) = 1$, this is equivalent to $Y \ne 0$.

Lemma 6.5. *Let v be a place of L. Let*

$$\kappa_v = \begin{cases} 1 & \text{if } v \in M_L^0, \\ \left(\frac{1}{2}\right)^{D_v} & \text{if } v \in M_L^\infty. \end{cases}$$

Then

$$\max\{\|\mu_1\|_v, \|\mu_3\|_v\}^2 \ge \kappa_v^2 \cdot \min\{1, \|\theta_1 - \theta_3\|_v\}^2 \cdot \max\{1, \|\mu_1\|_v\} \cdot \max\{1, \|\mu_3\|_v\}.$$

Proof. There is nothing to prove unless, $\|\mu_i\|_v \le 1$ for both $i = 1, 3$. In this case, it is enough to show that

$$\max\{\|\mu_1\|_v, \|\mu_3\|_v\} \ge \kappa_v \cdot \|\theta_1 - \theta_3\|_v. \tag{30}$$

Suppose first that v is finite and let $\mathfrak{P}$ be the prime ideal of $\mathcal{O}_L$ corresponding to v. Then (30) is equivalent to

$$\min\{\mathrm{ord}_{\mathfrak{P}}(\mu_1), \mathrm{ord}_{\mathfrak{P}}(\mu_3)\} \le \mathrm{ord}_{\mathfrak{P}}(\theta_1 - \theta_3).$$

Let $k = \min\{\mathrm{ord}_{\mathfrak{P}}(\mu_1), \mathrm{ord}_{\mathfrak{P}}(\mu_3)\}$. Then $\mathfrak{P}^k \mid \mu_i$ for $i = 1, 3$. Recall that $\mu_i = a_0 X - \theta_i Y$. Thus $\mathfrak{P}^k$ divides both

$$(\theta_1 - \theta_3) a_0 X = \theta_1 \mu_3 - \theta_3 \mu_1 \quad \text{and} \quad (\theta_1 - \theta_3) Y = \mu_3 - \mu_1.$$

However $\gcd(X, Y) = \gcd(a_0, Y) = 1$, thus $\mathfrak{P}^k \mid (\theta_1 - \theta_3)$ as desired.

Next suppose ν is infinite. As $(\theta_1 - \theta_3)Y = \mu_3 - \mu_1$, and $Y \neq 0$ is a rational integer, we have

$$\|\theta_1 - \theta_3\|_\nu \leq \|\mu_1 - \mu_3\|_\nu = |\mu_1 - \mu_3|_\nu^{D_\nu} \leq 2^{D_\nu} \cdot \max\{|\mu_1|_\nu, |\mu_3|_\nu\}^{D_\nu} \leq 2^{D_\nu} \cdot \max\{\|\mu_1\|_\nu, \|\mu_3\|_\nu\}.$$

This completes the proof. □

Lemma 6.6. *Let*

$$c_{16} := c_{14} + 2\log 2 + 2h(\theta) + h(\tau).$$

Then

$$h(\varepsilon) \leq c_{16} + c_{15} \cdot \log B. \tag{31}$$

Proof. First note that

$$\begin{aligned}
h(\mu_3/\mu_1) &= \frac{1}{D} \sum_{\nu \in M_L} \log \max\{1, \|\mu_3/\mu_1\|_\nu\} \\
&= \frac{1}{D} \sum_{\nu \in M_L} \log \max\{1, \|\mu_3/\mu_1\|_\nu\} + \frac{1}{D} \sum_{\nu \in M_L} \log \|\mu_1\|_\nu \quad \text{(from (19))} \\
&= \frac{1}{D} \sum_{\nu \in M_L} \log \max\{\|\mu_1\|, \|\mu_3\|_\nu\} \\
&\geq \tfrac{1}{2}(h(\mu_1) + h(\mu_3)) + \frac{1}{D} \sum_{\nu \in M_L} (\log \kappa_\nu + \log \min\{1, \|(\theta_1 - \theta_3)\|_\nu\})
\end{aligned}$$

by Lemma 6.5. However μ_1, μ_3 are conjugates of μ, thus $h(\mu_1) = h(\mu_3) = h(\mu)$. Moreover,

$$\frac{1}{D} \sum_{\nu \in M_L} \log \kappa_\nu = -\frac{\log 2}{D} \sum_{\nu \in M_L^\infty} D_\nu = -\log 2.$$

Thus

$$\begin{aligned}
h(\mu) &\leq h(\mu_3/\mu_1) + \log 2 - \frac{1}{D} \sum_{\nu \in M_L} \log \min\{1, \|(\theta_1 - \theta_3)\|_\nu\} \\
&= h(\mu_3/\mu_1) + \log 2 + \frac{1}{D} \sum_{\nu \in M_L} \log \max\{1, \|(\theta_1 - \theta_3)^{-1}\|_\nu\} \\
&= h(\mu_3/\mu_1) + \log 2 + h((\theta_1 - \theta_3)^{-1}) \\
&\leq h(\mu_3/\mu_1) + 2\log 2 + 2h(\theta),
\end{aligned}$$

by Lemmas 5.1 and 5.2. But $\varepsilon = \tau^{-1}\mu$, thus

$$h(\varepsilon) \leq h(\mu_3/\mu_1) + 2\log 2 + 2h(\theta) + h(\tau).$$

Applying Lemma 6.4 completes the proof. □

It is worthwhile to take stock for a moment. The inequality (31) relates the height of $\varepsilon = \delta_1^{b_1} \cdots \delta_r^{b_r}$ to $B = \max\{|b_1|, \ldots, |b_r|\}$. The constants $c_7, \ldots, c_{16}$ are given explicitly in terms of θ, τ, $\delta_1, \ldots, \delta_r$ (all belonging to K), the prime ideals of K belonging to S, the signature of K, and the degree D, which can be deduced from the Galois group of the minimal polynomial of θ. We do not need the field L explicitly.

Lemma 6.7. *Let U be any subset of $S \cup M_K^\infty$ of size r. Let $\mathcal{M}$ be the $r \times r$-matrix*

$$\mathcal{M} = (\log \|\delta_j\|_v)_{v \in U, 1 \le j \le r}.$$

The matrix $\mathcal{M}$ is invertible. Let c_{17} be the largest of the absolute values of the entries of $\mathcal{M}^{-1}$. Then

$$B \le 2d \cdot c_{17} \cdot h(\varepsilon).$$

Proof. The determinant of $\mathcal{M}$ is in fact

$$\pm\left(\prod_{v \in U} D_v\right) \cdot R(\delta_1, \ldots, \delta_r)$$

where $R(\delta_1, \ldots, \delta_r)$ is the regulator of system of S-units $\delta_1, \ldots, \delta_r$, and therefore does not vanish; see [Bugeaud and Győry 1996b, Section 3]. Consider the vectors $\boldsymbol{b} := [b_j]_{j=1,\ldots,r}$ and $\boldsymbol{u} := [\log \|\varepsilon\|_v]_{v \in U}$ in $\mathbb{R}^r$. As $\varepsilon = \delta_1^{b_1} \cdots \delta_r^{b_r}$ we see that $\boldsymbol{u} = \mathcal{M}\boldsymbol{b}$ and so $\boldsymbol{b} = \mathcal{M}^{-1}\boldsymbol{u}$. It follows, for $j = 1, \ldots, r$ that

$$|b_j| \le c_{17} \cdot \sum_{v \in U} |\log \|\varepsilon\|_v| \le c_{17} \cdot \sum_{v \in M_K} \log \max\{1, \|\varepsilon\|_v\} + \log \max\{1, \|\varepsilon^{-1}\|_v\} = 2d \cdot c_{17} \cdot h(\varepsilon)$$

as required. □

Remark. Observe that there are $r + 1$ possibilities for the set U. To compute c_{17} in practice, we iterate across all such sets and select c_{17} as the smallest possible value across each of the associated $r + 1$ matrices $\mathcal{M}$.

Proposition 6.8. *Let*

$$c_{18} := 2d \cdot c_{17} \cdot c_{16}, \quad c_{19} := 2d \cdot c_{17} \cdot c_{15}, \quad c_{20} := 2c_{18} + \max\{2c_{19} \log c_{19}, 4e^2\}.$$

Then

$$B \le c_{20}. \tag{32}$$

Proof. Combining Lemma 6.7 with (31) we have

$$B \le 2d \cdot c_{17} \cdot (c_{16} + c_{15} \cdot \log B) \le c_{18} + c_{19} \log B.$$

The proposition follows from a result of Pethő and de Weger [1998, Lemma B.1 in Appendix B]. □

6.1. ***Example 1.4 continued.*** We give some further details for Example 1.4. Here $a_0 = 5$ and the minimal polynomial for θ is

$$x^{11} + x^{10} + 20x^9 + 25x^8 + 750x^7 + 625x^6 + 18750x^5 + 468750x^3 + 7812500x - 19531250.$$

The field $K = \mathbb{Q}(\theta)$ has degree 11, and signature $(1, 5)$. In this case we have two possibilities for $(\tau, \delta_1, \ldots, \delta_r)$; one has S-unit rank $r = 9$ and the other has S-unit rank $r = 10$. We take a closer look

at one of these two possibilities, with $r = 10$. The set S is composed of the following five primes of ramification degree 1 and inertial degree 1:

$$\mathfrak{p}_1 = \langle 11, 3+\theta\rangle, \quad \mathfrak{p}_2 = \langle 7, 1+\theta\rangle, \quad \mathfrak{p}_3 = \langle 5, \phi\rangle, \quad \mathfrak{p}_4 = \langle 3, 5+\theta\rangle, \quad \mathfrak{p}_5 = \langle 2, 1+\theta\rangle, \tag{33}$$

where

$$\phi = \frac{1}{5^9}(4\theta^{10} + 9\theta^9 + 185\theta^8 + 425\theta^7 + 4625\theta^6 + 13750\theta^5 + 131250\theta^4 + 750000\theta^3 + 3203125\theta^2 + 26953125\theta + 5859375).$$

The bound for B given by Proposition 6.8 is

$$B \le 1.57 \times 10^{222}.$$

7. Controlling the valuations of $a_0X - \theta Y$

In this section and the next, we will suppose that we have a bound

$$B \le \mathcal{B}_\infty \tag{34}$$

and we will explain a method for replacing this bound with what is hopefully a smaller bound. Our subsequent constants will depend on $\mathcal{B}_\infty$. Initially we may take $\mathcal{B}_\infty = c_{20}$ by Proposition 6.8. However, if we succeed in obtaining a smaller bound for B, we may replace $\mathcal{B}_\infty$ by that bound and repeat the process.

We shall replace the reduction step using linear forms in $\mathfrak{p}$-adic logarithms as in the paper of Tzanakis and de Weger [1989]. In particular we will eliminate all computations with completions of extensions of K, as these are extremely tedious and error-prone.

7.1. ***The bounds $\mathcal{B}_\infty$, $\mathcal{B}_1$ and $\mathcal{B}_2$.*** Henceforth $\mathcal{B}_\infty$, $\mathcal{B}_1$ and $\mathcal{B}_2$ will denote the known bounds for the ∞-norm, 1-norm and 2-norm of our exponent vector $\boldsymbol{b} = [b_j]_{j=1,\dots,r}$:

$$B := \|\boldsymbol{b}\|_\infty \le \mathcal{B}_\infty, \quad \|\boldsymbol{b}\|_1 \le \mathcal{B}_1, \quad \|\boldsymbol{b}\|_2 \le \mathcal{B}_2. \tag{35}$$

Initially, thanks to Proposition 6.8, we can make the assignments

$$\mathcal{B}_\infty = c_{20}, \quad \mathcal{B}_2 = \sqrt{r}\cdot\mathcal{B}_\infty, \quad \mathcal{B}_1 = r\cdot\mathcal{B}_\infty \quad \text{(initial values for } \mathcal{B}_\infty, \mathcal{B}_1, \mathcal{B}_2). \tag{36}$$

However, as we progress in our algorithm, we will update the values of $\mathcal{B}_\infty$, $\mathcal{B}_1$, $\mathcal{B}_2$ so that (35) is still satisfied.

Given a lattice $L \subseteq \mathbb{Z}^r$ and a vector $\boldsymbol{w} \in \mathbb{Z}^r$, we denote by $D(L, \boldsymbol{w})$ the shortest length of a vector belonging to the coset $\boldsymbol{w} + L$. This value can be computed using a closest vector algorithm. Indeed, for $\boldsymbol{v} \in \mathbb{Z}^r$, write $\boldsymbol{c}(L, \boldsymbol{v})$ for the closest vector in L to $\boldsymbol{v}$ (if there is more than one at the closest distance, choose any of them).

Lemma 7.1. $D(L, \boldsymbol{w}) = \|\boldsymbol{w} + \boldsymbol{c}(L, -\boldsymbol{w})\|_2$.

Proof. Let $\boldsymbol{l} \in L$ and suppose

$$\|\boldsymbol{w} + \boldsymbol{l}\|_2 < \|\boldsymbol{w} + \boldsymbol{c}(L, -\boldsymbol{w})\|_2.$$

Then

$$\|\boldsymbol{l} - (-\boldsymbol{w})\|_2 < \|\boldsymbol{c}(L, -\boldsymbol{w}) - (-\boldsymbol{w})\|_2.$$

Thus $\boldsymbol{l}$ is a vector belonging to L that is strictly closer to $-\boldsymbol{w}$ than $\boldsymbol{c}(L, -\boldsymbol{w})$ giving a contradiction. □

Our first goal is to use the bounds (35) to deduce bounds on the valuations $\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y)$ for $\mathfrak{p} \in S$.

