COMPOSITIO MATHEMATICA

N. TZANAKIS
B. M. M. DE WEGER

How to explicitly solve a Thue-Mahler equation

Compositio Mathematica, tome 84, n° 3 (1992), p. 223-288
<http://www.numdam.org/item?id=CM_1992__84_3_223_0>

Compositio Mathematica **84**: 223–288, 1992.

How to explicitly solve a Thue-Mahler equation

N. TZANAKIS[1] and B. M. M. DE WEGER[2]

[1]*Department of Mathematics, University of Crete, Iraklion, Greece;*
[2]*Faculty of Applied Mathematics, University of Twente, Enschede, The Netherlands*

Received 19 November 1990; accepted 27 August 1991

Abstract. A general practical method for solving a Thue-Mahler equation is given. Using algebraic number theory and the theory of linear forms in logarithms of algebraic numbers in both the complex and p-adic case, an explicit upper bound for the solutions is derived. A practical method for a considerable reduction of this bound is presented, based on computational real and p-adic diophantine approximation techniques, in which the main tool is the LLL-algorithm. Special attention is paid to the problem, in general non-trivial, of finding the solutions below the reduced bound, using an algorithm of Fincke and Pohst for determining lattice points in a given sphere, and a sieving process. As an illustration of the usefulness of the method, the equation $x^3 - 23x^2y + 5xy^2 + 24y^3 = \pm 2^{z_1}3^{z_2}5^{z_3}7^{z_4}$ is completely solved.

1. Introduction

In this paper we develop a practical method for solving the general Thue-Mahler equation over $\mathbb{Z}$. This is the diophantine equation

$$F(X, Y) = c \cdot p_1^{z_1} \cdot \cdots \cdot p_v^{z_v}, \tag{1}$$

where

$$F(X, Y) = f_0X^n + f_1X^{n-1}Y + \cdots + f_{n-1}XY^{n-1} + f_nY^n$$

is a given irreducible binary form in $\mathbb{Z}[X, Y]$ of degree $n \geqslant 3$, the other parameters are the distinct rational primes $p_1, \ldots, p_v$ ($v \geqslant 1$) and the integer c (without loss of generality we assume that $(c, p_1 \cdot \cdots \cdot p_v) = 1$), and the unknowns are $(X, Y, z_1, \ldots, z_v) \in \mathbb{Z}^2 \times \mathbb{Z}_{\geqslant 0}^v$. Without loss of generality we may assume that

$$(X, Y) = (Y, f_0) = 1. \tag{2}$$

K. Mahler, in [Ma], was the first to prove that such an Equation (1) with condition (2) has at most finitely many solutions. Twenty four years earlier A. Thue had proved in [Th] that the equation $F(X, Y) = c$ (i.e. (1) with $v = 0$, the so-called Thue equation) has only finitely many solutions. This explains the name of Equation (1). The first proofs of these results were non-effective, and only after the work of A. Baker in the 1960's (the first generalizations to the p-

adic case, needed for the Thue-Mahler equation, are due to J. Coates), were effective proofs given. For the history of both equations we refer to Chapters 5 and 7 of T. N. Shorey's and R. Tijdeman's book [ST].

The present paper is a natural continuation of our 1989 paper [TW1], in which we develop a practical method for solving the general Thue equation. Compared to the Thue equation the study of the Thue-Mahler equation presents more difficulties, both from the theoretical and the computational point of view. It took us several years before we were able to develop our method in its present generality. The first general ideas (cf. [dW2]) were suggested by combining our ideas from the study of the general Thue equation with our ideas on p-adic diophantine approximation from a computational viewpoint (see [dW1, Chapters 3 (theory), 6, 7 (practice)]). Here we certainly were inspired by the 1980 paper [ACHP], which was until very recently the only paper in which a Thue-Mahler equation was solved by a similar method.

As a next step we tried to apply our general ideas to the solution of a specific Thue-Mahler equation, namely $X^3 - 3XY^2 - Y^3 = \pm 3^{z_1}17^{z_2}19^{z_3}$, see [TW2] and, for a brief exposition, [TW3]. In this specific example a very helpful fact is that the field associated with the cubic binary form is Galois; nevertheless the whole task proved far from trivial. Thus, in the last few years we have accumulated a certain experience on the various aspects of the practical solution of the Thue-Mahler equation. To this experience we ascribe our partially successful attempts to apply in practice the ideas that are presented in Chapter V of Sprindžuk's book [Sp]. The reader who compares Sprindžuk's approach (and also that of Shorey and Tijdeman [ST, Chapter 7]) to ours, will notice essential differences, mainly motivated by our urge to present a practical method, in which the algebraic number theoretical work should be minimized, both in quantity and complexity. Finally we felt that we had enough experience to share it with others, by presenting a practical way of 'how to solve a Thue-Mahler equation', which is the aim of the present paper. To convince the reader (and ourselves as well) that our method really works, we applied it to a specific example, on which we also report below.

As usual our method consists of three steps:

(1) A very large upper bound for the solutions is derived from the theory of (real/complex and p-adic) linear forms in logarithms. Here we use the best theorems available, due to Blass, Glass, Manski, Meronk and Steiner in the real/complex case, and Yu in the p-adic case. At this point, algebraic number theory makes its appearance, preparing our way towards the linear forms in logarithms of algebraic numbers.

(2) The upper bound can be considerably reduced in practice by diophantine approximation computations, based on applying the LLL-algorithm to the so-called approximation lattices related to the linear forms, both in the real/complex and p-adic case.

(3) The solutions below the reduced bound can be found by several methods (or a combination of them): more detailed computations with the approximation lattices, where the main tool is an algorithm of Fincke and Pohst for determining lattice points in a given sphere; a sieving process; and enumeration of possibilities. At this point we want to warn the reader not to underestimate this third step of finding all the solutions below a relatively small upper bound. It might well be the *computational* bottleneck of the entire method, especially when a more 'complicated' Thue-Mahler equation is studied (i.e. one with many primes and/or many fundamental units involved).

To help the reader understand better our method we have divided the paper into many numbered sections. Each Section N ($N \neq 13$) is followed by a Section N^{Ex}, typeset in a different style, in which we apply the general ideas of Section N to the specific equation we are solving.

1^{Ex} As an example we will study the Thue-Mahler equation

$$x^3 - 23x^2y + 5xy^2 + 24y^3 = \pm 2^{z_1}3^{z_2}5^{z_3}7^{z_4},$$

and solve it completely (a list of all the solutions is given in Section 18^{Ex}). Note that $f_0 = 1$, $c = 1$, $v = 4$, $n = 3$. This is a rather 'hazardous' Thue-Mahler equation, chosen by the mere facts that the field associated with the cubic form is not Galois, and that there are 'many' and 'large' solutions (there are 72 solutions, when we count only the (x, y) with $x \geqslant 0$). Note that by Evertse's famous result [Ev, Corollary 2] the best a priori information is that the number of solutions is less than 2×10^{251}.

2. The relevant algebraic number field

Let ξ be a root of $F(t, 1) = 0$, and put $K = \mathbb{Q}(\xi)$. The conjugates of ξ are denoted by $\xi^{(i)}$ $(i = 1, \ldots, n)$, and are ordered as follows:

$$\xi^{(1)}, \ldots, \xi^{(s)} \in \mathbb{R}, \quad \xi^{(s+1)} = \overline{\xi^{(s+t+1)}}, \ldots, \xi^{(s+t)} = \overline{\xi^{(s+2t)}} \in \mathbb{C} \setminus \mathbb{R},$$

with $s + 2t = n$. Now (1) is equivalent to

$$f_0 N_{K/\mathbb{Q}}(X - Y\xi) = c \cdot p_1^{z_1} \cdot \cdots \cdot p_v^{z_v}.$$

Put $x = f_0 X$, $y = Y$, $\theta = f_0 \xi$, so that (1) is equivalent to

$$N_{K/\mathbb{Q}}(x - y\theta) = f_0^{n-1} \cdot c \cdot p_1^{z_1} \cdot \cdots \cdot p_v^{z_v}. \tag{3}$$

Assumption (2) is equivalent to

$$(x, y) = 1. \tag{4}$$

Note that $K = \mathbb{Q}(\theta)$, $[K:\mathbb{Q}] = n$, and the minimal polynomial $g(t)$ of θ is monic, viz.

$$g(t) = t^n + f_1 t^{n-1} + f_2 f_0 t^{n-2} + \cdots + f_{n-1} f_0^{n-2} t + f_n f_0^{n-1},$$

thus θ is an algebraic integer. We need the following information:

- a basis of a convenient order $\mathcal{O}$ of K containing θ (not necessarily the maximal order = the ring of integers),
- a system of fundamental units in $\mathcal{O}$.

Note that we do not need the class number of K. For computing the above data efficient algorithms are known, cf. e.g. [Bi1], [Bi2], [Bu1], [Bu2], [Bu3], [Bu4], [Bu5], [DF], [PZ1], [PZ2], [PZ3], and even computer packages for such algebraic number theory computations are already in use, such as KANT (cf. [Sm]).

2^{Ex} Note that $x = X$, $y = Y$, $\theta = \xi$. The defining polynomial $g(t) = t^3 - 23t^2 + 5t + 24$ has $s = 3$ real roots, whence $t = 0$. The discriminant of g is $D_g = 1115525 = 5^2 \cdot 44621$ (44621 is prime). The field K is not Galois, since D_g is not a square; a basis of the ring of integers $\mathcal{O}_K$ is $\{1, \theta, \omega\}$ with $\omega = (2 + \theta - \theta^2)/5$ (apply [DF, Theorem II, §17]), so that the discriminant of K is $D_K = 44621$. A system of fundamental units of $\mathcal{O}_K$ is $\{\varepsilon_1, \varepsilon_2\}$ with $\varepsilon_1 = 1 + \theta - 6\omega$, $\varepsilon_2 = 3911 + 4397\theta + 1046\omega$. This system has been computed by the method of Berwick [Be], and was checked by R. J. Stroeker, who used the KANT package. The three conjugates of θ in $\mathbb{R}$ are

$$\theta^{(1)} = -0.9028831934\ldots, \quad \theta^{(2)} = 1.1692597799\ldots, \quad \theta^{(3)} = 22.7336234134\ldots$$

3. Decomposition of primes

Let p be any rational prime, and let

$$g(t) = g_1(t) \cdot \cdots \cdot g_m(t)$$

be the decomposition of $g(t)$ into irreducible polynomials $g_i(t) \in \mathbb{Q}_p[t]$. The prime ideals in K dividing p are in one-to-one correspondence with $g_1(t), \ldots, g_m(t)$ (cf. [BS, Theorem 3, Section 2, Chapter 4]). More precisely, we have in K the following decomposition of (p):

$$(p) = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_m^{e_m},$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ distinct prime ideals, and $e_1, \ldots, e_m \in \mathbb{N}$ (the ramification indices). For $i = 1, \ldots, m$ the residual degree of $\mathfrak{p}_i$ is the positive integer d_i for which $N\mathfrak{p}_i = p^{d_i}$, and then $e_i d_i = \deg g_i(t)$.