Proposition 7.2. *Let $\mathfrak{p} \in S$ and let p be the rational prime below $\mathfrak{p}$. Let $k \geq 1$. Then there is some $\theta_0 \in \mathbb{Z}$ such that*

$$\theta \equiv \theta_0 \pmod{\mathfrak{p}^k}.$$

Write

$$\mathfrak{a} := (p\mathcal{O}_K)/\mathfrak{p}, \quad \tau\mathcal{O}_K = \mathcal{T}_1/\mathcal{T}_2, \tag{37}$$

where $\mathcal{T}_1$ and $\mathcal{T}_2$ are coprime ideals. The following hold:

(i) *If* $\gcd(\mathfrak{a}^k, \theta - \theta_0) \neq \gcd(\mathfrak{a}^k, \mathcal{T}_1)$ *then*

$$\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \leq k - 1. \tag{38}$$

Suppose $\gcd(\mathfrak{a}^k, \theta - \theta_0) = \gcd(\mathfrak{a}^k, \mathcal{T}_1)$. *Let*

$$\mathfrak{b} := \mathfrak{a}^k / \gcd(\mathfrak{a}^k, \mathcal{T}_1).$$

Let

$$k' := \max_{\mathfrak{q} \mid \mathfrak{b}} \left\lceil \frac{\mathrm{ord}_{\mathfrak{q}}(\mathfrak{b})}{e(\mathfrak{q} \mid p)} \right\rceil;$$

this satisfies $\mathfrak{b} \cap \mathbb{Z} = p^{k'}\mathbb{Z}$ and therefore $(\mathbb{Z}/p^{k'}\mathbb{Z})^\times$ naturally injects into $(\mathcal{O}_K/\mathfrak{b})^\times$. Given $u \in K^\times$ whose support is coprime with $\mathfrak{b}$, denote its image in $(\mathcal{O}_K/\mathfrak{b})^\times/(\mathbb{Z}/p^{k'}\mathbb{Z})^\times$ by $\bar{u}$. Let

$$\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{b})^\times/(\mathbb{Z}/p^{k'}\mathbb{Z})^\times, \quad (n_1, \ldots, n_r) \mapsto \overline{\delta_1}^{n_1} \cdots \overline{\delta_r}^{n_r}.$$

Write

$$\tau_0 := \frac{(\theta_0 - \theta)}{\tau}.$$

Then the support of τ_0 is coprime with $\mathfrak{b}$:

(ii) *If $\overline{\tau_0}$ does not belong to* Image(ϕ) *then* (38) *holds.*

(iii) *Suppose $\overline{\tau_0} = \phi(\boldsymbol{w})$ for some $\boldsymbol{w} \in \mathbb{Z}^r$. Let $L = \mathrm{Ker}(\phi)$ and suppose $D(L, \boldsymbol{w}) > \mathcal{B}_2$. Then* (38) *holds.*

Proof. Let $\mathfrak{p}$, p, and k be as in the statement of the proposition. We suppose that

$$\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \geq k \tag{39}$$

and show that this leads to a contradiction under the hypotheses of any of (i), (ii), (iii). Recall $k \geq 1$. From the proof of Lemma 2.3, we know $p \nmid Y$.

Since $e(\mathfrak{p} \mid p) = f(\mathfrak{p} \mid p) = 1$, we have $\mathcal{O}_K/\mathfrak{p}^k \cong \mathbb{Z}/p^k$. Thus there is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$. However, $a_0X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$ and so therefore $a_0X - \theta_0 Y \equiv 0 \pmod{\mathfrak{p}^k}$. However

$a_0X - \theta_0 Y \in \mathbb{Z}$. Thus, recalling that $e(\mathfrak{p} \mid p) = 1$, we have $a_0X - \theta_0 Y \equiv 0 \pmod{p^k}$. From (15)

$$Y(\theta_0 - \theta) \equiv \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \pmod{(p\mathcal{O}_K)^k}.$$

Note that the prime $\mathfrak{p}$ belongs to the support of the δ_i. However the other primes $\mathfrak{p}' \mid p$, $\mathfrak{p}' \neq \mathfrak{p}$ do not belong to the support of the δ_i. We now eliminate $\mathfrak{p}$; as in the statement of the proposition we take $\mathfrak{a} := (p\mathcal{O}_K)/\mathfrak{p}$. Then

$$Y(\theta_0 - \theta) \equiv \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \pmod{\mathfrak{a}^k}.$$

Observe that $\mathfrak{a}$ is coprime to the support of the δ_i and Y. Recall $\tau\mathcal{O}_K = \mathcal{T}_1/\mathcal{T}_2$, where $\mathcal{T}_1$, $\mathcal{T}_2$ are coprime integral ideals. By Lemma 4.2, the ideal $\mathcal{T}_2$ is supported on S and therefore coprime to $\mathfrak{a}$. We therefore have a contradiction if $\gcd(\theta_0 - \theta, \mathfrak{a}^k) \neq \gcd(\mathcal{T}_1, \mathfrak{a}^k)$. This proves (i). Suppose $\gcd(\theta_0 - \theta, \mathfrak{a}^k) = \gcd(\mathcal{T}_1, \mathfrak{a}^k)$. Then

$$Y \cdot \tau_0 \equiv \delta_1^{b_1} \cdots \delta_r^{b_r} \pmod{\mathfrak{b}},$$

where Y, τ_0, and δ_i all have support disjoint from $\mathfrak{b}$. As in the proposition, k' is the smallest positive integer such that $\mathfrak{b} \mid p^{k'}$, and thus $(\mathbb{Z}/p^{k'}\mathbb{Z})^\times$ is a subgroup of $(\mathcal{O}_K/\mathfrak{b})^\times$ containing the image of Y. Therefore $\overline{Y} = \bar{1}$ and $\phi(\boldsymbol{b}) = \overline{\tau_0}$. If $\overline{\tau_0} \notin \mathrm{Image}(\phi)$, then we have a contradiction, and so our original assumption (39) is false. This proves (ii).

Suppose now that $\overline{\tau_0} \in \mathrm{Image}(\phi)$ and write $\overline{\tau_0} = \phi(\boldsymbol{w})$ with $\boldsymbol{w} \in \mathbb{Z}^r$. Then $\boldsymbol{b} \in \boldsymbol{w} + L$. Thus $\|\boldsymbol{b}\|_2 \geq D(L, \boldsymbol{w})$. If $D(L, \boldsymbol{w}) > \mathcal{B}_2$ then $\|\boldsymbol{b}\|_2 > \mathcal{B}_2$ and we contradict (35). This proves (iii). □

Remarks. • θ_0 can be easily computed using Hensel's lemma.

• To apply the proposition in practice, it is necessary to compute the abelian group structure of $(\mathcal{O}_K/\mathfrak{b})^\times$ for ideals $\mathfrak{b}$ of very large norm (but supported on the primes above p). For this we may apply the algorithms in [Cohen 2000, Section 4.2].

• $\boldsymbol{c}(-\boldsymbol{w}, L)$ (and therefore $D(\boldsymbol{w}, L)$) can be computed using a closest vector algorithm such as Fincke and Pohst [1985].

• To effectively apply Proposition 7.2 in practice, we need to guess a value of k such that $D(L, \boldsymbol{w}) > \mathcal{B}_2$. We expect $D(L, \boldsymbol{w})$ to be around $I^{1/r}$, where I is the index $[\mathbb{Z}^r : L]$. Let us make two simplifying assumptions: the first is that ϕ is surjective, and the second is that $\gcd(\mathfrak{a}^k, \mathcal{T}_1) = 1$ so that $\mathfrak{b} = \mathfrak{a}^k$ and $k' = k$. Then

$$I = \frac{\#(\mathcal{O}_K/\mathfrak{a}^k)^\times}{\#(\mathbb{Z}/p^k\mathbb{Z})^\times} \approx \frac{\mathrm{Norm}(\mathfrak{a})^k}{p^k} = p^{(d-2)k},$$

where d is the degree of K. Thus we should expect a contradiction if $p^{(d-2)k/r}$ is much bigger than $\mathcal{B}_2$, or equivalently

$$k \gg \frac{r \log \mathcal{B}_2}{(d-2)\log p}.$$

This heuristic gives a good guide for which values of k to try.

7.2. ***Example 1.4 continued.*** We continue giving details for Example 1.4, and in particular for the tuple $(\tau, \delta_1, \ldots, \delta_{10})$ alluded to on page 690. In Section 6 we noted that $B \le 1.57 \times 10^{222}$. Thus we take

$$\mathcal{B}_\infty = 1.57 \times 10^{222}, \quad \mathcal{B}_2 = \sqrt{10} \cdot \mathcal{B}_\infty \approx 4.96 \times 10^{222}. \tag{40}$$

We let $\mathfrak{p} = \mathfrak{p}_1 = \langle 11, 3+\theta \rangle$ which is a prime above 11. The above heuristic suggests that we choose k to be larger than

$$\frac{10 \log \mathcal{B}_2}{(11-2) \cdot \log 11} \approx 237.60.$$

Our program tries $k = 238$. It turns out (in the notation of Proposition 7.2) that $\gcd(\mathfrak{a}^k, \theta - \theta_0) = \gcd(\mathfrak{a}^k, \mathcal{T}_1) = 1$, thus $\mathfrak{b} = \mathfrak{a}^k$, and moreover $k' = k = 238$. The map ϕ is surjective, and thus L does indeed have index

$$I = \frac{\#(\mathcal{O}_K/\mathfrak{a}^k)^\times}{\#(\mathbb{Z}/p^k\mathbb{Z})^\times} = 2^7 \times 3^2 \times 5 \times 11^{2133} \times 61 \times 7321 \approx 5.02 \times 10^{2230}.$$

We do not give L as its basis vectors are naturally huge. However, we find that

$$D(L, \boldsymbol{w}) \approx 1.14 \times 10^{223}.$$

This is much larger than $\mathcal{B}_2$ and we therefore know from Proposition 7.2 that $\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) \le k - 1 = 237$.

It is interesting to note that $I^{1/10} \approx 1.18 \times 10^{223}$ which is rather close to $D(L, \boldsymbol{w})$. If instead we take $k = 237$, we find that $I^{1/10} \approx 1.36 \times 10^{222}$ and $D(L, \boldsymbol{w}) \approx 9.55 \times 10^{221}$ which is somewhat less than $\mathcal{B}_2$. We have generally found the above heuristic to be remarkably accurate in predicting a good choice for k.

Now let $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$ be the primes of S as in (33), where $\mathfrak{p}_1 = \mathfrak{p}$ as above. Proposition 7.2 gives upper bounds 237, 292, 354, 518, 821 for $\mathrm{ord}_{\mathfrak{p}_j}(a_0 X - \theta Y)$ with $j = 1, \ldots, 5$ respectively.

8. Linear forms in real logarithms

In this section, we determine bounds on linear forms in logarithms which we will subsequently use in Section 9 to successively reduce the large upper bound $\mathcal{B}_\infty$ established in Section 6.

We let $s := \#S$ and write

$$S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}.$$

Using Proposition 7.2, we suppose that we have obtained, for $1 \le j \le s$, integers k_j such that

$$\mathrm{ord}_{\mathfrak{p}_j}(a_0 X - \theta Y) \le k_j - 1. \tag{41}$$

Recall that

$$\delta_1^{b_1} \cdots \delta_r^{b_r} = \varepsilon = (a_0 X - \theta Y)/\tau. \tag{42}$$

We write $k_j' := \mathrm{ord}_{\mathfrak{p}_j}(\tau)$, and $k_j'' := k_j - 1 - k_j'$. We obtain

$$-k_j' \le \mathrm{ord}_{\mathfrak{p}_j}(\varepsilon) \le k_j''. \tag{43}$$

8.1. ***Updating $\mathcal{B}_1$ and $\mathcal{B}_2$.*** Recall that $\mathcal{B}_\infty, \mathcal{B}_1, \mathcal{B}_2$ are respectively the known bounds for $\|\boldsymbol{b}\|_\infty$, $\|\boldsymbol{b}\|_1$, $\|\boldsymbol{b}\|_2$ as in (35). Initially we take these as in (36). In practice, we are often able to update $\mathcal{B}_1$ and $\mathcal{B}_2$ with

a smaller bound after each iteration of Proposition 7.2. Let (u, v) be the signature of K. Since r is the rank of the S-unit group $\mathcal{O}_S^\times$, we have

$$r = u + v - 1 + s.$$

Recall our convention (page 681) on the choice of S-unit basis $\delta_1, \ldots, \delta_r$: we suppose that the basis is chosen so that $\delta_1, \ldots, \delta_{u+v-1}$ is in fact a basis for the unit group modulo torsion. Thus $\log\|\delta_i\|_v = 0$ for all $v \in M_K^0$ and $1 \le i \le u + v - 1$. Let $\mathcal{M}_0$ denote the $s \times s$ matrix

$$\mathcal{M}_0 = (\log \|\delta_j\|_v)_{v\in S, u+v\le j\le r}.$$

In Lemma 6.7 let $U = \{v_1, \ldots, v_r\}$ where $v_1, \ldots, v_{u+v-1}$ are any $u + v - 1$ elements of M_K^∞ and the remainder are the elements of S. Then, in the notation of Lemma 6.7,

$$\mathcal{M} = \left(\begin{array}{c|c} * & * \\ \hline 0 & \mathcal{M}_0 \end{array}\right).$$

Since $\mathcal{M}$ is invertible by Lemma 6.7, it follows that $\mathcal{M}_0$ is invertible. We partition our exponent vector $\boldsymbol{b}$ as

$$\boldsymbol{b} = [\boldsymbol{b}' \mid \boldsymbol{b}''], \quad \boldsymbol{b}' = [b_i]_{i=1,\ldots,u+v-1}, \quad \boldsymbol{b}'' = [b_i]_{i=u+v,\ldots,r}.$$