For $p = p_1, \ldots, p_v$ one has to compute the above mentioned decompositions. Algorithms to do so efficiently are known, cf. [PZ3].

3^{Ex} For $p = 2$ we have $m = 2$, $(2) = \mathfrak{p}_{21}\mathfrak{p}_{22}$, $e_1 = e_2 = d_1 = 1$, $d_2 = 2$. We have computed

$$\mathfrak{p}_{21} = (\pi_{21}), \quad \pi_{21} = 22 + 25\theta + 6\omega, \quad N(\pi_{21}) = 2,$$
$$\mathfrak{p}_{22} = (\pi_{22}), \quad \pi_{22} = -5 + 4\theta + \omega, \quad N(\pi_{22}) = 4.$$

For $p = 3$ we have $m = 2$, $(3) = \mathfrak{p}_{31}\mathfrak{p}_{32}$, $e_1 = e_2 = d_1 = 1$, $d_2 = 2$, and we have computed

$$\mathfrak{p}_{31} = (\pi_{31}), \quad \pi_{31} = 31 - 41\theta + 47\omega, \quad N(\pi_{31}) = -3,$$
$$\mathfrak{p}_{32} = (\pi_{32}), \quad \pi_{32} = 161923 + 182069\theta + 43702\omega, \quad N(\pi_{32}) = -9.$$

For $p = 5$ we have $m = 3$, $(5) = \mathfrak{p}_{51}\mathfrak{p}_{52}\mathfrak{p}_{53}$, $e_1 = e_2 = e_3 = d_1 = d_2 = d_3 = 1$, and we have found

$$\mathfrak{p}_{51} = (\pi_{51}), \quad \pi_{51} = 133 + 150\theta + 36\omega, \quad N(\pi_{51}) = -5,$$
$$\mathfrak{p}_{52} = (\pi_{52}), \quad \pi_{52} = 89 + 100\theta + 24\omega, \quad N(\pi_{52}) = 5,$$
$$\mathfrak{p}_{53} = (\pi_{53}), \quad \pi_{53} = 111 - 90\theta - 16\omega, \quad N(\pi_{53}) = 5.$$

For $p = 7$ we have $m = 2$, $(7) = \mathfrak{p}_{71}\mathfrak{p}_{72}$, $e_1 = e_2 = d_1 = 1$, $d_2 = 2$, and we have computed

$$\mathfrak{p}_{71} = (\pi_{71}), \quad \pi_{71} = 1 - \theta, \quad N(\pi_{71}) = 7,$$
$$\mathfrak{p}_{72} = (\pi_{72}), \quad \pi_{72} = 15 + 21\theta + 5\omega, \quad N(\pi_{72}) = -49.$$

Moreover, for $p = 2, 3, 7$ we have

$$g_1(t) = t - \theta, \quad g_2(t) = t^2 - (\theta - 23)t + (\theta^2 - 23\theta + 5).$$

4. *p*-adic valuations

In this section we give a concise exposition of p-adic valuations. By $\bar{\mathbb{Q}}_p$ we denote the algebraic closure of $\mathbb{Q}_p$, and by $\mathbb{C}_p$ the completion, with respect to the p-adic absolute value, of $\bar{\mathbb{Q}}_p$. As general references we give the books of Koblitz [Ko] and Narkiewicz [Na1] (especially Chapters I, IV and V). Let p be any rational prime, and let $x \in K$. Let $\mathfrak{p}_i$ be a prime ideal dividing p, and let d_i, e_i, $g_i(t)$ be defined as in Section 3. Now, $\operatorname{ord}_{\mathfrak{p}_i}(x)$ is defined as the exponent (a positive or negative integer, or 0) of $\mathfrak{p}_i$ in the decomposition of the principal (fractional) ideal (x). Since factorization into prime ideals does not depend on the choice of conjugates, this definition of $\operatorname{ord}_{\mathfrak{p}_i}(x)$ is independent of the choice of conjugates.

Let $i \in \{1, \ldots, m\}$. Put $K_{\mathfrak{p}_i} = \mathbb{Q}_p(\theta_i)$, where θ_i satisfies $g_i(\theta_i) = 0$. There are m embeddings (one for every i) defined by

$$\tau_i : K \hookrightarrow K_{\mathfrak{p}_i},$$
$$\alpha \to \alpha \quad \text{if } \alpha \in \mathbb{Q},$$
$$\theta \to \theta_i.$$

Now, let $\theta_i^{(1)}, \ldots, \theta_i^{(n_i)} \in \bar{\mathbb{Q}}_p$ be the conjugates of θ_i, where $n_i = \deg g_i(t)$. Then

there are n_i embeddings given by

$$\begin{aligned}\sigma_{ij}&: K_{\mathfrak{p}_i} \hookrightarrow \mathbb{C}_p,\\ &\alpha \to \alpha \quad \text{if } \alpha \in \mathbb{Q}_p,\\ &\theta_i \to \theta_i^{(j)}.\end{aligned}$$

Here, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n_i\}$. Note that, if $\theta^{(1)}, \ldots, \theta^{(n)}$ denote the roots of $g(t)$ in $\bar{\mathbb{Q}}_p$, then every $\theta_i^{(j)}$ coincides with some $\theta^{(k)}$. Since $n_1 + \cdots + n_m = n$, there are n embeddings given by

$$\begin{aligned}\sigma_{ij} \circ \tau_i&: K \hookrightarrow \mathbb{C}_p,\\ &\alpha \to \alpha \quad \text{if } \alpha \in \mathbb{Q},\\ &\theta \to \theta_i^{(j)}.\end{aligned}$$

If K is considered as embedded in $K_{\mathfrak{p}_i}$ (by means of τ_i), then the p-adic order of $x \in K$ is defined by

$$\operatorname{ord}_p(x) = \frac{1}{e_i} \operatorname{ord}_{\mathfrak{p}_i}(x).$$

Thus, m different p-adic orders can be defined in K, and which one we choose in a particular instance depends on how we view K, i.e. of which field $K_{\mathfrak{p}_i}$ we consider K to be a subfield. Given the p-adic order in K, we can define the p-adic absolute value in K by

$$|x|_p = p^{-\operatorname{ord}_p(x)}.$$

Now $K_{\mathfrak{p}_i} = \mathbb{Q}_p(\theta_i)$ is the completion of K with respect to $|\cdot|_p$. We also have

$$|x|_p = |N_{K_{\mathfrak{p}_i}/\mathbb{Q}_p}(x)|^{1/n_i}.$$

Here, as before, $n_i = \deg g_i(t) = [K_{\mathfrak{p}_i} : \mathbb{Q}_p]$. In fact, we can extend the p-adic absolute value to any finite extension L of $\mathbb{Q}_p$ by

$$|x|_p = |N_{L/\mathbb{Q}_p}(x)|^{1/[L:\mathbb{Q}_p]},$$

and, analogously,

$$\operatorname{ord}_p(x) = \frac{1}{[L:\mathbb{Q}_p]} \operatorname{ord}_p(N_{L/\mathbb{Q}_p}(x))$$

(note that these definitions are independent of the extension L containing x), so that $|x|_p = p^{-\mathrm{ord}_p(x)}$. Now we are in a position to define the p-adic order and absolute value of any $x \in \bar{\mathbb{Q}}_p$. Indeed, just consider any extension L of $\mathbb{Q}_p$ containing x, and apply the latter two formulas. Note that for $x, y \in \bar{\mathbb{Q}}_p$ it is still valid that $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$ and $\mathrm{ord}_p(x+y) \geqslant \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$. Note also that if K is embedded in $K_{\mathfrak{p}_i}$ then the $\mathrm{ord}_p(x)$ previously defined coincides with the p-adic order $\mathrm{ord}_p(\sigma_{ij} \circ \tau_i(x))$ of the p-adic number $\sigma_{ij} \circ \tau_i(x)$ (for any $j \in \{1, \ldots, n_i\}$).

Of course, in the special case $x \in \mathbb{Q}_p$ we can write

$$x = \sum_{j=\mu}^{\infty} c_j p^j, \quad 0 \leqslant c_j \leqslant p-1 \quad (j \geqslant \mu),$$

with $c_\mu \neq 0$ if $x \neq 0$, and then $\mathrm{ord}_p(x) = \mu$, $|x|_p = p^{-\mu}$. We adopt the following notation for $x \in \mathbb{Q}_p$:

$$x = c_\mu c_{\mu+1} \cdots c_{-1}.c_0 c_1 \cdots \quad \text{if } \mu < 0,$$

$$x = \qquad\qquad 0.c_0 c_1 \cdots \quad \text{if } \mu \geqslant 0,$$

where we take $c_i = 0$ for all $i < \mu$.

Finally we note that, having already defined the p-adic absolute value and p-adic order of any $x \in \bar{\mathbb{Q}}_p$, we can define the p-adic absolute value and p-adic order of any $x \in \mathbb{C}_p$ as follows. We consider any sequence (x_n) of elements of $\bar{\mathbb{Q}}_p$ converging to x; then we define $|x|_p = \lim_{n \to \infty} |x_n|_p$, and $\mathrm{ord}_p(x)$ by means of $|x|_p = p^{-\mathrm{ord}_p(x)}$.