Write $\boldsymbol{u}'' := [\log \|\varepsilon\|_v]_{v\in S}$ in $\mathbb{R}^s$. By the above, we have $\boldsymbol{u}'' = \mathcal{M}_0\boldsymbol{b}''$ and thus $\boldsymbol{b}'' = \mathcal{M}_0^{-1}\boldsymbol{u}''$. That is, for $1 \le i \le s$,

$$b_{u+v-1+i} = m_{i1}\log\|\varepsilon\|_{\mathfrak{p}_1} + \cdots + m_{is}\log\|\varepsilon\|_{\mathfrak{p}_s},$$

where $\mathcal{M}_0^{-1} = [m_{ij}]$. It follows that

$$|b_{u+v-1+i}| \le |m_{i1}| \cdot |\log\|\varepsilon\|_{\mathfrak{p}_1}| + \cdots + |m_{is}| \cdot |\log\|\varepsilon\|_{\mathfrak{p}_s}|. \tag{44}$$

Applying Proposition 7.2 to any $\mathfrak{p}_j$ for $1 \le j \le s$ and using (43) and (21), we obtain

$$|\log\|\varepsilon\|_{\mathfrak{p}_j}| \le \log(\mathrm{Norm}(\mathfrak{p}_j)) \cdot \max\{|k_j'|, |k_j''|\}.$$

Write

$$\rho_i' := \sum_{j=1}^{s} |m_{i,j}| \cdot \log(\mathrm{Norm}(\mathfrak{p}_j)) \cdot \max\{|k_j'|, |k_j''|\}, \quad \rho_i = \min\{\mathcal{B}_\infty, \rho_i'\}. \tag{45}$$

From equation (44) it follows that $|b_{u+v-1+i}| \le \rho_i'$ for $1 \le i \le s$. However, $\max\{|b_i|\}_{i=1}^r = \|\boldsymbol{b}\|_\infty \le \mathcal{B}_\infty$, so we know that $|b_{u+v-1+i}| \le \mathcal{B}_\infty$. We deduce that

$$|b_{u+v-1+i}| \le \rho_i, \quad 1 \le i \le s. \tag{46}$$

Hence

$$\|\boldsymbol{b}\|_1 = \|\boldsymbol{b}'\|_1 + \|\boldsymbol{b}''\|_1 \le (u + v - 1)\mathcal{B}_\infty + \rho_1 + \cdots + \rho_s$$

and

$$\|\boldsymbol{b}\|_2 = \sqrt{\|\boldsymbol{b}'\|_2^2 + \|\boldsymbol{b}''\|_2^2} \le \sqrt{(u + v - 1)\mathcal{B}_\infty^2 + \rho_1^2 + \cdots + \rho_s^2}.$$

We now update our values for $\mathcal{B}_1$ and $\mathcal{B}_2$:

$$\mathcal{B}_1 = (u+v-1)\mathcal{B}_\infty + \rho_1 + \cdots + \rho_s, \tag{47}$$

$$\mathcal{B}_2 = \sqrt{(u+v-1)\mathcal{B}_\infty^2 + \rho_1^2 + \cdots + \rho_s^2}. \tag{48}$$

Note, since by (45) we have $\rho_i \le \mathcal{B}_\infty$, these new values for $\mathcal{B}_1$ and $\mathcal{B}_2$ are bounded above by the old values given in (36). In practice we usually find that these give significantly better bounds for $\|\boldsymbol{b}\|_1$, $\|\boldsymbol{b}\|_2$.

8.2. ***Embeddings and improving the initial bound* (34).** To improve our initial bound (34), we rely on the inequality $B \le 2c_{17} \cdot d \cdot h(\varepsilon)$ furnished by Lemma 6.7. However $h(\varepsilon) = h(\varepsilon^{-1})$ and so

$$B \le 2c_{17} \sum_{v \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_v\}.$$

Since ε is an S-unit, for $v \notin M_K^\infty \cup S$, we have $\|\varepsilon\|_v = 1$. Thus

$$B \le 2c_{17} \sum_{v \in M_K^\infty \cup S} \log \max\{1, \|\varepsilon^{-1}\|_v\}. \tag{49}$$

Therefore, to obtain a better bound for B, it is enough to gain good control on the contributions to the sum on the right-hand side of (49).

Lemma 8.1. *Let*

$$c_{21} = \sum_{i=1}^{s} \max\{0, k_i''\} \cdot \log(\mathrm{Norm}(\mathfrak{p}_i)).$$

Then

$$B \le 2c_{17}\left(c_{21} + \sum_{v \in M_K^\infty} \log \max\{1, \|\varepsilon^{-1}\|_v\}\right). \tag{50}$$

Proof. From (43) and (21) we have

$$\sum_{v \in S} \log \max\{1, \|\varepsilon^{-1}\|_v\} \le c_{21}.$$

The lemma now follows from (49). □

We shall write

$$M_K^\infty = M_K^{\mathbb{R}} \cup M_K^{\mathbb{C}},$$

where $M_K^{\mathbb{R}}$ and $M_K^{\mathbb{C}}$ are respectively the sets of real and complex places. Recall that (u, v) denotes the signature of K. Thus we have embeddings

$$\sigma_1, \ldots, \sigma_u, \quad \sigma_{u+1}, \ldots, \sigma_{u+v}, \overline{\sigma_{u+1}}, \ldots, \overline{\sigma_{u+v}}$$

of K, where σ_i are real embeddings for $1 \le i \le u$, and σ_{u+i}, $\overline{\sigma_{u+i}}$ are pairs of complex conjugate embeddings. Let

$$\mathcal{E}_K^{\mathbb{R}} := \{\sigma_1, \ldots, \sigma_u\}, \quad \mathcal{E}_K^{\mathbb{C}} := \{\sigma_{u+1}, \ldots, \sigma_{u+v}\}. \tag{51}$$

For the membership of $\mathcal{E}_K^{\mathbb{C}}$, we are making an arbitrary choice of a member from each pair of conjugate complex embeddings, but that is unimportant. Note that $M_K^{\mathbb{R}}$ is in one-to-one correspondence with $\mathcal{E}_K^{\mathbb{R}}$ and $M_K^{\mathbb{C}}$ is in one-to-one correspondence with $\mathcal{E}_K^{\mathbb{C}}$. We consider the contribution to the sum (50) coming from $\nu \in M_K^{\mathbb{C}}$, or equivalently from $\sigma \in \mathcal{E}_K^{\mathbb{C}}$.

Let $\Im(z)$ denote the imaginary part of a complex number z.

Lemma 8.2. *Let*

$$c_{22} = 2 \sum_{\sigma \in \mathcal{E}_K^{\mathbb{C}}} \log \max\left\{1, \frac{|\sigma(\tau)|}{|\Im(\sigma(\theta))|}\right\}.$$

Then

$$B \le 2c_{17}\left(c_{21} + c_{22} + \sum_{\sigma \in \mathcal{E}_K^{\mathbb{R}}} \log \max\{1, |\sigma(\varepsilon)|^{-1}\}\right). \tag{52}$$

Proof. Note that (50) can be rewritten as

$$B \le 2c_{17}\left(c_{21} + 2\sum_{\sigma \in \mathcal{E}_K^{\mathbb{C}}} \log \max\{1, |\sigma(\varepsilon)|^{-1}\} + \sum_{\sigma \in \mathcal{E}_K^{\mathbb{R}}} \log \max\{1, |\sigma(\varepsilon)|^{-1}\}\right).$$

Let $\sigma \in \mathcal{E}_K^{\mathbb{C}}$. Then as $a_0X - \theta Y = \tau \cdot \varepsilon$, we have

$$|\sigma(\varepsilon)| = \frac{1}{|\sigma(\tau)|} \cdot |\sigma(a_0X - \theta Y)| \ge \frac{1}{|\sigma(\tau)|} \cdot |Y| \cdot |\Im(\sigma(\theta))| \ge \frac{|\Im(\sigma(\theta))|}{|\sigma(\tau)|},$$

because of our assumption $|Y| \ne 0$. The lemma follows. □

The following is immediate.

Proposition 8.3. *If K is totally imaginary then*

$$B \le 2c_{17}(c_{21} + c_{22}).$$

8.3. ***The nontotally complex case.*** Suppose now that K has one or more real embeddings. Recall that the signature of K is (u, v). Thus $u \ge 1$.

Lemma 8.4. *If $u = 1$ we let $c_{23} := 1$. If $u \ge 2$ we let*

$$c_{23} := \min\left\{\frac{|\sigma(\theta) - \sigma'(\theta)|}{|\sigma(\tau)| + |\sigma'(\tau)|} : \sigma, \sigma' \in \mathcal{E}_K^{\mathbb{R}}, \sigma \ne \sigma'\right\}.$$

Then there is at most one $\sigma \in \mathcal{E}_K^{\mathbb{R}}$ such that $|\sigma(\varepsilon)| < c_{23}$.

Proof. Suppose otherwise. Then there are $\sigma, \sigma' \in \mathcal{E}_K^{\mathbb{R}}$ with $\sigma \ne \sigma'$ such that $|\sigma(\varepsilon)| < c_{23}$ and $|\sigma'(\varepsilon)| < c_{23}$. As $a_0X - \theta Y = \tau \cdot \varepsilon$ we find that

$$|a_0X - \sigma(\theta)Y| < c_{23} \cdot |\sigma(\tau)|, \quad |a_0X - \sigma'(\theta)Y| < c_{23} \cdot |\sigma'(\tau)|.$$

Thus

$$|\sigma(\theta) - \sigma'(\theta)| \cdot |Y| < c_{23} \cdot (|\sigma(\tau)| + |\sigma'(\tau)|).$$

Recall our assumption that $Y \ne 0$. This inequality now contradicts our definition of c_{23}. □

Lemma 8.5. *Let*

$$c_{24} := c_{21} + c_{22} + (u-1)\log\max\{1, c_{23}^{-1}\}, \quad c_{25} := \exp(c_{24}) \quad \textit{and} \quad c_{26} := \frac{1}{2c_{17}}.$$

Suppose $B > 2c_{17} \cdot c_{24}$. *Let* $\sigma \in \mathcal{E}_K^{\mathbb{R}}$ *be chosen so that* $|\sigma(\varepsilon)|$ *is minimal. Then*

$$|\sigma(\varepsilon)| \le c_{25} \cdot \exp(-c_{26} \cdot B). \tag{53}$$

Proof. From Lemma 8.4, we have

$$|\sigma'(\varepsilon)| \ge c_{23}$$

for all $\sigma' \in \mathcal{E}_K^{\mathbb{R}}$ with $\sigma' \ne \sigma$. From (52) we deduce that

$$B \le 2c_{17}(c_{21}+c_{22}+(u-1)\log\max\{1, c_{23}^{-1}\}+\log\max\{1, |\sigma(\varepsilon)|^{-1}\}) = 2c_{17}(c_{24}+\log\max\{1, |\sigma(\varepsilon)|^{-1}\}).$$

It follows that

$$\log\max\{1, |\sigma(\varepsilon)|^{-1}\} \ge \frac{1}{2c_{17}}B - c_{24} = c_{26} \cdot B - c_{24}.$$

The hypothesis $B > 2c_{17} \cdot c_{24}$ forces the right-hand side to be positive, and so the left-hand side must simply be $\log|\sigma(\varepsilon)^{-1}|$. After exponentiating and rearranging, we obtain (53). □

8.4. ***Approximate relations.*** As in Lemma 8.5 we shall let $\sigma \in \mathcal{E}_K^{\mathbb{R}}$ be the real embedding that makes $|\sigma(\varepsilon)|$ minimal. Recall that the signature of K is (u, v); we keep the assumption that $u \ge 1$. Let

$$n := r + v. \tag{54}$$

In this section we introduce additional unknown integers $b_{r+1}, \dots, b_n$, closely related to the exponents $b_1, \dots, b_r$ found in (15). We shall use Lemma 8.5 to write down $d-2$ linear forms in $b_1, \dots, b_n$ with real coefficients, whose values are very small. We shall later give a method, based on standard ideas originally due to de Weger, that uses these "approximate relations" to reduce our bound for $B = \max(|b_1|, \dots, |b_r|, 1)$.

We label the elements of $\mathcal{E}_K^{\mathbb{R}}$ and $\mathcal{E}_K^{\mathbb{C}}$ as in (51), where $\sigma_1 = \sigma$. Write

$$\theta_j = \sigma_j(\theta), \quad \tau_j = \sigma_j(\tau), \quad \varepsilon_j = \sigma_j(\varepsilon), \quad \delta_{i,j} = \sigma_j(\delta_i), \quad 1 \le j \le u+v, 1 \le i \le r.$$

Let $2 \le j \le u+v$ and write

$$z_j := \frac{a_0X - \theta_1 Y}{a_0X - \theta_j Y}.$$

Observe that

$$\begin{aligned} Y(\theta_1 - \theta_j) &= (a_0X - \theta_j Y) - (a_0X - \theta_1 Y) \\ &= (a_0X - \theta_j Y) \cdot (1 - z_j) \\ &= \tau_j \cdot \delta_{1,j}^{b_1} \cdots \delta_{r,j}^{b_r} \cdot (1 - z_j). \end{aligned} \tag{55}$$

In the following lemma, as always, log denotes the principal determination of the logarithm (i.e., the imaginary part of log lies in $(-\pi, \pi]$).