4^{Ex} For $p = 5$ the situation is easy: in Section 3^{Ex} we have seen that $g(t)$ has three roots in $\mathbb{Q}_5$, which we denote by $\theta^{(1)}, \theta^{(2)}, \theta^{(3)}$. In this case $m = 3$, and for every $i = 1, 2, 3$ we have $g_i(t) = t - \theta^{(i)}$ so that (in the notation of Section 4) $\theta_i = \theta^{(i)}$, $K_{\mathfrak{p}_{5i}} = \mathbb{Q}_5(\theta^{(i)}) = \mathbb{Q}_5$, $\tau_i(\theta) = \theta^{(i)}$, and the three embeddings $K \hookrightarrow \mathbb{Q}_5$ are σ_{i1} with $\sigma_{i1}(\theta) = \theta^{(i)}$ for $i = 1, 2, 3$. We have the Table

$p = 5$	(1)	(2)	(3)
θ	0.4320132113...	0.2212320101...	0.2312041230...
π_{51}	0.0331023331...	0.2133034404...	0.4402441104...
π_{52}	0.2042343042...	0.0122021301...	0.3121134001...
π_{53}	0.4113312002...	0.2224044144...	0.0240042203...

Note that $\mathrm{ord}_5(\pi_{5i}^{(j)}) = 1$ if $i = j$ and 0 otherwise.

For $p = 2, 3, 7$ the situation is somewhat more complicated. According to Section 3^{Ex}, $m = 2$, and if we denote by $\theta^{(1)}$ the root of $g_1(t)$ and by $\theta^{(2)}, \theta^{(3)}$ the roots of $g_2(t)$, then $\theta_1 = \theta^{(1)} \in \mathbb{Q}_p$, $K_{\mathfrak{p}_{p1}} = \mathbb{Q}_p(\theta_1) = \mathbb{Q}_p$, $\tau_1(\theta) = \theta_1 = \theta^{(1)}$. Further θ_2 satisfies $g_2(\theta_2) = 0$, $K_{\mathfrak{p}_{p2}} = \mathbb{Q}_p(\theta_2)$ (a quadratic extension of $\mathbb{Q}_p$), $\tau_2(\theta) = \theta_2$. Then the three embeddings $K \hookrightarrow \mathbb{C}_p$ are $\sigma_{11} \circ \tau_1$ which maps θ to $\theta^{(1)}$, and $\sigma_{2j} \circ \tau_2$ which map θ to $\theta^{(j+1)}$ for $j = 1, 2$. We have the following Tables:

$p=2$	(1), $K_{\mathfrak{p}_{21}}=\mathbb{Q}_2$	(2), (3), $[K_{\mathfrak{p}_{22}}:\mathbb{Q}_2]=2$	ord_2
θ	0.0001000110...	roots of $t^2+0.10001...t+0.10110...$	0
π_{21}	0.0101011111...	roots of $t^2+0.10101...t+0.10111...$	0
π_{22}	0.1011101001...	roots of $t^2+0.01001...t+0.00101...$	1

$p=3$	(1), $K_{\mathfrak{p}_{31}}=\mathbb{Q}_3$	(2), (3), $[K_{\mathfrak{p}_{32}}:\mathbb{Q}_3]=2$	ord_3
θ	0.0210020022...	roots of $t^2+0.10222...t+0.20211...$	0
π_{31}	0.0212211000...	roots of $t^2+0.22101...t+0.12022...$	0
π_{32}	0.2020002122...	roots of $t^2+0.02112...t+0.00110...$	1

$p=7$	(1), $K_{\mathfrak{p}_{71}}=\mathbb{Q}_7$	(2), (3), $[K_{\mathfrak{p}_{72}}:\mathbb{Q}_7]=2$	ord_7
θ	0.1544035230...	roots of $t^2+0.61440...t+0.44216...$	0
π_{71}	0.0222631436...	roots of $t^2+0.64226...t+0.46656...$	0
π_{72}	0.3001001201...	roots of $t^2+0.02600...t+0.00222...$	1

Note that for $p=2, 3, 7$ always $\mathrm{ord}_{\mathfrak{p}_{p2}}(\pi_{p2})=1$, $e_2=1$, hence $\mathrm{ord}_p(\pi_{p2}^{(j)})=1$ for $j=2, 3$. The same conclusion could have been drawn as follows: $N_{K_{\mathfrak{p}_{p2}}/\mathbb{Q}_p}(\pi_{p2}^{(j)})=0.00*...$ (where $*$ is nonzero), so $\mathrm{ord}_p(\pi_{p2}^{(j)})=(1/[K_{\mathfrak{p}_{p2}}:\mathbb{Q}_p])\,\mathrm{ord}_p(N_{K_{\mathfrak{p}_{p2}}/\mathbb{Q}_p}(\pi_{p2}^{(j)}))=\frac{1}{2}\cdot 2=1$.

5. Removal of prime ideals

After the general remarks of Sections 3 and 4 we now return to our Thue-Mahler equation (3). We assume that $(x, y, z_1, \ldots, z_v)\in\mathbb{Z}^2\times\mathbb{Z}_{\geqslant 0}^v$ is a solution of (3) satisfying (4). The decomposition of $(x-y\theta)$ into prime ideals may contain (apart from a bounded contribution from $f_0^{n-1}c$) any prime ideal dividing one of the p_i. The following lemma shows that in fact for each p_i, at most one prime ideal dividing it may have a nontrivial contribution to $(x-y\theta)$. Thus the number of prime ideals to be considered is at most v. Therefore we may call the next lemma 'The Prime Ideal Removing Lemma', and it is an ideal prime removing lemma indeed.

Let p be any prime, and let $\mathfrak{p}_i$, d_i, e_i, $g_i(t)$ have the same meaning as above. Again we denote by $\theta_i^{(j)}$ the roots of $g_i(t)$, for $i=1,\ldots,m$ and $j=1,\ldots,n_i=\deg g_i(t)$. Further, let $e=\max\{e_1,\ldots,e_m\}$, and let D_θ be the discriminant of θ.

LEMMA 1 (The Prime Ideal Removing Lemma).

(i) *For every pair $i, j\in\{1,\ldots,m\}$ with $i\neq j$ there is at most one $\mathfrak{p}\in\{\mathfrak{p}_i,\mathfrak{p}_j\}$ satisfying*

$$\mathrm{ord}_{\mathfrak{p}}(x-y\theta)>\max\{e_i,e_j\}\cdot\mathrm{ord}_p(\theta_i^{(k)}-\theta_j^{(l)}). \tag{5}$$

Here $k \in \{1, \ldots, n_i\}$ *and* $l \in \{1, \ldots, n_j\}$ *are arbitrary.*

(ii) *If* (5) *is satisfied for* $\mathfrak{p} = \mathfrak{p}_i$ *and* $\mathfrak{p}_i$ has $d_i > 1$ *or* $e_i > 1$ *then*

$$\operatorname{ord}_{\mathfrak{p}_i}(x - y\theta) \leqslant e_i \cdot \operatorname{ord}_p(\theta_i^{(k)} - \theta_i^{(l)}). \tag{6}$$

Here $k, l \in \{1, \ldots, n_i\}$ *with* $k \neq l$ *arbitrary.*

FIRST COROLLARY OF LEMMA 1

(i) *There is at most one* $\mathfrak{p}_i$ *dividing* p *with*

$$\operatorname{ord}_{\mathfrak{p}_i}(x - y\theta) > \max_{1 \leqslant j < k \leqslant m} (\max\{e_j, e_k\} \cdot \operatorname{ord}_p(\theta_j^{(h)} - \theta_k^{(l)})). \tag{7}$$

Here $h \in \{1, \ldots, n_j\}$ *and* $l \in \{1, \ldots, n_k\}$ *are arbitrary.*

(ii) *If* $\mathfrak{p}_i$ *satisfies* (7) *and has* $d_i > 1$ *or* $e_i > 1$ *then it satisfies* (6).

SECOND COROLLARY OF LEMMA 1. *There is at most one* $\mathfrak{p}_i$ *dividing* p *with*

$$\operatorname{ord}_{\mathfrak{p}_i}(x - y\theta) > \tfrac{1}{2}e \cdot \operatorname{ord}_p(D_\theta), \tag{8}$$

and it satisfies $d_i = e_i = 1$.

THIRD COROLLARY OF LEMMA 1. *If* $p \nmid D_\theta$ *then there is at most one* $\mathfrak{p}_i$ *dividing* p *with*

$$\operatorname{ord}_{\mathfrak{p}_i}(x - y\theta) > 0,$$

and, if so, it must have $e_i = d_i = 1$.

Proof of Lemma 1. (i) It suffices to prove that if

$$(x - y\theta) = \mathfrak{p}_i^{\nu_i} \mathfrak{p}_j^{\nu_j} \mathfrak{a},$$

where $\mathfrak{a}$ is some integral ideal, then

$$\nu_0 = \min\{\nu_i, \nu_j\} \leqslant \max\{e_i, e_j\} \cdot \operatorname{ord}_p(\theta_i^{(k)} - \theta_j^{(l)}).$$

In view of the discussion of Section 4 we have:

$$\operatorname{ord}_p(x - y\theta_i^{(k)}) = \operatorname{ord}_p(\sigma_{ik} \circ \tau_i(x - y\theta)) = \frac{1}{e_i} \operatorname{ord}_{\mathfrak{p}_i}(x - y\theta) \geqslant \frac{\nu_i}{e_i} \geqslant \frac{\nu_0}{\max\{e_i, e_j\}},$$

and analogously

$$\mathrm{ord}_p(x - y\theta_j^{(l)}) \geqslant \frac{v_0}{\max\{e_i, e_j\}}.$$

Since ord_p is well defined on $\mathbb{C}_p$, and $x - y\theta_i^{(k)}$ and $x - y\theta_j^{(l)}$ are elements of $\mathbb{C}_p$, we obtain

$$\mathrm{ord}_p(y(\theta_i^{(k)} - \theta_j^{(l)})) \geqslant \min\{\mathrm{ord}_p(x - y\theta_i^{(k)}), \mathrm{ord}_p(x - y\theta_j^{(l)})\} \geqslant \frac{v_0}{\max\{e_i, e_j\}}.$$

The result now follows if $\mathrm{ord}_p(y) = 0$. But if $p \mid y$ then, by (4), $p \nmid x$, hence $\mathrm{ord}_{\mathfrak{p}}(x - y\theta) = 0$ for any $\mathfrak{p}$ dividing p, and it follows that $v_0 = 0$, which implies the result.