Lemma 8.6. *Let*

$$c_{27} := \frac{|\tau_1| \cdot c_{25}}{\min\{|\tau_i| : \sigma_i \in \mathcal{E}_K^{\mathbb{R}}, \sigma_i \neq \sigma\} \cdot c_{23}}, \quad c_{28} := \frac{|\tau_1| \cdot c_{25}}{\min\{|\Im(\theta_i)| : \sigma_i \in \mathcal{E}_K^{\mathbb{C}}\}},$$

and

$$c_{29}(j) := \begin{cases} |\tau_1| \cdot c_{25}/(|\tau_j| \cdot c_{23}) & \text{for } 2 \leq j \leq u, \\ |\tau_1| \cdot c_{25}/|\Im(\theta_j)| & \text{for } u+1 \leq j \leq u+v. \end{cases}$$

Define

$$c_{30} := \max\{2c_{17} \cdot c_{24}, \log(2c_{27})/c_{26}, \log(2c_{28})/c_{26}\}$$

and suppose $B > c_{30}$. *Then*

$$|\log(1 - z_j)| \leq 2c_{29}(j) \cdot \exp(-c_{26} \cdot B) \quad \text{for } 2 \leq j \leq u+v.$$

Proof. Let $2 \leq j \leq u+v$. If $\sigma_j \in \mathcal{E}_K^{\mathbb{R}}$, Lemma 8.4 yields

$$|a_0 X - \theta_j Y| = |\tau_j| \cdot |\varepsilon_j| \geq |\tau_j| \cdot c_{23}.$$

Conversely, if $\sigma_j \in \mathcal{E}_K^{\mathbb{C}}$, following the proof of Lemma 8.2, we have

$$|a_0 X - \theta_j Y| = |\tau_j| \cdot |\varepsilon_j| \geq |\Im(\theta_j)|.$$

Now, by Lemma 8.5 we have

$$|a_0 X - \theta_1 Y| = |\tau_1| \cdot |\varepsilon_1| \leq |\tau_1| \cdot c_{25} \cdot \exp(-c_{26} \cdot B);$$

it is in invoking this lemma that we have made use of the assumption $B > 2c_{17} \cdot c_{24}$. Thus

$$|z_j| \leq c_{29}(j) \cdot \exp(-c_{26} \cdot B).$$

Our assumption $B > c_{30} \geq \log(2c_{29}(j))/c_{26}$ gives $|z_j| < \frac{1}{2}$. From the standard Maclaurin expansion for $\log(1-x)$ we conclude that $|\log(1 - z_j)| \leq 2 \cdot |z_j|$, completing the proof. □

To ease notation, let

$$w := u + v - 2. \tag{56}$$

We now give our first set of w approximate relations. These only involve our original unknown exponents $b_1, \ldots, b_r$ found in (15).

Lemma 8.7. *Suppose* $B > c_{30}$ *holds. Let* $1 \leq j \leq w$. *Let*

$$\beta_j := \log\left|\frac{(\theta_1 - \theta_2) \cdot \tau_{j+2}}{(\theta_1 - \theta_{j+2}) \cdot \tau_2}\right|, \quad \alpha_{1,j} := \log\left|\frac{\delta_{1,j+2}}{\delta_{1,2}}\right|, \ldots, \alpha_{r,j} := \log\left|\frac{\delta_{r,j+2}}{\delta_{r,2}}\right|.$$

Then

$$|\beta_j + b_1\alpha_{1,j} + \cdots + b_r\alpha_{r,j}| \leq 2(c_{29}(2) + c_{29}(j+2)) \cdot \exp(-c_{26} \cdot B). \tag{57}$$

Proof. From (55),

$$\frac{(\theta_1-\theta_2)\cdot\tau_{j+2}}{(\theta_1-\theta_{j+2})\cdot\tau_2}\cdot\left(\frac{\delta_{1,j+2}}{\delta_{1,2}}\right)^{b_1}\cdots\left(\frac{\delta_{r,j+2}}{\delta_{r,2}}\right)^{b_r}=\frac{1-z_2}{1-z_{j+2}}.$$

Taking absolute values and then logs gives

$$|\beta_j+b_1\alpha_{1,j}+\cdots+b_r\alpha_{r,j}|\le|\log|1-z_2||+|\log|1-z_{j+2}||.$$

For a complex number z, we have

$$|\log|z||\le|\log z|$$

since $\log|z|$ is the real part of $\log z$. The lemma now follows from Lemma 8.6. □

In essence, in the above lemma, we have made use of the fact that

$$K^\times\to\mathbb{R},\quad \phi\mapsto\log|\sigma(\phi)| \tag{58}$$

is a homomorphism for each embedding σ of K, and applied this to the approximate multiplicative relation (55) to obtain an approximate (additive) relation (57). If σ is complex, then σ and its conjugate $\bar\sigma$ induce the same homomorphism (58), and thus we need only consider the embeddings $\sigma_1,\dots,\sigma_{u+v}$. Note that although these are $u+v$ embeddings, we have obtained only $u+v-2$ approximate relations so far. That is, we have had to sacrifice embeddings because we wanted to eliminate the two unknowns, X and Y. For σ real, $\log|\sigma(\phi)|$ determines $\sigma(\phi)$ up to signs. However, if σ is complex, then (58) loses the argument of $\sigma(\phi)$. Thus we should consider another homomorphism

$$K^\times\to\mathbb{R}/\mathbb{Z}\pi,\quad \phi\mapsto\Im(\log\sigma(\phi)) \tag{59}$$

where $\Im(z)$ denotes the imaginary part of a complex number z. Observe that $\Im(\log\sigma(\phi))$ denotes the argument of $\sigma(\phi)$ which naturally lives in $\mathbb{R}/\mathbb{Z}2\pi$, whilst here we use $\mathbb{R}/\mathbb{Z}\pi$ as the codomain. In practice, we have found that using $\mathbb{R}/\mathbb{Z}2\pi$ introduces extra factors but only results in negligible improvements to the bounds. Applying these homomorphisms to (55) allows us to obtain additional approximate relations. Since there are v complex embeddings, we obtain an additional v approximate relations. However since these homomorphism are into $\mathbb{R}/\mathbb{Z}\pi$, the approximate relations are only valid after shifting by an appropriate multiple of π; thus for each complex embedding σ_{u+j}, we will need an additional parameter b_{r+j}.

Recall that $w=u+v-2$.

Lemma 8.8. *Let* $1\le j\le v$. *Let*

$$\beta_{w+j}:=\Im\left(\log\left(\frac{\theta_1-\theta_{u+j}}{\tau_{u+j}}\right)\right),$$

$$\alpha_{1,w+j}:=-\Im(\log\delta_{1,u+j}),\dots,\alpha_{r,w+j}:=-\Im(\log\delta_{r,u+j}),\quad \alpha_{r+j,w+j}:=\pi.$$

Suppose $B>c_{30}$ *holds. Then there is some* $b_{r+j}\in\mathbb{Z}$ *such that*

$$|\beta_{w+j}+b_1\alpha_{1,w+j}+\cdots+b_r\alpha_{r,w+j}+b_{r+j}\alpha_{r+j,w+j}|\le 2c_{29}(u+j)\cdot\exp(-c_{26}\cdot B). \tag{60}$$

Moreover,

$$|b_{r+j}|\le|b_1|+\cdots+|b_r|+\frac{\pi+1}{\pi}. \tag{61}$$

Proof. From (55), and Lemma 8.6,

$$|\log(Y) + \log((\theta_1 - \theta_{u+j})/\tau_{u+j}) - b_1 \log \delta_{1,u+j} - \cdots - b_r \log \delta_{r,u+j} + b' \cdot \pi i| \leq 2c_{29}(u+j) \cdot \exp(-c_{26} \cdot B),$$

for some $b' \in \mathbb{Z}$. Thus

$$|\Im(\log(Y)) + \beta_{w+j} + b_1\alpha_{1,w+j} + \cdots + b_r\alpha_{r,w+j} + b'\pi| \leq 2c_{29}(u+j) \cdot \exp(-c_{26} \cdot B).$$

Recall that $Y \in \mathbb{Z} \setminus \{0\}$, so $\Im(\log(Y))$ is either 0 or π depending on whether Y is positive or negative. We take $b_{r+j} = b'$ in the former case and $b_{r+j} = b' + 1$ in the latter case. This gives (60).

It remains to prove (61). Our assumption $B > c_{30}$ gives

$$2c_{29}(u+j) \cdot \exp(-c_{26} \cdot B) < 1.$$

Moreover, $|\beta_{w+j}| \leq \pi$ and $|\alpha_{i,w+j}| \leq \pi$ for $0 \leq i \leq r$. From (60),

$$\begin{aligned} \pi \cdot |b_{r+j}| &= |\alpha_{r+j,w+j}| \cdot |b_{r+j}| \\ &\leq |\beta_{w+j}| + |\alpha_{1,w+j}| \cdot |b_1| + \cdots + |\alpha_{r,w+j}| \cdot |b_r| + 1 \\ &\leq \pi(1 + |b_1| + \cdots + |b_r|) + 1. \end{aligned}$$

The lemma follows. □

Summing up, Lemmas 8.7 and 8.8 give us $(u+v-2)+v = d-2$ approximate relations (57), (60) in integer unknowns $b_1, \ldots, b_{r+v}$.

9. Reduction of bounds

We do not know which real embedding $\sigma \in \mathcal{E}_K^{\mathbb{R}}$ makes $|\sigma(\varepsilon)|$ minimal. So the procedure described below for reducing the bound (34) needs to be repeated for each possible choice of embedding σ in $\mathcal{E}_K^{\mathbb{R}}$. Thus, for every possible choice of $\sigma \in \mathcal{E}_K^{\mathbb{R}}$, we let $\sigma_1 = \sigma$ and we choose an ordering of the other embeddings as in (51). Given a real number γ, we denote by $[\gamma]$ the nearest integer to γ, with the convention that $[k + 1/2] = k + 1$ for $k \in \mathbb{Z}$. Let n be as in (54) and observe that

$$n = (s+1) + d - 2,$$

where we recall that $s = \#S$. Let C be a positive integer to be chosen later. Let $\boldsymbol{I}_m$ and $\mathbf{0}_{i,j}$ be the $m \times m$ identity matrix and $i \times j$ zero matrix, respectively. Let M be the $n \times n$ matrix

$$M := \left[\begin{array}{c|ccc|ccc} & [C\alpha_{1,1}] & \cdots & [C\alpha_{1,w}] & [C\alpha_{1,w+1}] & \cdots & [C\alpha_{1,d-2}] \\ \mathbf{0}_{w,s+1} & \vdots & & \vdots & \vdots & & \vdots \\ & [C\alpha_{w,1}] & \cdots & [C\alpha_{w,w}] & [C\alpha_{w,w+1}] & \cdots & [C\alpha_{w,d-2}] \\ \hline & [C\alpha_{w+1,1}] & \cdots & [C\alpha_{w+1,w}] & [C\alpha_{w+1,w+1}] & \cdots & [C\alpha_{w+1,d-2}] \\ \boldsymbol{I}_{s+1} & \vdots & & \vdots & \vdots & & \vdots \\ & [C\alpha_{r,1}] & \cdots & [C\alpha_{r,w}] & [C\alpha_{r,w+1}] & \cdots & [C\alpha_{r,d-2}] \\ \hline \mathbf{0}_{v,s+1} & \multicolumn{3}{c|}{\mathbf{0}_{v,w}} & \multicolumn{3}{c}{[C\pi] \cdot \boldsymbol{I}_v} \end{array}\right]$$

and let L be the sublattice of $\mathbb{Z}^n$ spanned by the rows of M. Recall that $\mathcal{B}_\infty$, $\mathcal{B}_1$, $\mathcal{B}_2$ are respectively the known bounds for $\|\boldsymbol{b}\|_\infty$, $\|\boldsymbol{b}\|_1$, $\|\boldsymbol{b}\|_2$. Let

$$\begin{aligned}
\boldsymbol{w} &:= (\underbrace{0, 0, \ldots, 0}_{s+1}, [C\beta_1], \ldots, [C\beta_{d-2}]) \in \mathbb{Z}^n,\\
\mathcal{A}_1 &:= \frac{1+\mathcal{B}_1}{2}, \quad \mathcal{A}_2 := \frac{2\pi(1+\mathcal{B}_1)+1}{2\pi},\\
\mathcal{B}_3 &:= \sum_{j=1}^{w} (c_{29}(2) + c_{29}(j+2))^2 + \sum_{j=1}^{v} c_{29}(u+j)^2,\\
\mathcal{B}_4 &:= \mathcal{A}_1 \sum_{j=1}^{w} (c_{29}(2) + c_{29}(j+2)) + \mathcal{A}_2 \sum_{j=1}^{v} c_{29}(u+j), \text{ and}\\
\mathcal{B}_5 &:= \sqrt{\mathcal{B}_2^2 - w\mathcal{B}_\infty^2 + w\mathcal{A}_1^2 + v\mathcal{A}_2^2}.
\end{aligned}$$

By (48), we observe that

$$\mathcal{B}_2^2 = (w+1)\mathcal{B}_\infty^2 + \rho_1^2 + \cdots + \rho_s^2$$

so that $\mathcal{B}_2^2 - w\mathcal{B}_\infty^2 \geq 0$ and thus the argument of the square root in the above definition of $\mathcal{B}_5$ is positive.

Write

$$\boldsymbol{b}_e := (b_1, b_2, \ldots, b_r, b_{r+1}, \ldots, b_{r+v}),$$

where $b_{r+1}, \ldots, b_{r+v}$ are as in Lemma 8.8. We think of this as the "extended exponent vector". Note that the number of entries in $\boldsymbol{b}_e$ is

$$r + v = u + v + s - 1 + v = d + s - 1 = n. \tag{62}$$

If $\boldsymbol{b}_e$ is known, then the solution is known.

Lemma 9.1. $$\|\boldsymbol{b}_e\|_2 \leq \sqrt{\mathcal{B}_2^2 + v\left(\mathcal{B}_1 + \frac{\pi+1}{\pi}\right)^2}.$$

Proof. This follows immediately from (61) and the definitions of $\mathcal{B}_1, \mathcal{B}_2$. □

Proposition 9.2. *Suppose $\boldsymbol{b}_e \cdot M \neq -\boldsymbol{w}$. Let*

$$\mathcal{D} := \begin{cases} D(L, \boldsymbol{w}) & \text{if } \boldsymbol{w} \notin L, \\ \min_{\substack{\boldsymbol{x} \in L \\ \boldsymbol{x} \neq \boldsymbol{0}}} \|\boldsymbol{x}\|_2 & \text{if } \boldsymbol{w} \in L. \end{cases} \tag{63}$$

Suppose $\mathcal{D} > \mathcal{B}_5$. Then

$$B \leq \max\left(c_{30}, \frac{1}{c_{26}} \cdot \log\left(\frac{2C \cdot \mathcal{B}_3}{\sqrt{\mathcal{B}_3(\mathcal{D}^2 - \mathcal{B}_5^2) + \mathcal{B}_4^2} - \mathcal{B}_4}\right)\right). \tag{64}$$

Proof. If $B \leq c_{30}$ then (64) holds. We will therefore suppose that $B > c_{30}$. Thus, inequalities (57) and (60) hold. Write

$$\boldsymbol{w} + \boldsymbol{b}_e \cdot M = (b_{u+v-1}, b_{u+v}, \ldots, b_r, \Theta_1, \Theta_2, \ldots, \Theta_{d-2}),$$

where we take this equality as the definition of $\Theta_1, \dots, \Theta_{d-2}$. That is, for $1 \le j \le w$,

$$\Theta_j = [C\beta_j] + b_1[C\alpha_{1,j}] + \cdots + b_r[C\alpha_{r,j}].$$

Hence, again for $1 \le j \le w$,

$$\begin{aligned}|\Theta_j| &\le \tfrac{1}{2} + \tfrac{1}{2}|b_1| + \cdots + \tfrac{1}{2}|b_r| + C \cdot |\beta_j + b_1\alpha_{1,j} + \cdots + b_r\alpha_{r,j}| \\ &\le \tfrac{1}{2}(1 + \mathcal{B}_1) + 2C \cdot (c_{29}(2) + c_{29}(j+2)) \cdot \exp(-c_{26} \cdot B) \\ &\le \mathcal{A}_1 + (c_{29}(2) + c_{29}(j+2)) \cdot \eta,\end{aligned}$$

where the second inequality follows by (34) and (57), and

$$\eta := 2C \cdot \exp(-c_{26} \cdot B).$$

Recall that $w = u + v - 2$. For $1 \le j \le v$,

$$\Theta_{w+j} = [C\beta_{w+j}] + b_1[C\alpha_{1,w+j}] + \cdots + b_r[C\alpha_{r,w+j}] + b_{r+j}[C\pi].$$

Thus, for $1 \le j \le v$,

$$\begin{aligned}|\Theta_{w+j}| &\le \tfrac{1}{2} + \tfrac{1}{2}|b_1| + \cdots + \tfrac{1}{2}|b_r| + \tfrac{1}{2}|b_{r+j}| + C \cdot |\beta_{w+j} + b_1\alpha_{1,w+j} + \cdots + b_r\alpha_{r,w+j} + b_{r+j}\pi| \\ &\le \frac{2\pi + 1}{2\pi} + \mathcal{B}_1 + 2C \cdot c_{29}(u+j) \cdot \exp(-c_{26} \cdot B) \\ &\le \mathcal{A}_2 + c_{29}(u+j) \cdot \eta,\end{aligned}$$

where the second inequality follows from (34), (60), and (61).

By assumption, $\boldsymbol{w} + \boldsymbol{b}_e \cdot M \ne \mathbf{0}$; hence

$$\begin{aligned}\mathcal{D}^2 &\le \|\boldsymbol{w} + \boldsymbol{b}_e \cdot M\|_2^2 \\ &= b_{u+v-1}^2 + \cdots + b_r^2 + \Theta_1^2 + \cdots + \Theta_{d-2}^2 \\ &\le b_{u+v-1}^2 + \cdots + b_r^2 + w\mathcal{A}_1^2 + v\mathcal{A}_2^2 + 2\mathcal{B}_4\eta + \mathcal{B}_3\eta^2.\end{aligned}$$

However, $|b_{u+v-1}| \le \|\boldsymbol{b}\|_\infty \le \mathcal{B}_\infty$. Moreover, by (46) we have $|b_{u+v-1+i}| \le \rho_i$ for $i = 1, \dots, s$, where ρ_i is given in (45). It follows that

$$\begin{aligned}\mathcal{D}^2 &\le \mathcal{B}_\infty^2 + \rho_1^2 + \cdots + \rho_s^2 + w\mathcal{A}_1^2 + v\mathcal{A}_2^2 + 2\mathcal{B}_4\eta + \mathcal{B}_3\eta^2 \\ &= \mathcal{B}_2^2 - w\mathcal{B}_\infty^2 + w\mathcal{A}_1^2 + v\mathcal{A}_2^2 + 2\mathcal{B}_4\eta + \mathcal{B}_3\eta^2 \qquad \text{(from (48))} \\ &= \mathcal{B}_5^2 + 2\mathcal{B}_4\eta + \mathcal{B}_3\eta^2 \\ &= \mathcal{B}_5^2 + \mathcal{B}_3\left(\eta + \frac{\mathcal{B}_4}{\mathcal{B}_3}\right)^2 - \frac{\mathcal{B}_4^2}{\mathcal{B}_3}.\end{aligned}$$

Recall our assumption that $\mathcal{B}_5 < \mathcal{D}$. Thus

$$\frac{\mathcal{B}_4^2}{\mathcal{B}_3} < \mathcal{D}^2 - \mathcal{B}_5^2 + \frac{\mathcal{B}_4^2}{\mathcal{B}_3} \le \mathcal{B}_3\left(\eta + \frac{\mathcal{B}_4}{\mathcal{B}_3}\right)^2,$$

and so

$$0 < \frac{\sqrt{\mathcal{B}_3(\mathcal{D}^2 - \mathcal{B}_5^2) + \mathcal{B}_4^2} - \mathcal{B}_4}{\mathcal{B}_3} \leq \eta.$$

However $\eta = 2C \cdot \exp(-c_{26} \cdot B)$. This yields the bound

$$B \leq \frac{1}{c_{26}} \cdot \log\left(\frac{2C \cdot \mathcal{B}_3}{\sqrt{\mathcal{B}_3(\mathcal{D}^2 - \mathcal{B}_5^2) + \mathcal{B}_4^2} - \mathcal{B}_4}\right),$$

which gives (64). □

Heuristic. It remains to decide on a reasonable choice for C. We expect that the determinant of the matrix M is approximately C^{d-2}. Thus the distance between adjacent vectors in L is expected to be in the region of $C^{(d-2)/n}$, and so we anticipate (very roughly) that $\mathcal{D} \sim C^{(d-2)/n}$. We would like $\mathcal{D} > \mathcal{B}_5$. Therefore it is reasonable to choose $C \gg \mathcal{B}_5^{n/(d-2)}$. If, for a particular choice of C, the condition $\mathcal{D} > \mathcal{B}_5$ fails, then we simply try again with a larger choice of C.

Remarks. Our approach is somewhat unusual in that it uses all $d-2$ available approximate relations to reduce the initial bound. In contrast, it is much more common to use one relation (e.g., [Tzanakis and de Weger 1989, Section 16]) to reduce the bound. In most examples, we have found that both approaches give similar reductions in the size of the bound and that there is no advantage in using one over the other. However in some examples the approach of using only one relation fails spectacularly. Here are two such scenarios:

(i) Suppose δ_1 (say) belongs to a proper subfield K' of K. Now let σ_2, σ_3 be distinct embeddings of K that agree on K'. Then, in the notation of Lemma 8.7 we find $\alpha_{1,3} = \log|\sigma_3(\delta_1)/\sigma_2(\delta_1)| = 0$, and so the coefficient of the unknown b_1 is zero in the approximate relation (57). Therefore the one relation (57) on its own fails to provide any information on the size of b_1. In practice, the lattice constructed in [Tzanakis and de Weger 1989, Section 16] from this one relation will contain the tiny vector $(1, 0, \ldots, 0)$, and this will result in the computational failure of the closest vector algorithm.

(ii) We continue to suppose that δ_1 belongs to the proper subfield K' as above. Let σ_{u+1} be a complex embedding of K that extends a real embedding of K', and suppose for simplicity that $\sigma_{u+1}(\delta_1)$ is positive. Then again, $\alpha_{1,w+1} = 0$ in the approximate relation (60), and so that relation on its own fails to control b_1.

In the above two examples, we chose to illustrate the possible failure of the approach of using one relation by imposing $\delta_1 \in K'$ where K' is a subfield of K. However, a similar failure occurs (and is more difficult to find) if the S-unit basis $\delta_1, \ldots, \delta_r$ is multiplicatively dependent over K', meaning that there is some nontrivial $(c_1, \ldots, c_r) \in \mathbb{Z}^r$ such that $\delta_1^{c_1} \cdots \delta_r^{c_r} \in K'$.

In Proposition 9.2, we require $\boldsymbol{b}_e \cdot M \neq -\boldsymbol{w}$. Of course, if M is nonsingular, we can simply check whether $\boldsymbol{b}_e = -\boldsymbol{w} \cdot M^{-1}$ yields a solution, and therefore there is no harm in making this assumption. In all our examples, M has been nonsingular, and we expect that by choosing C large enough we can ensure that this happens. However, if M is singular then the equation $\boldsymbol{b}_e \cdot M = -\boldsymbol{w}$ either has no solutions or the solutions belong to the translate of a sublattice of $\mathbb{Z}^n$ whose rank is the corank of the matrix M. A glance

at the matrix M reveals that this corank is at most $w = u + v - 2$. If this case was to ever arise in practice, we would need to enumerate all vectors $\boldsymbol{b}_e$ satisfying $\boldsymbol{b}_e \cdot M = -\boldsymbol{w}$ and the bound in Lemma 9.1 and test if they lead to solutions.

9.1. ***Example 1.4 continued.*** We continue giving details for the tuple $(\tau, \delta_1, \ldots, \delta_{10})$ alluded to on page 690. The values of $\mathcal{B}_\infty$ and $\mathcal{B}_2$ are given in (40). The set S consists of five primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$ given by (33). By applying Proposition 7.2 we had (page 694) obtained bounds 237, 292, 354, 518, 821 for $\mathrm{ord}_{\mathfrak{p}_j}(a_0 X - \theta Y)$ with $i = 1, \ldots, 5$ respectively; these are the values denoted $k_j - 1$ in (41). Now $\mathrm{ord}_{\mathfrak{p}_j}(\tau) = 0, 0, 1, 0, 0$ respectively for $j = 1, \ldots, 5$. Letting ε be as in (42), we may take $(-k_j', k_j'')$ in (43) to be $(0, 237)$, $(0, 292)$, $(-1, 353)$, $(0, 518)$, $(0, 821)$ respectively. This allows us to compute the constant c_{21} defined in Lemma 8.1. We find that $c_{21} \approx 2842.79$. The field K has signature $(u, v) = (1, 5)$ and thus there is only one possibility for $\sigma \in \mathcal{E}_K^{\mathbb{R}}$. We therefore take $\sigma_1 = \sigma$ to be the unique real embedding. For illustration, we give the values of constants appearing in Section 8:

$$c_{22} \approx 30.31, \quad c_{23} = 1, \quad c_{24} \approx 2873.10, \quad c_{25} \approx 5.91 \times 10^{1247}, \quad c_{26} \approx 0.35,$$
$$c_{27} \approx 5.91 \times 10^{1247}, \quad c_{28} \approx 1.40 \times 10^{1246}, \quad c_{29}(2) \approx 1.25 \times 10^{1246},$$
$$c_{29}(3) \approx 8.30 \times 10^{1245}, \quad c_{29}(4) \approx 7.83 \times 10^{1245}, \quad c_{29}(5) \approx 9.21 \times 10^{1245},$$
$$c_{29}(6) \approx 1.40 \times 10^{1246}, \quad c_{30} \approx 8290.02.$$

Lemma 8.7 gives $w = u + v - 2 = 4$ approximate relations and Lemma 8.8 gives another $v = 5$ relations. Therefore we have $d - 2 = 9$ relations altogether, and $n = \#S + d - 2 = 15$. Therefore the matrix M is 15×15 and the lattice L belongs to $\mathbb{Z}^{15}$. We find that

$$\mathcal{B}_1 \approx 7.85 \times 10^{222}, \quad \mathcal{A}_1 \approx 3.92 \times 10^{222}, \quad \mathcal{A}_2 \approx 7.85 \times 10^{222}, \quad \mathcal{B}_3 \approx 2.59 \times 10^{2493},$$
$$\mathcal{B}_4 \approx 7.57 \times 10^{1469}, \quad \mathcal{B}_5 \approx 1.93 \times 10^{223}.$$

In accordance with the above heuristic, our program chooses

$$C = [\mathcal{B}_5^{n/(d-2)}] \approx 1.39 \times 10^{372}.$$

The matrix M and the lattice L are too huge to reproduce here, but we point out that

$$[\mathbb{Z}^{15} : L] \approx 2.66 \times 10^{3357}; \quad \mathcal{D} \approx 7.23 \times 10^{223}.$$

In this case, $\boldsymbol{w} \notin L$ so that $\mathcal{D}$ is computed using $D(L, \boldsymbol{w})$. Hence the hypothesis $\mathcal{D} > \mathcal{B}_5$ of Proposition 9.2 is satisfied. We may therefore apply Proposition 9.2 to obtain a new bound for B given by (64):

$$B \leq 9270.82.$$

We now start again with $\mathcal{B}_\infty = 9270$ and repeat the previous steps, first for obtaining bounds for $\mathrm{ord}_{\mathfrak{p}_j}(a_0 X - \theta Y)$ and then for writing down the lattice L and applying Proposition 9.2. Table 2 illustrates the results.

Iteration	$\mathcal{B}_\infty$	bounds for $\mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)$ with $1\le j\le 5$				
0	1.57×10^{222}	237	292	354	518	821
1	9270	4	5	8	10	15
2	251	3	3	5	6	10
3	190	2	3	5	6	9
4	180	2	3	5	6	9
5	180	2	3	5	6	9

Table 2. We successively reduce the bounds for B and for $\mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)$, where $j=1,\dots,5$.