(ii) Since $n_i = \deg g_i(t) = e_i d_i > 1$, there are $k, l \in \{1, \ldots, n_i\}$ with $k \neq l$. We write

$$(x - y\theta) = \mathfrak{p}_i^v \mathfrak{a}, \quad v = \mathrm{ord}_{\mathfrak{p}_i}(x - y\theta)$$

for some integral ideal $\mathfrak{a}$, and we obtain

$$\mathrm{ord}_p(x - y\theta_i^{(k)}) = \mathrm{ord}_p(\sigma_{ik} \circ \tau_i(x - y\theta)) = \frac{1}{e_i} \mathrm{ord}_{\mathfrak{p}_i}(x - y\theta) = \frac{v}{e_i},$$

and analogously

$$\mathrm{ord}_p(x - y\theta_i^{(l)}) = \frac{v}{e_i}.$$

As in the proof of (i) we obtain the result. □

Proof of first corollary of Lemma 1. Trivial. □

Proof of second corollary of Lemma 1. We have

$$D_\theta = \prod_{1 \leqslant h < l \leqslant n} (\theta^{(h)} - \theta^{(l)})^2,$$

and since θ is an algebraic integer, we have

$$\mathrm{ord}_p(D_\theta) \geqslant 2 \cdot \mathrm{ord}_p(\theta^{(h)} - \theta^{(l)})$$

for all $h, l \in \{1, \ldots, n\}$ with $h \neq l$. On the other hand, if $j, k \in \{1, \ldots, m\}$ with $j \neq k$, and $\theta_j^{(\cdot)}$, $\theta_k^{(\cdot)}$ are arbitrary conjugates of θ_j, θ_k respectively, then $\theta_j^{(\cdot)} = \theta^{(h)}$ and $\theta_k^{(\cdot)} = \theta^{(l)}$ for some $h, l \in \{1, \ldots, n\}$ with $h \neq l$. Then $\mathrm{ord}_p(D_\theta) \geqslant 2 \cdot \mathrm{ord}_p(\theta_j^{(\cdot)} - \theta_k^{(\cdot)})$; hence (8) implies (7), and the 1st Corollary (ii) can be applied to prove that at

most one $\mathfrak{p}_i$ dividing p satisfies (8). Also, (8) implies (5) (because it implies (7)), as well as the negation of (6), so that, by Lemma 1(ii), we must have $d_i = e_i = 1$. □

Proof of third corollary of Lemma 1. Obvious from the 2nd Corollary. □

5^{Ex} For $p = 2, 3, 7$ we apply the 3rd Corollary of Lemma 1. It follows that $\mathfrak{p}_{22}, \mathfrak{p}_{32}, \mathfrak{p}_{72}$ will not divide $(x - y\theta)$, whereas $\mathfrak{p}_{21}, \mathfrak{p}_{31}, \mathfrak{p}_{71}$ may divide $(x - y\theta)$ to some power.

For $p = 5$ we can apply the 2nd Corollary of Lemma 1 with $e = 1$, $\operatorname{ord}_5(D_\theta) = 2$. It follows that at most one of $\mathfrak{p}_{51}, \mathfrak{p}_{52}, \mathfrak{p}_{53}$ can divide $(x - y\theta)$ to the power at least 2, and it may be any of the three. But now Lemma 1(i) itself gives more information. Note that $e_1 = e_2 = e_3 = 1$, and

$$\operatorname{ord}_5(\theta_1 - \theta_2) = \operatorname{ord}_5(\theta_1 - \theta_3) = 0, \operatorname{ord}_5(\theta_2 - \theta_3) = 1.$$

Hence, if $\mathfrak{p}_{51}$ divides $(x - y\theta)$, then $\mathfrak{p}_{52}$ and $\mathfrak{p}_{53}$ don't. If $\mathfrak{p}_{52}$ or $\mathfrak{p}_{53}$ divides $(x - y\theta)$, then $\mathfrak{p}_{51}$ doesn't. If $\mathfrak{p}_{52}$ divides $(x - y\theta)$ to the power at least 2, then $\mathfrak{p}_{53}$ divides $(x - y\theta)$ to the power at most 1, and if $\mathfrak{p}_{53}$ divides $(x - y\theta)$ to the power at least 2, then $\mathfrak{p}_{52}$ divides $(x - y\theta)$ to the power at most 1. Thus $(x - y\theta)$ has one of the following five forms:

$$\mathfrak{p}_{21}^{n_1}\mathfrak{p}_{31}^{n_2}\mathfrak{p}_{51}^{n_3}\mathfrak{p}_{71}^{n_4},\ \mathfrak{p}_{21}^{n_1}\mathfrak{p}_{31}^{n_2}\mathfrak{p}_{52}^{n_3}\mathfrak{p}_{71}^{n_4},\ \mathfrak{p}_{21}^{n_1}\mathfrak{p}_{31}^{n_2}\mathfrak{p}_{52}^{n_3}\mathfrak{p}_{53}\mathfrak{p}_{71}^{n_4},\ \mathfrak{p}_{21}^{n_1}\mathfrak{p}_{31}^{n_2}\mathfrak{p}_{53}^{n_3}\mathfrak{p}_{71}^{n_4},\ \mathfrak{p}_{21}^{n_1}\mathfrak{p}_{31}^{n_2}\mathfrak{p}_{52}\mathfrak{p}_{53}^{n_3}\mathfrak{p}_{71}^{n_4}$$

for nonnegative integers n_1, n_2, n_3, n_4.

6. Factorization of the Thue-Mahler equation

For every $i \in \{1, \ldots, v\}$ let

$$\mathscr{P}_i = \{\mathfrak{p} \mid \mathfrak{p} \text{ prime ideal dividing } p_i \text{ with } d_i = e_i = 1\}.$$

Thus $\mathscr{P}_i$ is finite, and it may even be empty. In view of the Prime Ideal Removing Lemma, (3) implies a finite number of ideal equations of the form

$$(x - y\theta) = \mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{p}_1^{u_1} \cdot \cdots \cdot \mathfrak{p}_v^{u_v}. \tag{9}$$

Here,

- $\mathfrak{a}$ is an integral ideal with $N\mathfrak{a} = f_0^{n-1}c$,
- $(\mathfrak{p}_1, \ldots, \mathfrak{p}_v) \in \mathscr{P}_1 \times \cdots \times \mathscr{P}_v$, where $\mathfrak{p}_i^{u_i}$ stands for the unit ideal if $\mathscr{P}_i = \varnothing$,
- the prime ideal factors of $\mathfrak{b}$ are those that divide one of the p_i but are not equal to one of $\mathfrak{p}_1, \ldots, \mathfrak{p}_v$,
- $u_i + \operatorname{ord}_{p_i}(N\mathfrak{b}) = z_i$ for $i = 1, \ldots, v$.

For convenience we assume (without loss of generality) that none of the $\mathscr{P}_i$ is empty.

For any $i = 1, \ldots, v$ let h_i be a positive integer such that $\mathfrak{p}_i^{h_i}$ is a principal ideal. The smallest such h_i is a divisor of the class number h of K. In practice it will be

useful to take h_i minimal, to reduce the number of cases to be considered in the sequel, but this is not essential. For $i = 1, \ldots, v$ the nonnegative integers n_i, s_i are defined by

$$u_i = h_i n_i + s_i, \quad 0 \leqslant s_i < h_i,$$

and we put

$$\mathfrak{p}_i^{h_i} = (\pi_i)\ (\pi_i \in K), \quad t_i = \mathrm{ord}_{\mathfrak{p}_i}(N\mathfrak{b}).$$

Then

$$z_i = n_i h_i + s_i + t_i, \tag{10}$$

and (9) is equivalent to

$$x - y\theta = \alpha \cdot \varepsilon_1^{a_1} \cdot \ldots \cdot \varepsilon_r^{a_r} \cdot \pi_1^{n_1} \cdot \ldots \cdot \pi_v^{n_v}, \tag{11}$$

where

$$(\alpha) = \mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{p}_1^{s_1} \cdot \ldots \cdot \mathfrak{p}_v^{s_v}$$

(note that this is a principal ideal indeed), and $\{\varepsilon_1, \ldots, \varepsilon_r\}$ is a set of fundamental units in some order $\mathcal{O}$ of K containing θ. Here, $r = s + t - 1$, and one usually takes $\mathcal{O}$ to be the maximal order, i.e. the ring of integers $\mathcal{O}_K$ of K, but again this is not essential. Note that the finite number of equations (9) leads to a finite number of equations (11). Each of these cases has to be treated separately in the sequel. In practice, one has to compute all the possibilities for α (which is determined up to a unit), and, as remarked before, one has to know the set of fundamental units in $\mathcal{O}$, and the nontrivial roots of unity, if any (such roots exist only if $s = 0$). One also has to know the h_i, and in achieving that, a knowledge of h is not required, although it might be useful.

6^{Ex} As remarked in Section 5^{Ex}, we have five equations (9). Since we can take all h_i equal to 1 (in fact, we believe that $h = 1$, but we didn't check), all the s_i are 0, and for equation (11) we also have five possibilities. Note that $\mathfrak{a} = (1)$, $\mathfrak{p}_p = \mathfrak{p}_{p1}$ and $\pi_p = \pi_{p1}$ for $p = 2, 3, 7$, and the 5 cases are:

Case	$\mathfrak{b}$	$\mathfrak{p}_5$	α	π_5
I	(1)	$\mathfrak{p}_{51}$	1	π_{51}
II	(1)	$\mathfrak{p}_{52}$	1	π_{52}
III	$\mathfrak{p}_{53}$	$\mathfrak{p}_{52}$	π_{53}	π_{52}
IV	(1)	$\mathfrak{p}_{53}$	1	π_{53}
V	$\mathfrak{p}_{52}$	$\mathfrak{p}_{53}$	π_{52}	π_{53}

Note that $t_1 = t_2 = t_4 = 0$ in all cases, whereas $t_3 = \begin{cases} 0 & \text{in Cases I, II, IV} \\ 1 & \text{in Cases III, V} \end{cases}$.