Note that at the fifth iteration we fail to obtain any improvement on the bounds, and so we stop there. Recall that $r=10$ and that $B=\max(|b_1|,\dots,|b_{10}|)$, where $b_1,\dots,b_{10}$ are the exponents in (15). Our final bound is $B\le 180$. The set of possible integer tuples $(b_1,\dots,b_{10})$ satisfying this bound has size

$$(2\times 180+1)^{10}=362^{10}\approx 3.86\times 10^{25}.$$

The huge size of this region does not allow brute force enumeration of the solutions. Instead, one can reduce the number of tuples to consider by using the bounds we have obtained for $\mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)$. We let $\kappa_j=2,3,5,6,9$ for $j=1,\dots,5$, respectively. We know that $0\le \mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)\le\kappa_j$, and so there are κ_j+1 possibilities for the $\mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)$. Let $(k_1,\dots,k_5)$ be some tuple of integers satisfying $0\le k_j\le\kappa_j$. The condition $\mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)=k_j$ simply defines a hyperplane of codimension 1 in the space of possible $(b_1,\dots,b_{10})$. Imposing all five conditions $\mathrm{ord}_{\mathfrak{p}_j}(a_0X-\theta Y)=k_j$ with $j=1,\dots,5$ cuts down the dimension from 10 to 5. Thus we expect that the search region should (very roughly) have size

$$(\kappa_1+1)\cdots(\kappa_5+1)\cdot 362^5\approx 3.13\times 10^{16}.$$

This is still way beyond brute force enumeration and motivates our next section.

10. Sieving

In order to resolve the Thue–Mahler equation

$$F(X,Y)=a\cdot p_1^{z_1}\cdots p_v^{z_v},\quad X,Y\in\mathbb{Z},\ \gcd(X,Y)=\gcd(a_0,Y)=1,$$

we have first reduced the problem to that of resolving a number of equations of the form (15), subject to the restrictions (16), (17). Recall that $B=\max\{|b_1|,\dots,|b_r|\}$, where $\boldsymbol{b}=(b_1,\dots,b_r)\in\mathbb{Z}^r$ denotes the vector of unknown exponents to solve for. For each such equation (15), we have used the theory of linear forms in logarithms to obtain a bound for B, and moreover, we have explained how to repeatedly reduce this bound. During each of these iterations, we have simultaneously reduced the bounds on the ∞-norm, the 1-norm, and the 2-norm of $\boldsymbol{b}$. Let us denote the final bound for the ∞-norm of $\boldsymbol{b}$ by $\mathcal{B}'_f$ and write $\mathcal{B}_f$ for the final bound on the 2-norm of $\boldsymbol{b}$. Thus

$$\|\boldsymbol{b}\|_2\le\mathcal{B}_f,\quad \|\boldsymbol{b}\|_\infty\le\mathcal{B}'_f. \tag{65}$$

We have also explained how to obtain and reduce the bounds on $\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y)$ for $\mathfrak{p} \in S$. Suppose that at the end of this process, our bounds are

$$0 \le \mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \le \kappa_{\mathfrak{p}} \quad \text{for } \mathfrak{p} \in S. \tag{66}$$

Unfortunately, in our high-rank examples (i.e., when the S-unit rank r is large) the final bound $\mathcal{B}'_f$ is often too large to allow for brute force enumeration of solutions. Instead, we shall sieve for solutions using both the primes $\mathfrak{p}$ in S, and also rational primes p whose support in $\mathcal{O}_K$ is disjoint from S. The objective of the sieve is to show that the solutions $\boldsymbol{b}$ belong to a union of a certain (hopefully small) number of cosets $\boldsymbol{w} + L$, where the L are sublattices of $\mathbb{Z}^r$. As the sieve progresses, the determinants of the lattices L will grow. The larger the determinant, the fewer vectors we expect belonging to $\boldsymbol{w} + L$ and satisfying $\|\boldsymbol{b}\|_2 \le \mathcal{B}_f$, and the easier it should be to find these vectors using the algorithm of Fincke and Pohst [1985]. The following lemma is a helpful guide to when Fincke and Pohst should be applied.

Lemma 10.1. *Let L be a sublattice of $\mathbb{Z}^r$. Suppose $\lambda(L) > 2\mathcal{B}_f$, where $\lambda(L)$ denotes the length of the shortest nonzero vector in L. Then there is at most one vector $\boldsymbol{b}$ in the coset $\boldsymbol{w} + L$ satisfying $\|\boldsymbol{b}\|_2 \le \mathcal{B}_f$. Moreover, any such $\boldsymbol{b}$ is equal to $\boldsymbol{w} + \boldsymbol{c}(L, -\boldsymbol{w})$.*

Proof. Suppose there are vectors $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \boldsymbol{w} + L$ both satisfying $\|\boldsymbol{b}_i\|_2 \le \mathcal{B}_f$. Then $\boldsymbol{b}_1 - \boldsymbol{b}_2 \in L$ and $\|\boldsymbol{b}_1 - \boldsymbol{b}_2\|_2 \le 2\mathcal{B}_f$. As $\lambda(L) > 2\mathcal{B}_f$ we see that $\boldsymbol{b}_1 = \boldsymbol{b}_2$. The second part follows from Lemma 7.1. □

We continue sieving until the lattices L satisfy $\lambda(L) > 2\mathcal{B}_f$. We then apply the Fincke–Pohst algorithm to determine $\boldsymbol{c}(L, -\boldsymbol{w})$ and check whether the vector $\boldsymbol{b} = \boldsymbol{w} + \boldsymbol{c}(L, -\boldsymbol{w})$ leads to a solution.

10.1. ***Sieving using the primes of S.*** To recap, we seek solutions $(X, Y, \boldsymbol{b})$ to

$$a_0X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r},$$

subject to the conditions

$$X, Y \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad \gcd(a_0, Y) = 1, \quad b_i \in \mathbb{Z},$$

and such that

$$\|\boldsymbol{b}\|_2 \le \mathcal{B}_f, \quad \text{and} \quad 0 \le \mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \le \kappa_{\mathfrak{p}} \quad \text{for every } \mathfrak{p} \in S.$$

In particular, this last inequality (66) asserts that $\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y)$ belongs to a certain set of values $0, 1, \ldots, \kappa_{\mathfrak{p}}$. The following proposition reduces this list somewhat, and for any k in this reduced list, yields a vector $\boldsymbol{w}_k$ and a sublattice L_k of $\mathbb{Z}^r$ such that $\boldsymbol{b} \in \boldsymbol{w}_k + L_k$ whenever $\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) = k$.

Proposition 10.2. *Let $\mathfrak{p} \in S$. Let $\theta_0 \in \mathbb{Z}$ satisfy $\theta_0 \equiv \theta \pmod{\mathfrak{p}^{\kappa_{\mathfrak{p}}}}$. Let $\mathfrak{a}$ and $\mathcal{T}_1$ be as in* (37)*. Define*

$$\eta : \mathbb{Z}^r \to \mathbb{Z}, \quad \eta(n_1, \ldots, n_r) = n_1 \,\mathrm{ord}_{\mathfrak{p}}(\delta_1) + \cdots + n_r \,\mathrm{ord}_{\mathfrak{p}}(\delta_r), \quad L'' = \mathrm{Ker}(\eta).$$

Let

$$\mathcal{K}'' := (\mathrm{ord}_{\mathfrak{p}}(\tau) + \mathrm{Image}(\eta)) \cap \{0 \le k \le \kappa_{\mathfrak{p}} : \gcd(\mathfrak{a}^k, \theta - \theta_0) = \gcd(\mathfrak{a}^k, \mathcal{T}_1)\}.$$

For $k \in \mathcal{K}''$, let $\boldsymbol{w}_k''$ be any vector in $\mathbb{Z}^r$ satisfying $\eta(\boldsymbol{w}_k'') = k - \mathrm{ord}_{\mathfrak{p}}(\tau)$. If $k \in \mathcal{K}''$ satisfies $k \geq 1$, we will let ϕ and τ_0 be as in Proposition 7.2 (these depend on k). Let

$$\mathcal{K}' := \begin{cases} \{k \in \mathcal{K}'' : \overline{\tau}_0 \in \mathrm{Image}(\phi)\} & \text{if } 0 \notin \mathcal{K}'', \\ \{0\} \cup \{k \in \mathcal{K}'' : \overline{\tau}_0 \in \mathrm{Image}(\phi)\} & \text{if } 0 \in \mathcal{K}''. \end{cases}$$

For $k \in \mathcal{K}'$ with $k \geq 1$, we let $L_k' = \mathrm{Ker}(\phi)$ and $\boldsymbol{w}_k'$ be any vector in $\mathbb{Z}^r$ satisfying $\phi(\boldsymbol{w}_k') = \overline{\tau}_0$. Let $\boldsymbol{w}_0' = \boldsymbol{0}$, $L_0' = \mathbb{Z}^r$, and

$$\mathcal{K} := \{k \in \mathcal{K}' : (\boldsymbol{w}_k'' + L'') \cap (\boldsymbol{w}_k' + L_k') \neq \varnothing\}.$$

For $k \in \mathcal{K}$, write

$$L_k := L'' \cap L_k'$$

and choose any $\boldsymbol{w}_k \in \mathbb{Z}^r$ such that

$$\boldsymbol{w}_k + L_k := (\boldsymbol{w}_k'' + L'') \cap (\boldsymbol{w}_k' + L_k').$$

Let $k = \mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y)$. Then $k \in \mathcal{K}$ and $\boldsymbol{b} \in \boldsymbol{w}_k + L_k$.

Proof. By (66), the valuation $k := \mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y)$ satisfies $0 \leq k \leq \kappa_{\mathfrak{p}}$. Moreover, by Proposition 7.2, part (i), we have $\gcd(\mathfrak{a}^k, \theta - \theta_0) = \gcd(\mathfrak{a}^k, \mathcal{T}_1)$. By (15), we know $k \in \mathrm{ord}_{\mathfrak{p}}(\tau) + \eta(\boldsymbol{b})$ and thus $k \in \mathcal{K}''$ and $\boldsymbol{b} \in \boldsymbol{w}_k'' + L''$. In particular, the proposition follows in the case $k = 0$. We therefore suppose $k \geq 1$. By Proposition 7.2, part (ii) and its proof, it follows that $k \in \mathcal{K}'$ and $\boldsymbol{b} \in \boldsymbol{w}_k' + L_k'$, completing the proof. □

Remark. For each prime $\mathfrak{p} \in S$, Proposition 10.2 yields a number of cosets $\boldsymbol{w}_k + L_k$ and tells us that $\boldsymbol{b}$ belongs to one of them. Note that L'' is a subgroup of $\mathbb{Z}^r$ of rank $r-1$. Moreover, the subgroup L_k' has finite index in $\mathbb{Z}^r$. Therefore $L_k := L_k' \cap L''$ has rank $r-1$. From the remarks following Proposition 7.2 (where L_k' is called L) we expect L_k' to have index $p^{(d-2)k}$ in $\mathbb{Z}^r$. In particular, the larger the value of k, the larger the index of L_k'. Of course the number of cosets is bounded above by $\kappa_p + 1$.

10.2. ***Sieving with other primes.*** Given a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, write $\mathcal{O}_{\mathfrak{q}}$ for the localization of $\mathcal{O}_K$ at $\mathfrak{q}$,

$$\mathcal{O}_{\mathfrak{q}} = \{\alpha \in K : \mathrm{ord}_{\mathfrak{q}}(\alpha) \geq 0\}.$$

Now let q be a rational prime. Define

$$\mathcal{O}_q = \bigcap_{\mathfrak{q} \mid q} \mathcal{O}_{\mathfrak{q}} = \{\alpha \in K : \mathrm{ord}_{\mathfrak{q}}(\alpha) \geq 0 \text{ for all } \mathfrak{q} \mid q\}.$$

The group of invertible elements $\mathcal{O}_q^\times$ consists of all $\alpha \in K$ such that $\mathrm{ord}_{\mathfrak{q}}(\alpha) = 0$ for all prime ideals $\mathfrak{q} \mid q$.

Let $\tau, \delta_1, \ldots, \delta_r$ be as in (15). Let q be a rational prime coprime to the supports of $\tau, \delta_1, \ldots, \delta_r$. Thus $\tau, \delta_1, \ldots, \delta_r$ all belong to $\mathcal{O}_q^\times$. Let

$$\mathfrak{A}_q := (\mathcal{O}_q / q\mathcal{O}_q)^\times.$$

This is canonically isomorphic to $(\mathcal{O}_K / q\mathcal{O}_K)^\times$. Let

$$\mu : \mathbb{F}_q^\times \hookrightarrow \mathfrak{A}_q, \quad \alpha + q\mathbb{Z} \mapsto \alpha + q\mathcal{O}_q$$

be the natural map, and let

$$\mathfrak{B}_q := \mathfrak{A}_q / \mu(\mathbb{F}_q^\times)$$

be the cokernel of μ. We denote the induced homomorphism $\mathcal{O}_q^\times \to \mathfrak{B}_q$ by

$$\pi_q : \mathcal{O}_q^\times \to \mathfrak{B}_q, \quad \beta \mapsto (\beta + q\mathcal{O}_q) \cdot \mu(\mathbb{F}_q^\times).$$

Define

$$\phi_q : \mathbb{Z}^r \to \mathfrak{B}_q, \quad (m_1, \dots, m_r) \mapsto \pi_q(\delta_1)^{m_1} \cdots \pi_q(\delta_r)^{m_r}.$$

Proposition 10.3. *Let*

$$R_q = \{a_0 u - \theta : u \in \{0, 1, \dots, q-1\}\} \cup \{a_0\} \quad \textit{and} \quad S_q = \{\pi_q(r)/\pi_q(\tau) : r \in R_q \cap \mathcal{O}_q^\times\} \subseteq \mathfrak{B}_q.$$

Let

$$T_q = S_q \cap \phi_q(\mathbb{Z}^r) \quad \textit{and} \quad L_q = \mathrm{Ker}(\phi_q).$$

Finally, let $W_q \subset \mathbb{Z}^r$ be a set of size $\#T_q$ such that for every $t \in T_q$ there is some $\boldsymbol{w} \in W_q$ with $\phi_q(\boldsymbol{w}) = t$. Then $\boldsymbol{b} \in W_q + L_q$.

Proof. Since $\tau, \delta_1, \dots, \delta_r \in \mathcal{O}_q^\times$, we have $a_0 X - \theta Y \in \mathcal{O}_q^\times$. We want to determine the possibilities for the image of the algebraic integer $a_0 X - \theta Y$ in $\mathfrak{B}_q$. Since X and Y are coprime, q divides at most one of X, Y. If $q \nmid Y$ then

$$a_0 X - \theta Y \equiv v \cdot (a_0 u - \theta) \pmod{q\mathcal{O}_q}$$

for some $u \in \{0, 1, \dots, q-1\}$ and some $v \in \mathbb{F}_q^\times$. If $q \mid Y$ then $q \nmid X$ and

$$a_0 X - \theta Y \equiv a_0 v \pmod{q\mathcal{O}_q}$$

for some $v \in \mathbb{F}_q^\times$. We conclude that $a_0 X - \theta Y \equiv v \cdot r \pmod{q\mathcal{O}_q}$ where $v \in \mathbb{F}_q^\times$ and $r \in R_q$. Moreover, since $a_0 X - \theta Y \in \mathcal{O}_q^\times$ we see that $r \in R_q \cap \mathcal{O}_q^\times$. Now

$$\pi_q(a_0 X - \theta Y) = \pi_q(r)\pi_q(v) = \pi_q(r).$$

It follows that $\pi_q(a_0 X - \theta Y)/\pi_q(\tau) \in S_q$. However

$$\phi_q(\boldsymbol{b}) = \pi_q(\delta_1)^{b_1} \cdots \pi_q(\delta_r)^{b_r} = \pi_q(a_0 X - \theta Y)/\pi_q(\tau),$$

where the first equality follows from the definition of ϕ_q and the second from (15). Thus $\phi_q(\boldsymbol{b}) = t$ for some $t \in T_q$. By definition of W_q, there is some $\boldsymbol{w} \in W_q$ with $\phi_q(\boldsymbol{w}) = t = \phi_q(\boldsymbol{b})$, thus $\boldsymbol{b} - \boldsymbol{w} \in L_q$. □

Heuristic. It is appropriate that we heuristically "measure" the quality of information that Proposition 10.3 gives us about the solutions. A priori, $\phi_q(\boldsymbol{b})$ could be any element in $\phi_q(\mathbb{Z}^r) \subseteq \mathfrak{B}_q$. However, the lemma tells us that $\phi_q(\boldsymbol{b})$ belongs to T_q. We want to estimate the ratio $\#T_q/\#\phi_q(\mathbb{Z}^r)$; the smaller this ratio is, the better the information is. It is convenient to suppose that q is unramified in $\mathcal{O}_K$. Thus

$$\mathcal{O}_q/q\mathcal{O}_q \cong \mathcal{O}_K/q\mathcal{O}_K \cong \bigoplus_{\mathfrak{q} \mid q} \mathcal{O}_K/\mathfrak{q}.$$

Each summand $\mathcal{O}_K/\mathfrak{q}$ is a finite field of cardinality $\mathrm{Norm}(\mathfrak{q})$. By definition

$$\mathfrak{A}_q := (\mathcal{O}_q/q\mathcal{O}_q)^\times \cong \prod_{\mathfrak{q} \mid q} (\mathcal{O}_K/\mathfrak{q})^\times.$$

Thus

$$\#\mathfrak{A}_q = \prod_{\mathfrak{q}\mid q}(\mathrm{Norm}(\mathfrak{q})-1), \quad \#\mathfrak{B}_q = \frac{1}{q-1}\cdot\prod_{\mathfrak{q}\mid q}(\mathrm{Norm}(\mathfrak{q})-1).$$

Moreover $\prod_{\mathfrak{q}\mid q}\mathrm{Norm}(\mathfrak{q}) = q^d$ where $d = [K:\mathbb{Q}]$ is the degree of the original Thue–Mahler equation. Thus $\#\mathfrak{B}_q \approx q^{d-1}$. However $S_q \subseteq \phi(\mathbb{Z}^r) \subseteq \mathfrak{B}_q$ has at most $q+1$ elements, and so $\#S_q/\#\mathfrak{B}_q \lessapprox 1/q^{d-2}$. Now

$$\frac{\#T_q}{\#\phi_q(\mathbb{Z}^r)} = \frac{\#S_q \cap \phi_q(\mathbb{Z}^r)}{\#\phi_q(\mathbb{Z}^r)}.$$

It is reasonable to expect that the elements of S_q are uniformly distributed among the elements of $\mathfrak{B}_q$ and so we expect $\#T_q/\#\phi_q(\mathbb{Z}^r) \lessapprox 1/q^{d-2}$.

10.3. ***The sieve.*** We will sieve with the primes $\mathfrak{p} \in S$ as in Proposition 10.2 and also with additional rational primes q as in Proposition 10.3. We would like to choose a suitable set $\mathfrak{S}$ of such primes q. The most expensive computation we will need to do for $q \in \mathfrak{S}$ is to compute, for each $t \in T_q$, some $\boldsymbol{w} \in \mathbb{Z}^r$ such that $\phi_q(\boldsymbol{w}) = t$. This involves a discrete logarithm computation in the group $\mathfrak{B}_q$, and to do this quickly we need $\mathfrak{B}_q$ to be a product of cyclic factors that have relatively small order. We therefore like to avoid those q where there are $\mathfrak{q} \mid q$ that have large norm. In all our examples we found it enough to take $\mathfrak{S}$ to be the set of primes $q \le 500$, where each $\mathfrak{q} \mid p$ satisfies $\mathrm{Norm}(\mathfrak{q}) \le 10^{10}$ and where the support of q is disjoint from the supports of $\tau, \delta_1, \ldots, \delta_r$.

Procedure 10.4. `Solutions`$(L_c, \boldsymbol{w}_c, S_c, \mathfrak{S}_c)$.
Input: L_c sublattice of $\mathbb{Z}^r$, $\boldsymbol{w}_c \in \mathbb{Z}^r$, $S_c \subseteq S$, $\mathfrak{S}_c \subseteq \mathfrak{S}$.
Output: Set of solutions $(X, Y, \boldsymbol{b})$ to (15), (16) satisfying $\boldsymbol{b} \in \boldsymbol{w}_c + L_c$ and $\|\boldsymbol{b}\|_2 \le \mathcal{B}_f$.

1. **IF** $\lambda(L_c) > 2\mathcal{B}_f$ or ($S_c = \varnothing$ and $\mathfrak{S}_c = \varnothing$) **THEN**
2. Apply Fincke–Pohst to find all vectors in $\boldsymbol{b} \in \boldsymbol{w}_c + L$ satisfying $\|\boldsymbol{b}\|_2 \le \mathcal{B}_f$.
3. Keep only those $\boldsymbol{b}$ that lead to solutions (X, Y) on (15), (16).
4. **RETURN:** Set of $(X, Y, \boldsymbol{b})$.
5. **END**.
6. **ELSE**
7. **IF** $S_c \neq \varnothing$ **THEN**
8. Choose $\mathfrak{p} \in S_c$. Let $S_c' = S_c \setminus \{\mathfrak{p}\}$.
9. Compute $\mathcal{K}$ as in Proposition 10.2.
10. For each $k \in \mathcal{K}$ compute $\boldsymbol{w}_k$, L_k as in Proposition 10.2.
11. Let $\mathcal{K}^*$ be the subset of $k \in \mathcal{K}$ such that $(\boldsymbol{w}_k + L_k) \cap (\boldsymbol{w}_c + L_c) \neq \varnothing$.
12. For each $k \in \mathcal{K}^*$ let $L_{c,k} = L_c \cap L_k$.
13. For each $k \in \mathcal{K}^*$ choose $\boldsymbol{w}_{c,k} \in \mathbb{Z}^r$ so that $\boldsymbol{w}_{c,k} + L_{c,k} = (\boldsymbol{w}_k + L_k) \cap (\boldsymbol{w}_c + L_c)$.
14. **RETURN:** $\bigcup_{k\in\mathcal{K}^*}$ `Solutions`$(L_{c,k}, \boldsymbol{w}_{c,k}, S_c', \mathfrak{S}_c)$.
15. **END**.
16. **ELSE**

17. Choose $q \in \mathfrak{S}_c$. Let $\mathfrak{S}_c' = \mathfrak{S}_c \setminus \{q\}$.
18. Compute W_q, L_q as in Proposition 10.3.
19. Let $L_c' = L_c \cap L_q$.
20. Let $W_q^* = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ be the subset of $\boldsymbol{w} \in W_q$ such that $(\boldsymbol{w} + L_q) \cap (\boldsymbol{w}_c + L_c) \neq \varnothing$.
21. For $i = 1, \ldots, m$ choose $\boldsymbol{w}_{c,i}$ such that $\boldsymbol{w}_{c,i} + L_c' = (\boldsymbol{w} + L_q) \cap (\boldsymbol{w}_c + L_c)$.
22. **RETURN:** $\bigcup_{i=1}^{m} \texttt{Solutions}(L_c', \boldsymbol{w}_{c,i}, \varnothing, \mathfrak{S}_c')$.
23. **END**.
24. **ENDIF**
25. **ENDIF**

Let us explain how Procedure 10.4 works. The procedure starts with a coset $\boldsymbol{w}_c + L_c$ and sets $S_c \subseteq S$ and $\mathfrak{S}_c \subseteq \mathfrak{S}$ (the subscript c stands for "cumulative"). The objective is to return all solutions $(X, Y, \boldsymbol{b})$ to (15), (16) with $\boldsymbol{b} \in \boldsymbol{w}_c + L_c$ and satisfying $\|\boldsymbol{b}\|_2 \leq \mathcal{B}_f$. The primes in S_c and $\mathfrak{S}_c$ are used, via Propositions 10.2 and 10.3, to replace $\boldsymbol{w}_c + L_c$ by a union of cosets of sublattices of L_c.

We now explain lines 1–5 of the procedure. If $\lambda(L) > 2\mathcal{B}_f$, then by Lemma 10.1, the coset $\boldsymbol{w}_c + L_c$ has at most one vector $\boldsymbol{b}$ that satisfies $\|\boldsymbol{b}\|_2 \leq \mathcal{B}_f$, and this maybe found by the algorithm of Fincke and Pohst. If $S_c = \varnothing$ and $\mathfrak{S}_c = \varnothing$, then we have run out of sieving primes and we simply apply the Fincke–Pohst algorithm to determine all $\boldsymbol{b} \in \boldsymbol{w}_c + L_c$ such that $\|\boldsymbol{b}\|_2 \leq \mathcal{B}_f$. We test all resulting $\boldsymbol{b}$ to see if they lead to solutions $(X, Y, \boldsymbol{b})$ and return the set of solutions. We end here. In both these cases, no further branching of the procedure occurs.

If we have reached line 6, then either S_c is nonempty or $\mathfrak{S}_c$ is nonempty. We first treat the case where S_c is nonempty (lines 8–14). We choose $\mathfrak{p} \in S_c \subseteq S$ to sieve with and let $S_c' = S_c \setminus \{\mathfrak{p}\}$. Here we apply Proposition 10.2. This gives a finite set $\mathcal{K}$ of values k and lattice cosets $\boldsymbol{w}_k + L_k$ such that $\boldsymbol{b} \in \boldsymbol{w}_k + L_k$ for some $k \in \mathcal{K}$. However, the $\boldsymbol{b}$ we are interested in belong to $\boldsymbol{w}_c + L_c$. We let $\mathcal{K}^*$ be those values $k \in \mathcal{K}$ such that $(\boldsymbol{w}_c + L_c) \cap (\boldsymbol{w}_k + L_k) \neq \varnothing$. It is now clear that every $\boldsymbol{b}$ we seek belongs to $(\boldsymbol{w}_c + L_c) \cap (\boldsymbol{w}_k + L_k)$ for some $k \in \mathcal{K}^*$. However $(\boldsymbol{w}_c + L_c) \cap (\boldsymbol{w}_k + L_k) = \boldsymbol{w}_{c,k} + L_{c,k}$ where $L_{c,k} = L_c \cap L_k$, for a suitable coset representative $\boldsymbol{w}_{c,k}$. We apply the procedure to the set $(L_{c,k}, \boldsymbol{w}_{c,k}, S_c', \mathfrak{S}_c)$ for each $k \in \mathcal{K}^*$ to compute those $\boldsymbol{b}$ belonging to $\boldsymbol{w}_{c,k} + L_{c,k}$ and return the union.