7. The S-unit equation

Let $p \in \{p_1, \ldots, p_v, \infty\}$, and denote the roots of $g(t)$ in $\mathbb{C}_p$ (where $\mathbb{C}_\infty = \mathbb{C}$) by $\theta^{(1)}, \ldots, \theta^{(n)}$. Let $i_0, j, k \in \{1, \ldots, n\}$ be distinct, and apply the three isomorphic embeddings of K into $\mathbb{C}_p$ given by $\theta \to \theta^{(i_0)}, \theta^{(j)}, \theta^{(k)}$ to

$$\beta = x - y\theta.$$

From the three conjugate equations thus obtained we eliminate x and y, which is possible just because $F(X, Y)$ was supposed to be irreducible and of degree $\geqslant 3$ (cf. Section 2). Then we obtain

$$\lambda = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \frac{\beta^{(k)}}{\beta^{(j)}} - 1 = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \frac{\beta^{(i_0)}}{\beta^{(j)}}.$$

Now we apply (11), and thus we find the so-called 'S-unit equation'

$$\lambda = \delta_1 \prod_{i=1}^{v} \left(\frac{\pi_i^{(k)}}{\pi_i^{(j)}}\right)^{n_i} \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} - 1 = \delta_2 \prod_{i=1}^{v} \left(\frac{\pi_i^{(i_0)}}{\pi_i^{(j)}}\right)^{n_i} \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i}, \tag{12}$$

where

$$\delta_1 = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}}{\alpha^{(j)}}, \quad \delta_2 = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}}{\alpha^{(j)}}$$

are constants. We will now study for each p (for the time being, $p \neq \infty$) the p-adic absolute value of λ for suitably chosen indices i_0, j, k.

LEMMA 2. *If $\gamma \in K$ is an algebraic integer with $N_{K/\mathbb{Q}}(\gamma) \not\equiv 0 \pmod{p}$, then $\gamma^{(l)} \in \mathbb{C}_p$ is a p-adic unit for every $l \in \{1, \ldots, n\}$.*

Proof of Lemma 2. This is an easy exercise, that we leave to the reader. □

Let $l \in \{1, \ldots, v\}$. We consider the prime $p = p_l$.

COROLLARY OF LEMMA 2

(i) *Let $i \in \{1, \ldots, r\}$. Then $\dfrac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}$ and $\dfrac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}$ are p_l-adic units.*

(ii) *Let $i \in \{1, \ldots, v\}$ with $i \neq l$. Then $\dfrac{\pi_i^{(i_0)}}{\pi_i^{(j)}}$ and $\dfrac{\pi_i^{(k)}}{\pi_i^{(j)}}$ are p_l-adic units.*

Proof of the corollary. Obvious from Lemma 2. □

We now show how to choose i_0. We may assume that $g_1(t)$ is the irreducible factor of $g(t)$ over $\mathbb{Q}_{p_l}$ that corresponds to the prime ideal $\mathfrak{p}_l \in \mathscr{P}_l$ that appears in (9). Since $\mathfrak{p}_l \in \mathscr{P}_l$, we have $\deg g_1(t) = 1$. We denote by $\theta^{(i_0)}$ the root of $g_1(t)$. In this way a direct connection between l and i_0 is established. The other two indices j, k appearing in (12) are fixed, but arbitrary. Note that it is always possible, and it is

advisable, to take j, k as follows:

- If there are at least three $g_i(t)$ with $\deg g_i(t) = 1$, then $\theta^{(j)}$ and $\theta^{(k)}$ should be roots of such linear polynomials. Then j, k can be taken so that $\mathrm{ord}_{p_l}(\delta_1) \geqslant 0$.
- If there are at most two linear $g_i(t)$, then there is a $g_i(t)$ with $\deg g_i(t) \geqslant 2$, and $\theta^{(j)}$ and $\theta^{(k)}$ should be roots of the same such $g_i(t)$. Then

$$\mathrm{ord}_{p_l}(\delta_1) = \mathrm{ord}_{p_l}\left(\frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}}\right) + \mathrm{ord}_{p_l}\left(\frac{\alpha^{(k)}}{\alpha^{(j)}}\right) = 0 + 0 = 0.$$

  Moreover, if there is a $g_i(t)$ with $\deg g_i(t) = 2$, then it is advisable to choose $\theta^{(j)}$ and $\theta^{(k)}$ to be roots of that quadratic polynomial, for reasons to be given later.

LEMMA 3

(i) $\dfrac{\pi_l^{(k)}}{\pi_l^{(j)}}$ *is a* p_l*-adic unit.*

(ii) $\mathrm{ord}_{p_l}\left(\dfrac{\pi_l^{(i_0)}}{\pi_l^{(j)}}\right) = h_l$.

Proof of Lemma 3. Let $\theta^{(j)}$ be a root of $g_2(t)$ say, and let $\mathfrak{p}'$ be the prime ideal dividing p_l that corresponds to $g_2(t)$, with ramification index e'. Then

$$\mathrm{ord}_{p_l}(\pi_l^{(j)}) = \frac{1}{e'}\,\mathrm{ord}_{\mathfrak{p}'}(\pi_l) = 0,$$

since $(\pi_l) = \mathfrak{p}_l^{h_l}$ and $\mathfrak{p}_l \neq \mathfrak{p}'$. Analogously we find $\mathrm{ord}_{p_l}(\pi_l^{(k)}) = 0$, and (i) follows. Further, (ii) follows from

$$\mathrm{ord}_{p_l}(\pi_l^{(i_0)}) = \frac{1}{e_1}\,\mathrm{ord}_{\mathfrak{p}_l}(\pi_l) = h_l,$$

since the ramification index e_1 of $\mathfrak{p}_l$ equals 1. □

Note that δ_1 and δ_2 are just constants, hence so are their p_l-adic orders. They must be computed explicitly.

7^{Ex} The number of cases has now grown to twenty: each of the five cases of Section 6^{Ex} has to be treated for each of the four primes $p_l = 2, 3, 5, 7$. *For* $p_l = 2, 3, 7$ we always have $i_0 = 1$, and we choose $j = 2$, $k = 3$. For $p_l = 5$ we take, according to the advice given above for choosing j and k:

Case	i_0	j	k
I	1	2	3
II	2	3	1
III	2	1	3
IV	3	2	1
V	3	1	2

With these choices we have:

	$\mathrm{ord}_p(\delta_1)$				$\mathrm{ord}_p(\delta_2)$			
Case	$p=2$	$p=3$	$p=5$	$p=7$	$p=2$	$p=3$	$p=5$	$p=7$
I	0	0	0	0	0	0	1	0
II	0	0	1	0	0	0	0	0
III	0	0	0	0	0	0	−1	0
IV	0	0	1	0	0	0	0	0
V	0	0	0	0	0	0	−1	0

8. A bound for N in terms of $\log H$

Put

$$N = \max\{n_1, \ldots, n_v\}, \quad A = \max\{|a_1|, \ldots, |a_r|\}, \quad H = \max\{N, A\}.$$

In this section we obtain an upper bound for N in terms of $\log H$. First we treat a special case, which turns out to be trivial. Then we give the main result of this section, based on the theory of p-adic linear forms in logarithms of algebraic numbers.

LEMMA 4. *If* $\mathrm{ord}_{p_l}(\delta_1) > 0$ *then* $n_l = \dfrac{-1}{h_l}\,\mathrm{ord}_{p_l}(\delta_2)$.

Proof of Lemma 4. Applying the Corollary of Lemma 2 and Lemma 3 to both expressions of λ in (12) we compute on the one hand $\mathrm{ord}_{p_l}(\lambda) = \min\{\mathrm{ord}_{p_l}(\delta_1), \mathrm{ord}_{p_l}(1)\} = 0$, and on the other hand $\mathrm{ord}_{p_l}(\lambda) = \mathrm{ord}_{p_l}(\delta_2) + n_l h_l$, hence the result follows. □

THEOREM 5. *There exist positive constants* $c_{10}(p_l)$, $c_{11}(p_l)$, *depending on* F *and* c *too, that can be explicitly calculated, such that*

$$n_l \leqslant c_{10}(p_l)(\log H + c_{11}(p_l)).$$

Proof of Theorem 5. Obviously we may assume $H \geqslant 1$. Let $c_{10}(p_l) \geqslant 1$, $c_{11}(p_l) > \dfrac{-1}{h_l}\mathrm{ord}_{p_l}(\delta_2)$. Then we may assume $n_l > \dfrac{-1}{h_l}\mathrm{ord}_{p_l}(\delta_2)$, and Lemma 4 implies $\mathrm{ord}_{p_l}(\delta_1) = 0$. From (12), the Corollary of Lemma 2 and Lemma 3 we infer

$$\mathrm{ord}_{p_l}(\lambda) = \mathrm{ord}_{p_l}(\delta_2) + n_l h_l > 0, \tag{13}$$

and also that all the ratios appearing in the first expression for λ in (12) are p_l-

adic units; hence δ_1 is a p_l-adic unit as well. Applying Yu's theorem (see Appendix A2) to the first expression for λ in (12) we find

$$\mathrm{ord}_{p_l}(\lambda) \leqslant c'_{10}(\log H + c'_{11})$$

for some positive constants c'_{10}, c'_{11} depending on p_l, which can be explicitly calculated (c'_{10} will be 'large'). We may assume $c'_{10} \geqslant h_l$. Now (13) implies the theorem with

$$c_{10}(p_l) = \frac{c'_{10}}{h_l}, \quad c_{11}(p_l) = \max\left\{c'_{11} - \frac{1}{c'_{10}}\,\mathrm{ord}_{p_l}(\delta_2), \frac{-1}{h_l}\,\mathrm{ord}_{p_l}(\delta_2)\right\}. \qquad \square$$

On putting

$$c_{13} = \max_{l=1,\ldots,v} c_{10}(p_l), \quad c_{14} = \max_{l=1,\ldots,v} c_{11}(p_l),$$

Theorem 5 implies

$$N \leqslant c_{13}(\log H + c_{14}). \tag{14}$$

8^{Ex} Lemma 4 implies $n_5 = 0$ in cases II and IV. Hence, they can be incorporated in case I with $n_5 = 0$. As a result, from now on we need only consider cases I, III and V. The constants $c_{10}(p_l)$ and $c_{11}(p_l)$ have to be computed from [Yu2]; see Appendix $A2^{\mathrm{Ex}}$. We obtained:

$p=$	2	3	5	7
$c_{10}<$	1.020×10^{47}	8.051×10^{43}	2.787×10^{44}	7.050×10^{41}
$c_{11}<$	4.970			

so that $c_{13} < 1.020\times 10^{47}$, $c_{14} < 4.970$.

9. A bound for H

Theorem 5 was the first important step towards an upper bound for H. In fact, it contains all the p-adic arguments. We will also need real/complex arguments, which we will give in this and the next section. Our aim is to bound A from above by a linear function of H. Put

$$\varepsilon = \varepsilon_1^{a_1}\cdot\ldots\cdot\varepsilon_r^{a_r}.$$

For any $r \times r$ matrix $U = (u_{ij})$ we define the *row-norm* $\mathbb{N}[U]$ of U as

$$\mathbb{N}[U] = \max_{1 \leqslant i \leqslant r} (|u_{i1}| + \cdots + |u_{ir}|).$$

LEMMA 6. *Let $I = \{i_1, \ldots, i_r\} \subset \{1, \ldots, s+t\}$ be any set of r distinct indices, and consider*

$$U_I = \begin{bmatrix} \log|\varepsilon_1^{(i_1)}| & \cdots & \log|\varepsilon_r^{(i_1)}| \\ \vdots & & \vdots \\ \log|\varepsilon_1^{(i_r)}| & \cdots & \log|\varepsilon_r^{(i_r)}| \end{bmatrix}.$$

Let I_0 be an index set such that

$$\mathbb{N}[U_{I_0}^{-1}] = \min_{I} \mathbb{N}[U_I^{-1}],$$

and let $k \in I_0$ be an index such that

$$|\log|\varepsilon^{(k)}|| = \max_{h \in I_0} |\log|\varepsilon^{(h)}||.$$

Then either $|\varepsilon^{(k)}| \geqslant e^{c_{15}A}$ or $|\varepsilon^{(k)}| \leqslant e^{-c_{15}A}$, where $c_{15} = 1/\mathbb{N}[U_{I_0}^{-1}]$.

Proof of Lemma 6. Let $I_0 = \{i_1, \ldots, i_r\}$. Then

$$\begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} = U_{I_0}^{-1} \cdot \begin{bmatrix} \log|\varepsilon^{(i_1)}| \\ \vdots \\ \log|\varepsilon^{(i_r)}| \end{bmatrix},$$

and it is straightforward to see that

$$A \leqslant \mathbb{N}[U_{I_0}^{-1}] \cdot |\log|\varepsilon^{(k)}||.$$

The lemma follows at once. □

Now we choose a positive constant

$$c_{16} < \frac{c_{15}}{n-1}.$$

Although it can be chosen arbitrarily, in any specific example of a Thue-Mahler

equation its choice will affect the size of the upper bound for H to be found. Later we will indicate what might be an optimal size for c_{16}.

We distinguish three cases. In the first two, k will be the index defined in Lemma 6.

Case 1. $\min\limits_{1\leqslant i\leqslant n} |\beta^{(i)}| > e^{-c_{16}A}$ and $|\varepsilon^{(k)}| \geqslant e^{c_{15}A}$. We have

$$|\beta^{(k)}| \cdot \prod_{i\neq k} |\beta^{(i)}| = |f_0^{n-1}c| \cdot p_1^{z_1} \cdot \ldots \cdot p_v^{z_v},$$

therefore

$$|\beta^{(k)}| < |f_0^{n-1}c| \cdot p_1^{z_1} \cdot \ldots \cdot p_v^{z_v} \cdot e^{(n-1)c_{16}A}.$$

Hence, for this case, using (10) and (11), it follows that

$$\begin{aligned} e^{c_{15}A} \leqslant |\varepsilon^{(k)}| &= \frac{|\beta^{(k)}|}{|\alpha^{(k)}| \cdot |\pi_1^{(k)}|^{n_1} \cdot \ldots \cdot |\pi_v^{(k)}|^{n_v}} < \frac{|f_0^{n-1}c| \cdot p_1^{z_1} \cdot \ldots \cdot p_v^{z_v} \cdot e^{(n-1)c_{16}A}}{|\alpha^{(k)}| \cdot |\pi_1^{(k)}|^{n_1} \cdot \ldots \cdot |\pi_v^{(k)}|^{n_v}} \\ &< \frac{|f_0^{n-1}c| \cdot p_1^{s_1+t_1} \cdot \ldots \cdot p_v^{s_v+t_v}}{|\alpha^{(k)}|} \cdot \left|\frac{p_1^{h_1}}{\pi_1^{(k)}}\right|^{n_1} \cdot \ldots \cdot \left|\frac{p_v^{h_v}}{\pi_v^{(k)}}\right|^{n_v} \cdot e^{(n-1)c_{16}A} \\ &< \exp\{c'_{18} + c'_{17}N + (n-1)c_{16}A\}, \end{aligned}$$

where

$$c'_{17} = \log \frac{p_1^{h_1} \cdot \ldots \cdot p_v^{h_v}}{\min\limits_{1\leqslant j\leqslant n} |\pi_1^{(j)} \cdot \ldots \cdot \pi_v^{(j)}|}, \quad c'_{18} = \log \frac{|f_0^{n-1}c| \cdot p_1^{h_1+t_1-1} \cdot \ldots \cdot p_v^{h_v+t_v-1}}{\min\limits_{1\leqslant j\leqslant n} |\alpha^{(j)}|}.$$

It follows that

$$A < \frac{c'_{18} + c'_{17}N}{c_{15} - (n-1)c_{16}}. \tag{15}$$

Case 2. $\min\limits_{1\leqslant i\leqslant n} |\beta^{(i)}| > e^{-c_{16}A}$ and $|\varepsilon^{(k)}| \leqslant e^{-c_{15}A}$. Now,

$$e^{-c_{15}A} \geqslant |\varepsilon^{(k)}| = \frac{|\beta^{(k)}|}{|\alpha^{(k)}| \cdot |\pi_1^{(k)}|^{n_1} \cdot \ldots \cdot |\pi_v^{(k)}|^{n_v}} > \frac{e^{-c_{16}A}}{|\alpha| \, |\pi_1 \cdot \ldots \cdot \pi_v|^N},$$

from which it follows that

$$A < \frac{c''_{18} + c''_{17}N}{c_{15} - c_{16}} \tag{16}$$

with

$$c''_{17} = \log\boxed{\pi_1 \cdot \cdots \cdot \pi_v}, \quad c''_{18} = \log\boxed{\alpha}.$$

Note that, in view of Lemma 6, the cases 1 and 2 are exhaustive with respect to the condition $\min_{1 \leqslant i \leqslant n} |\beta^{(i)}| > e^{-c_{16}A}$. Summarizing, we have

PROPOSITION 7. *If*

$$\min_{1 \leqslant i \leqslant n} |\beta^{(i)}| > e^{-c_{16}A}$$

then

$$A < c_{18} + c_{17}N, \tag{17}$$

where

$$c_{17} = \max\left\{\frac{c'_{17}}{c_{15} - (n-1)c_{16}}, \frac{c''_{17}}{c_{15} - c_{16}}\right\},$$

$$c_{18} = \max\left\{\frac{c'_{18}}{c_{15} - (n-1)c_{16}}, \frac{c''_{18}}{c_{15} - c_{16}}\right\}.$$

Now, Theorem 5 and Proposition 7 imply the following

PROPOSITION 8. *If*

$$\min_{1 \leqslant i \leqslant n} |\beta^{(i)}| > e^{-c_{16}A}$$

then

$$H < c_{19} + c_{20} \log H, \tag{18}$$

where

$$c_{19} = \max\{c_{13}c_{14}, c_{13}c_{14}c_{17} + c_{18}\}, \; c_{20} = c_{13} \max\{c_{17}, 1\}.$$

Proof of Proposition 8. If $H = N$ then Theorem 5 implies $H < c_{13}c_{14} + c_{13} \log H$. If $H \neq N$ then $H = A > N$, and Proposition 7 and

Theorem 5 imply

$$H = A < c_{18} + c_{17}N < c_{18} + c_{17}c_{13}(\log H + c_{14}),$$

and in both cases the result follows. □

9^{Ex} We have:

	(1)	(2)	(3)
$\log\lvert\varepsilon_1\rvert$	$-1.422188\ldots$	$-4.998188\ldots$	$6.420376\ldots$
$\log\lvert\varepsilon_2\rvert$	$-15.983272\ldots$	$9.151570\ldots$	$6.831702\ldots$

(so the regulator of the field K is $R = 92.902663\ldots$). Clearly, $I_0 = \{2, 3\}$, and

$$U_{I_0}^{-1} = \begin{pmatrix} -0.07353613\ldots & 0.09850707\ldots \\ 0.06910863\ldots & 0.05380027\ldots \end{pmatrix}$$

with $\mathbb{N}[U_{I_0}^{-1}] = 0.17204321\ldots, c_{15} > 5.812$. Further we have

$$c'_{17} \leqslant \log \frac{2\cdot 3\cdot 5\cdot 7}{|\pi_{21}^{(2)}\pi_{31}^{(2)}\pi_{53}^{(2)}\pi_{71}^{(2)}|} < 24.455,\ c'_{18} \leqslant \log \frac{5}{|\pi_{53}^{(2)}|} < 11.142,$$

$$c''_{17} \leqslant \log|\pi_{21}^{(3)}\pi_{31}^{(3)}\pi_{53}^{(3)}\pi_{71}^{(3)}| < 15.753,\ c''_{18} \leqslant \log|\pi_{53}^{(3)}| < 5.888.$$

For the time being we do not specify c_{16}. Thus

$$c_{17} < \max\left\{\frac{24.455}{5.812 - 2c_{16}}, \frac{15.753}{5.812 - c_{16}}\right\} = \frac{24.455}{5.812 - 2c_{16}},$$

$$c_{18} < \max\left\{\frac{11.142}{5.812 - 2c_{16}}, \frac{5.888}{5.812 - c_{16}}\right\} = \frac{11.142}{5.812 - 2c_{16}},$$

$$c_{19} < \max\left\{5.070\times 10^{47}, \frac{1.240\times 10^{49}}{5.812 - 2c_{16}}\right\} = \frac{1.240\times 10^{49}}{5.812 - 2c_{16}},$$

$$c_{20} < \max\left\{1.020\times 10^{47}, \frac{2.495\times 10^{48}}{5.812 - 2c_{16}}\right\} = \frac{2.495\times 10^{48}}{5.812 - 2c_{16}}.$$

10. A bound for H, continued

In this section we deal with the remaining case.