If however $S_c = \varnothing$, then (lines 17–22) we choose a prime $q \in \mathfrak{S}_c \subseteq \mathfrak{S}$ to sieve with, and we let $\mathfrak{S}_c' = \mathfrak{S}_c \setminus \{q\}$. Now we apply Proposition 10.3. This gives a lattice L_q and a finite set W_q such that $\boldsymbol{b} \in W_q + L_q$. Therefore there is some $\boldsymbol{w} \in W_q$ such that $\boldsymbol{b} \in (\boldsymbol{w} + L_q) \cap (\boldsymbol{w}_c + L_c)$. We let W_q^* be the subset of those $\boldsymbol{w} \in W_q$ such that $(\boldsymbol{w} + L_q) \cap (\boldsymbol{w}_c + L_c) \neq \varnothing$, and write $W_q^* = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$. Now $\boldsymbol{b} \in (\boldsymbol{w}_i + L_q) \cap (\boldsymbol{w}_c + L_c)$ for some $i = 1, \ldots, m$. Write $L_c' = L_c \cap L_q$. Then $(\boldsymbol{w}_i + L_q) \cap (\boldsymbol{w}_c + L_c)$ is a coset of L_c' for $i = 1, \ldots, m$, and we choose $\boldsymbol{w}_{c,i}$ so that $\boldsymbol{w}_{c,i} + L_c' = (\boldsymbol{w}_i + L_q) \cap (\boldsymbol{w}_c + L_c)$. It is therefore enough to find the $\boldsymbol{b}$ belonging to each one of these $\boldsymbol{w}_{c,i} + L_c'$. Thus we apply the procedure to $(L_c', \boldsymbol{w}_{c,i}, \varnothing, \mathfrak{S}_q')$ for $i = 1, \ldots, m$, collect the solutions and return their union (line 22).

Remarks. • To compute the solutions to (15) satisfying (16), it is clearly enough to apply the above procedure to $(\mathbb{Z}^r, \mathbf{0}, S, \mathfrak{S})$.

$\mathfrak{p}$	$\mathcal{K}$	$\det(L_k)$ with $k \in \mathcal{K}$
$\mathfrak{p}_1$	$\{0, 1\}$	1, 6616761038619033600
$\mathfrak{p}_2$	$\{0, 1, 2, 3\}$	1, 2114272224838656, 344290964061164559443776151654 4, 560648087514898072191283054359385558374396825 6
$\mathfrak{p}_3$	$\{0, 1, 2, 3, 4, 5\}$	1, 1, 3800066789376, 1449610439062500000000000 0, 552982497811317443847656250000000000 0, 210946082233931520022451877593994140625000000000 00
$\mathfrak{p}_4$	$\{0, 1, 2, 3, 6\}$	1, 504631296, 21722722606780416, 935091979414469275815936, 543753526766035378167022205594996829560956679 33184
$\mathfrak{p}_5$	$\{0, 1, 5\}$	1, 57600, 106253245864567017308 1600

Table 3. This table gives the sets $\mathcal{K}$ and the determinants of the sublattices $L_k \subset \mathbb{Z}^{10}$ with $k \in \mathcal{K}$ as in Proposition 10.2. Observe that the sublattices L_k all have rank $r - 1 = 9$.

• Recall that $\delta_1, \ldots, \delta_r$ is a basis for the S-units (modulo torsion); in particular this allows us to identify the S-units (modulo torsion) with $\mathbb{Z}^r$. Let $\mathfrak{p} \in S$ and η be as in Proposition 10.2. Note that L_k is a subgroup of finite index in $\mathrm{Ker}(\eta)$. Now $\mathrm{Ker}(\eta)$ itself corresponds to the $(S \setminus \{\mathfrak{p}\})$-units, and therefore has rank $r - 1$. Therefore L_k has rank $r - 1$. That is, if we apply the procedure to $(\mathbb{Z}^r, \mathbf{0}, S, \mathfrak{S})$, then at depth $\#S + 1$ (when the set S has been entirely depleted), the lattice L_c will have rank $r - \#S$ which is the unit rank. Beyond this depth, the rank remains constant but the determinant of the lattice grows.

• The reader will note that we have not specified how to choose the next prime $\mathfrak{p} \in S$ or $q \in \mathfrak{S}$. In our implementation we order the primes in $\mathfrak{p} \in S$ by the size of their norms; from largest to smallest. The reason is that the primes $\mathfrak{p} \in S$ of large norm lead to lattices of large determinants and we therefore expect few short vectors. Once S is exhausted, the choices we make for the next $q \in \mathfrak{S}$ actually depend on the cumulative lattice L_c. We choose the prime $q \in \mathfrak{S}_c$ that minimizes $\#W_q/[L_c : L_c \cap L_q]$. Our justification for this is that we are replacing one coset of L_c with a union of cosets of $L_c \cap L_q$. The number of such cosets is bounded by $\#W_q$. The function $q \mapsto \#W_q/[L_c : L_c \cap L_q]$ estimates the "relative change in density" between the old lattice and the new union for that particular choice of q.

10.4. ***Example 1.4 continued.*** Recall that $\mathcal{B}'_f = 180$. Following the remark in Section 8, we find that $\mathcal{B}_f \approx 402.67$. Consider the information given by Proposition 10.2. Recall there are five possibilities for $\mathfrak{p} \in S$, ordered as $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$, in order of decreasing norm. Table 2 yields 2, 3, 5, 6, 9 for $\kappa_{\mathfrak{p}_j}$ with $j = 1, \ldots, 5$, respectively.

We take $\mathfrak{S}$ to be the set of rational primes $q < 200$ coprime to the prime ideals in S and such that every prime ideal factor of $q\mathcal{O}_K$ has norm $\leq 10^{10}$. This is done in order to keep our computations fast, as previously explained. However, of this set, our program only needs to use the primes 23 and 71, selected in that order using the heuristic detailed in the above remarks. For $q = 23$ and $q = 71$, Proposition 10.3

gives a lattice $L_q \subset \mathbb{Z}^{10}$ (now of rank 10) and a set W_q such that $\boldsymbol{b} \in W_q + L_q$. We find that

$$[\mathbb{Z}^{10} : L_{71}] = 3253933989048960000 \approx 3.26 \times 10^{18}, \quad \text{with } \#W_{71} = 71,$$

and

$$[\mathbb{Z}^{10} : L_{23}] = 41191874887680 \approx 4.12 \times 10^{13}, \quad \text{with } \#W_{23} = 23.$$

Observe that in Procedure 10.4 branching occurs at lines 14, 20. Thus we obtain "paths" through the algorithm depending on the choice of $k \in \mathcal{K}^*$ (line 14) or the choice of $\boldsymbol{w}_i \in W_q^*$ (line 20). A path "dies" if the criterion of line 1 is satisfied, or if $\mathcal{K}^*$ (defined in line 11) is empty, or if W_q^* (defined in line 20) is empty. Our program needs to check a total of 98 paths. Five of these terminate at line 1 with the condition $\lambda(L_c) > 2\mathcal{B}_f$ being satisfied, and the remaining 93 paths terminate at line 11 with $\mathcal{K}^* = \varnothing$. Of the 5 paths that terminate at line 1, three of these yield a vector $\boldsymbol{b} \in W_c + L_c$ satisfying $\|\boldsymbol{b}\|_2 \le \mathcal{B}_f$. These three vectors are

$$(-1,-1,-2,0,2,0,3,0,1,1), \quad (0,0,-1,1,1,1,1,1,0,0), \quad \text{and} \quad (-1,-1,-2,3,2,5,0,0,0,0).$$

These vectors respectively lead to the solutions

$$F(1,2) = 3^3 \cdot 7 \cdot 11, \quad F(1,-1) = 2 \cdot 3 \cdot 5, \quad F(1,1) = 2^5.$$

Acknowledgements

The authors are grateful to Mike Bennett, Rafael von Känel and Benjamin Matschke for stimulating discussions. The authors are indebted to the referee for many pertinent corrections and improvements.

References

[Agrawal et al. 1980] M. K. Agrawal, J. H. Coates, D. C. Hunt, and A. J. van der Poorten, "Elliptic curves of conductor 11", *Math. Comp.* **35**:151 (1980), 991–1002. MR Zbl

[Bennett and Dahmen 2013] M. A. Bennett and S. R. Dahmen, "Klein forms and the generalized superelliptic equation", *Ann. of Math.* (2) **177**:1 (2013), 171–239. MR Zbl

[Bennett and Siksek 2023a] M. A. Bennett and S. Siksek, "Differences between perfect powers: prime power gaps", *Algebra Number Theory* **17**:10 (2023), 1789–1846. MR Zbl

[Bennett and Siksek 2023b] M. A. Bennett and S. Siksek, "Differences between perfect powers: the Lebesgue–Nagell equation", *Trans. Amer. Math. Soc.* **376**:1 (2023), 335–370. MR Zbl

[Bennett et al. 2019] M. A. Bennett, A. Gherga, and A. Rechnitzer, "Computing elliptic curves over $\mathbb{Q}$", *Math. Comp.* **88**:317 (2019), 1341–1390. MR Zbl

[Bennett et al. 2020] M. A. Bennett, A. Gherga, and D. Kreso, "An old and new approach to Goormaghtigh's equation", *Trans. Amer. Math. Soc.* **373**:8 (2020), 5707–5745. MR

[Bennett et al. 2022] M. A. Bennett, A. Gherga, V. Patel, and S. Siksek, "Odd values of the Ramanujan tau function", *Math. Ann.* **382**:1-2 (2022), 203–238. MR

[Bombieri 1987] E. Bombieri, "On the Thue–Mahler equation", pp. 213–243 in *Diophantine approximation and transcendence theory* (Bonn, Germany, 1985), edited by G. Wüstholz, Lecture Notes in Math. **1290**, Springer, 1987. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Bruin and Stoll 2008] N. Bruin and M. Stoll, "Deciding existence of rational points on curves: an experiment", *Exp. Math.* **17**:2 (2008), 181–189. MR Zbl

[Bruin and Stoll 2010] N. Bruin and M. Stoll, "The Mordell–Weil sieve: proving non-existence of rational points on curves", *LMS J. Comput. Math.* **13** (2010), 272–306. MR Zbl

[Bugeaud and Győry 1996a] Y. Bugeaud and K. Győry, "Bounds for the solutions of Thue–Mahler equations and norm form equations", *Acta Arith.* **74**:3 (1996), 273–292. MR Zbl

[Bugeaud and Győry 1996b] Y. Bugeaud and K. Győry, "Bounds for the solutions of unit equations", *Acta Arith.* **74**:1 (1996), 67–80. MR

[Bugeaud et al. 2006] Y. Bugeaud, M. Mignotte, and S. Siksek, "Classical and modular approaches to exponential Diophantine equations, I: Fibonacci and Lucas perfect powers", *Ann. of Math.* (2) **163**:3 (2006), 969–1018. MR Zbl

[Bugeaud et al. 2008] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and S. Tengely, "Integral points on hyperelliptic curves", *Algebra Number Theory* **2**:8 (2008), 859–885. MR Zbl

[Cangül et al. 2010] İ. N. Cangül, M. Demirci, G. Soydan, and N. Tzanakis, "On the Diophantine equation $x^2 + 5^a \cdot 11^b = y^n$", *Funct. Approx. Comment. Math.* **43**:2 (2010), 209–225. MR Zbl

[Coates 1970] J. Coates, "An effective p-adic analogue of a theorem of Thue, II: The greatest prime factor of a binary form", *Acta Arith.* **16** (1970), 399–412. MR Zbl

[Cohen 2000] H. Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math. **193**, Springer, 2000. MR Zbl

[Evertse 1984] J.-H. Evertse, "On equations in S-units and the Thue–Mahler equation", *Invent. Math.* **75**:3 (1984), 561–584. MR Zbl

[Fincke and Pohst 1985] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis", *Math. Comp.* **44**:170 (1985), 463–471. MR Zbl

[Gallegos-Ruiz 2011] H. R. Gallegos-Ruiz, "S-integral points on hyperelliptic curves", *Int. J. Number Theory* **7**:3 (2011), 803–824. MR Zbl

[Hambrook 2011] K. D. Hambrook, *Implementation of a Thue–Mahler equation solver*, Ph.D. thesis, University of British Columbia, 2011, available at http://hdl.handle.net/2429/38244.

[von Känel and Matschke 2023] R. von Känel and B. Matschke, *Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via the Shimura–Taniyama conjecture*, Mem. Amer. Math. Soc. **1419**, Amer. Math. Soc., Providence, RI, 2023. MR Zbl

[Kim 2017] D. Kim, "A modular approach to cubic Thue–Mahler equations", *Math. Comp.* **86**:305 (2017), 1435–1471. MR Zbl

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

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

[Matveev 2000] E. M. Matveev, "An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II", *Izv. Ross. Akad. Nauk Ser. Mat.* **64**:6 (2000), 125–180. In Russian; translated in *Izv. Math.* **64**:6 (2000), 1217–1269. MR Zbl

[Pethő and de Weger 1998] A. Pethő and B. M. M. de Weger, "Appendix B: Two useful lemmata", pp. 229–230 in *The algorithmic resolution of Diophantine equations*, Lond. Math. Soc. Stud. Texts **41**, Cambridge Univ. Press, 1998. MR Zbl

[Soydan and Tzanakis 2016] G. Soydan and N. Tzanakis, "Complete solution of the Diophantine equation $x^2 + 5^a \cdot 11^b = y^n$", *Bull. Hellenic Math. Soc.* **60** (2016), 125–151. MR Zbl

[Thue 1909] A. Thue, "Über Annäherungswerte algebraischer Zahlen", *J. Reine Angew. Math.* **135** (1909), 284–305. MR Zbl

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

[Vinogradov and Sprindzhuk 1968] A. I. Vinogradov and V. G. Sprindzhuk, "The representation of numbers by binary forms", *Mat. Zametki* **3** (1968), 369–376. In Russian; translated in *Math. Notes* **3**:4 (1968), 235–239. MR Zbl

[Yu 2007] K. Yu, "p-adic logarithmic forms and group varieties, III", *Forum Math.* **19**:2 (2007), 187–280. MR Zbl

Communicated by Antoine Chambert-Loir
Received 2022-07-28 Revised 2024-04-09 Accepted 2024-06-15

adelagherga@gmail.com *Tutte Institute for Mathematics and Computing, Ottawa, Ontario, Canada*

s.siksek@warwick.ac.uk *Mathematics Institute, University of Warwick, Coventry, United Kingdom*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 19 No. 4 2025