Case 3. $\min\limits_{1\leqslant i\leqslant n} |\beta^{(i)}| \leqslant e^{-c_{16}A}$. We treat the S-unit equation in a way which is essentially the same as that we used in [TW1] for the unit equation resulting from a Thue equation. Put

$$|\beta^{(i_0)}| = \min_{1\leqslant i\leqslant n} |\beta^{(i)}| \leqslant e^{-c_{16}A}, \tag{19}$$

(note that we have no prior knowledge of i_0, which depends on the solution (x, y)), and

$$c_{12} = \begin{cases} \max\left\{\left\lceil -\frac{1}{c_{16}} \log \min_{s+1 \leqslant j \leqslant s+t} |\operatorname{Im} \theta^{(j)}| \right\rceil, 1\right\} & \text{if } t > 0, \\ 1 & \text{if } t = 0. \end{cases}$$

First we treat the case $s = 0$ (called the 'totally complex case').

PROPOSITION 9. *If* $\min_{1 \leqslant i \leqslant n} |\beta^{(i)}| \leqslant e^{-c_{16}A}$ *and* $s = 0$, *then*

$$H \leqslant c_{12} \quad \text{if } H = A,$$
$$H \leqslant c_{13}c_{14} + c_{13} \log H \quad \text{if } H = N.$$

Proof of Proposition 9. If $H = A$ then $H \leqslant c_{12}$ by (19), since $t > 0$ and either $y = 0$, whence $|\beta^{(i_0)}| = |x| = 1$, $A = 0$, or $\beta^{(i_0)} \notin \mathbb{R}$, whence $|\beta^{(i_0)}| \geqslant |\operatorname{Im} \theta^{(i_0)}|$. If $H \neq A$ then $H = N > A$, and (14) implies $H \leqslant c_{13}c_{14} + c_{13} \log H$. □

Next we assume $s > 0$. We distinguish between the case $s = 1, 2$ (called 'the complex case'), and $s \geqslant 3$ (called 'the real case'). The characterizations 'complex' and 'real' refer to the kind of logarithms that we will use below.

From now on we will assume $A \geqslant c_{12}$, so that as in the proof of Proposition 9, (19) implies $i_0 \in \{1, \ldots, s\}$. We choose $j, k \in \{1, \ldots, n\}$ such that $i_0 \neq j \neq k \neq i_0$. Moreover, in the real case we choose j, k arbitrarily from $\{1, \ldots, s\}$, so that all three of $\theta^{(i_0)}$, $\theta^{(j)}$, $\theta^{(k)}$ are in $\mathbb{R}$, while in the complex case we choose j arbitrarily from $\{s + 1, \ldots, s + t\}$, and then $k = j + t$, so that $\theta^{(k)} = \overline{\theta^{(j)}}$. This choice of j and k is not absolutely essential, but turns out to be convenient.

From

$$|y| \cdot |\theta^{(j)} - \theta^{(i_0)}| = |\beta^{(j)} - \beta^{(i_0)}| \leqslant 2|\beta^{(j)}|$$

it follows that

$$|\beta^{(j)}| \geqslant \tfrac{1}{2} \min_{i \neq l} |\theta^{(l)} - \theta^{(i)}|.$$

Here, the minimum is taken over all $i, l \in \{1, \ldots, s\}$ in the real case, and over all $i \in \{1, \ldots, s\}$, $l \in \{s + 1, \ldots, s + t\}$ in the complex case. Using this and (19) we find from (12)

$$|\lambda| \leqslant \frac{2}{\min_{i \neq l} |\theta^{(l)} - \theta^{(i)}|} \cdot \left| \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \right| \cdot e^{-c_{16}A} \leqslant c_{21} e^{-c_{16}A}, \tag{20}$$

where

$$c_{21} = \frac{2}{\min\limits_{i \neq l} |\theta^{(l)} - \theta^{(i)}|} \cdot \max_{i_1 \neq i_2 \neq i_3 \neq i_1} \left| \frac{\theta^{(i_2)} - \theta^{(i_3)}}{\theta^{(i_3)} - \theta^{(i_1)}} \right|.$$

Here the minimum is taken as above, and the maximum is taken over all $i_1, i_2, i_3 \in \{1, \ldots, s\}$ in the real case, and over all $i_1 \in \{1, \ldots, s\}$, $i_2 \in \{s+1, \ldots, s+t\}$, $i_3 = i_2 + t$ in the complex case.

Note that if $H = N$, then (14) implies

$$H < c_{13}c_{14} + c_{13} \log H, \tag{21}$$

and H is already bounded. So now assume $H = A > N$. Further we assume that

$$H \geqslant c_{22}, \tag{22}$$

where

$$c_{22} = \max \left\{ c_{12}, \left\lceil \frac{\log(2c_{21})}{c_{16}} \right\rceil \right\}.$$

In the real case, put

$$\Lambda_0 = \log(1 + \lambda).$$

This is well defined by (22), since then (20) implies $|\lambda| \leqslant \frac{1}{2}$, so $1 + \lambda > 0$. Note that $\Lambda_0 \neq 0$. We find $|e^{\Lambda_0} - 1| = |\lambda| \leqslant \frac{1}{2}$, hence

$$0 < |\Lambda_0| < 1.39|\lambda| < 1.39c_{21}e^{-c_{16}A}, \tag{23}$$

where Λ_0 can be written as

$$\Lambda_0 = \log \left| \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}}{\alpha^{(j)}} \right| + \sum_{i=1}^{v} n_i \log \left| \frac{\pi_i^{(k)}}{\pi_i^{(j)}} \right| + \sum_{i=1}^{r} a_i \log \left| \frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right|.$$

On the other hand, by the theory of linear forms in logarithms of algebraic numbers (cf. [Wa], (BGMMS]), we can find a lower bound for $|\Lambda_0|$ of the following form:

$$|\Lambda_0| > \exp\{-c_7(\log H + c_8)\}, \tag{24}$$

where the constants c_7, c_8 can be explicitly calculated (see Appendix A3). Thus (22), (23) and (24) combine to

$$\text{if } H = A \geqslant c_{22} \text{ then } H < \frac{\log(1.39c_{21}) + c_7c_8}{c_{16}} + \frac{c_7}{c_{16}} \log H. \tag{25}$$

We now put

$$c_{23} = \max\left\{c_{13}c_{14}, c_{22}, \frac{\log(1.39c_{21}) + c_7c_8}{c_{16}}\right\}, \quad c_{24} = \max\left\{c_{13}, \frac{c_7}{c_{16}}, e^2\right\}.$$

Thus in the real case, in both the cases $H = N$ and $H = A$, we conclude in view of (21) and (25) that

$$H \leqslant c_{23} + c_{24} \log H, \quad c_{24} > e^2. \tag{26}$$

In the complex case, put

$$\Lambda_0 = \frac{1}{i} \operatorname{Log}(1 + \lambda).$$

Here, Log(z) stands for the principal value of the complex logarithm of z, thus $-\pi < \operatorname{Im} \operatorname{Log}(z) \leqslant \pi$. Since we have $\theta^{(i_0)} \in \mathbb{R}$ and $\theta^{(k)} = \overline{\theta^{(j)}}$, we have

$$\Lambda_0 = \frac{1}{i} \operatorname{Log}\left(\frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{x - y\theta^{(k)}}{x - y\theta^{(j)}}\right) \in \mathbb{R},$$

and hence $|\Lambda_0| \leqslant \pi$. Again we note that $\Lambda_0 \neq 0$. Now, again assuming (22), $|\lambda| \leqslant \frac{1}{2}$ implies $|\sin \frac{1}{2}\Lambda_0| = \frac{1}{2}|e^{i\Lambda_0} - 1| = \frac{1}{2}|\lambda| \leqslant \frac{1}{4}$, hence

$$|\Lambda_0| \leqslant 2 \frac{1/4}{\sin 1/4} |\sin \tfrac{1}{2}\Lambda_0| < 1.02|\lambda|.$$

Thus

$$0 < |\Lambda_0| < 1.02c_{21}e^{-c_{16}A}, \tag{27}$$

and Λ_0 may be written as

$$\Lambda_0 = \operatorname{Arg}\left(\frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}}{\alpha^{(j)}}\right) + \sum_{i=1}^{v} n_i \operatorname{Arg}\left(\frac{\pi_i^{(k)}}{\pi_i^{(j)}}\right) + \sum_{i=1}^{r} a_i \operatorname{Arg}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right) + a_0 \cdot 2\pi.$$

For $z \in \mathbb{C}$ we have $-\pi < \mathrm{Arg}(z) \leqslant \pi$, and since $\mathrm{Arg}(z_1 z_2) = \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2)$ holds only modulo 2π, one more unknown integer a_0 has entered the scene. By elementary estimations we see that $2\pi|a_0| \leqslant |\Lambda_0| + vN\pi + rA\pi$, hence by $|\Lambda_0| \leqslant \frac{1}{2}$ and $a_0 \in \mathbb{Z}$ we find

$$|a_0| \leqslant \tfrac{1}{2}(1 + vN + rA) \leqslant \tfrac{1}{2}(1 + v + r)H$$

under the assumption $H \geqslant 1$.

Since $|\Lambda_0| = |i\Lambda_0|$ and $i\Lambda_0$ is a linear form in logarithms of algebraic numbers (note that $2\pi i = 2\,\mathrm{Log}(-1)$), we get, by analogy with (24),

$$|\Lambda_0| > \exp\{-c_7(\log H + c_8')\},$$

with $c_8' = c_8 + \log \frac{1}{2}(1 + v + r)$. We conclude, as in the real case, but now from (22) and (27), that

$$H \leqslant c_{23}' + c_{24} \log H, \quad c_{24} > e^2, \tag{28}$$

where

$$c_{23}' = \max\left\{c_{13}c_{14},\ c_{22},\ \frac{\log(1.02c_{21}) + c_7 c_8'}{c_{16}}\right\}.$$

10^{Ex} Since $t = 0$ we have $c_{12} = 1$. We are, of course, in the real case. Now the value of i_0 can be any of 1, 2, 3, so we have to perform the computations for three cases, namely $(i_0, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$. Then

$$c_{21} = \frac{2}{|\theta^{(1)} - \theta^{(2)}|} \cdot \frac{|\theta^{(3)} - \theta^{(1)}|}{|\theta^{(1)} - \theta^{(2)}|} < 11.009659,$$

$$c_{22} = \max\left\{1, \left\lceil \frac{3.091921}{c_{16}} \right\rceil\right\} < \frac{3.091921}{c_{16}} + 1 < \frac{6}{c_{16}}.$$

From Appendix $A3^{\mathrm{Ex}}$ we see

$$c_7 < 2.289 \times 10^{33}, \quad c_8 < 885.955,$$

so we obtain

$$c_{23} < \max\left\{5.070 \times 10^{47}, \frac{2.028 \times 10^{36}}{c_{16}}\right\},$$

$$c_{24} < \max\left\{1.020 \times 10^{47}, \frac{2.289 \times 10^{33}}{c_{16}}\right\}.$$

11. The main theorem

We are now in a position to state and prove the main result of this paper. Put

$$c_{25} = \max\{c_{19}, c_{23}\},\ c'_{25} = \max\{c_{19}, c'_{23}\},\ c_{26} = \max\{c_{20}, c_{24}\},$$

$$c^+_{20} = \max\{c_{20}, e^2\},\ c^+_{13} = \max\{c_{13}, e^2\},$$

$$c_{\text{real}} = 2c_{25} + 2c_{26}\log c_{26},$$

$$c_{\text{complex}} = 2c'_{25} + 2c_{26}\log c_{26},$$

$$c_{\text{totally complex}} = \max\{c_{12}, 2c_{13}c_{14} + 2c^+_{13}\log c^+_{13}, 2c_{19} + 2c^+_{20}\log c^+_{20}\}.$$

THEOREM 10

(i) *In the real case* $s \geqslant 3$ *we have* $H < c_{\text{real}}$.

(ii) *In the complex case* $s = 1, 2$ *we have* $H < c_{\text{complex}}$.

(iii) *In the totally complex case* $s = 0$ *we have* $H < c_{\text{totally complex}}$.

Proof of Theorem 10. In each of the cases we have an inequality of the shape

$$H \leqslant c' + c''\log H,$$

for fully explicit constants c', c'' with $c'' > e^2$. Then apply Lemma 2.2 of [PW]. □

In practice, the constants coming from the estimates for linear forms in logarithms of algebraic numbers, and all constants depending on them, are very large compared to the others. These large constants are c'_{10}, $c_{10}(p_l)$, c_{13}, c^+_{13}, c_{19}, c_{20}, c^+_{20} all of which depend on the p-adic estimate for linear forms [Yu2], c_7 that comes from the real/complex estimate [BGMMS], and c_{23}, c'_{23}, c_{24}, c_{25}, c'_{25}, c_{26} which depend on both estimates. Note that c_{real} and c_{complex} depend on the p-adic and real estimates, whereas $c_{\text{totally complex}}$ depends on the p-adic estimate only. Further note that the final bounds c_{real}, c_{complex} are essentially of the size of $\max\{c_7, c_{13}\}$, and $c_{\text{totally complex}}$ is of the size of c_{13}.

The choice of c_{16} is free, so it can be taken such that the final bound of Theorem 10 becomes optimal. Generally speaking, an optimal c_{16} will be of the size of c_7/c_{13} if $c_{13} \gg c_7$, and of the size of $c_{15}/(n-1)$ if $c_{13} \ll c_7$ or if c_{13} and c_7 are of the same size. Here, c_{13} comes from the p-adic estimate, and c_7 from the real/complex estimate.

If, in the real or complex case, $c_{13} \ll c_7$, then we can find a better upper bound for N, namely one of the size of c_{13}. Indeed, with

$$c_N = \begin{cases} c_{13}(\log c_{\text{real}} + c_{14}) & \text{in the real case} \\ c_{13}(\log c_{\text{complex}} + c_{14}) & \text{in the complex case} \end{cases}$$

we have the following corollary.

COROLLARY OF THEOREM 10. *In the real and complex cases,* $N \leqslant c_N$.

Proof of the Corollary. Obvious from Theorem 10 and (14). □

11^{Ex} We find

$$c_{25} < \max\left\{\frac{1.240 \times 10^{49}}{5.812 - 2c_{16}}, \frac{2.028 \times 10^{36}}{c_{16}}\right\},$$

$$c_{26} < \max\left\{\frac{2.495 \times 10^{48}}{5.812 - 2c_{16}}, \frac{2.289 \times 10^{33}}{c_{16}}\right\}.$$

We found that $c_{16} = 10^{-12}$ is more or less optimal (it is indeed of the size of c_7/c_{13}). Then

$$c_{\text{real}} < 9.844 \times 10^{49}.$$

In this case the corollary gives no essential improvement, since $c_{13} \gg c_7$.

12. Preliminaries for the reduction process

In the following sections we show how the bound for H, given by Theorem 10, can be considerably reduced. To do so we use methods from Computational Diophantine Approximation Theory.

First, we need some results from the theory of p-adic numbers. Recall that for any $z \in \mathbb{C}_p$ with $\text{ord}_p(z-1) > 0$ the p-adic logarithm of z is defined by the convergent p-adic power series

$$\log_p z = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} (z-1)^i.$$

Moreover, if $\text{ord}_p(z-1) > 1/(p-1)$, then all the usual properties of the logarithmic function are valid. In view of the following lemma, we can extend the definition of the p-adic logarithm of z to all p-adic units of $\mathbb{C}_p$.

LEMMA 11. *If* $z \in \mathbb{C}_p$ *is a p-adic unit, then a positive integer* ϕ *can be explicitly found such that*

$$\text{ord}_p(z^\phi - 1) > \frac{1}{p-1}.$$

Proof of Lemma 11. If z is algebraic over $\mathbb{Q}_p$, our claim follows from Fermat's Little Theorem for algebraic number fields, cf. [BS, Chapter 3, Section 7, Problem 6]. Then the general case follows since every $z \in \mathbb{C}_p$ is the limit of a sequence of elements of $\mathbb{C}_p$ that are algebraic over $\mathbb{Q}_p$. □

For z as in Lemma 11 we define

$$\log_p z = \frac{1}{\phi} \log_p z^\phi.$$

Although ϕ is not uniquely defined, the above definition is independent of ϕ, as can be easily established.

LEMMA 12. *Let* $z_1, \ldots, z_q \in \mathbb{C}_p$ be *p-adic units. Let* $b_1, \ldots, b_q \in \mathbb{Z}$. *If*

$$\operatorname{ord}_p(z_1^{b_1} \cdot \cdots \cdot z_q^{b_q} - 1) > \frac{1}{p-1}$$

then

$$\operatorname{ord}_p(b_1 \log_p z_1 + \cdots + b_q \log_p z_q) = \operatorname{ord}_p(z_1^{b_q} \cdot \cdots \cdot z_q^{b_1} - 1).$$

Proof of Lemma 12. This lemma is an easy consequence of the relation $\operatorname{ord}_p(z-1) = \operatorname{ord}_p \log_p z$, which is valid for $z \in \mathbb{C}_p$ with $\operatorname{ord}_p(z-1) > 1/(p-1)$ (see [Yu1, Section 1.1]). □

Now, let $p = p_l \in \{p_1, \ldots, p_v\}$ and let the factorization of p into prime ideals of K be as in Section 3. If among the polynomials $g_1(t), \ldots, g_m(t) \in \mathbb{Q}_p[t]$ there are at least three of the first degree, then, by the choice of i_0, j, k (cf. just before Lemma 3), all the p-adic numbers appearing in (12) are in $\mathbb{Q}_p$ itself. If however we are forced to use a conjugate for which $\deg g_i(t) \geqslant 2$, then, as we remarked just before Lemma 3, we take indices i_0, j, k in such a way that $\theta^{(i_0)} \in \mathbb{Q}_p$ and $\theta^{(j)}$, $\theta^{(k)}$ are roots of the same $g_i(t)$ with $\deg g_i(t) \geqslant 2$. In the latter case we consider K embedded in $K_{\mathfrak{p}_i}$ (where $\mathfrak{p}_i$ corresponds to $g_i(t)$; see Section 3), and the p-adic order and absolute value are defined in accordance with this embedding (see Section 4; for simplicity in our notation we do not distinguish between $x \in K$ and the image of x under the embedding $K \hookrightarrow K_{\mathfrak{p}_i}$). Now, all the numbers appearing in (12) belong to a finite extension of $\mathbb{Q}_p$.

In either case, all the numbers $\dfrac{\pi_1^{(k)}}{\pi_1^{(j)}}, \ldots, \dfrac{\pi_v^{(k)}}{\pi_v^{(j)}}, \dfrac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}, \ldots, \dfrac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}$ are p-adic units by the Corollary of Lemma 2 and Lemma 3, and $\operatorname{ord}_p(\delta_1) \geqslant 0$. Moreover, we may suppose that δ_1 is a p-adic unit as well. Indeed, if $\operatorname{ord}_p(\delta_1) > 0$, then by Lemma 4 n_l is 'very small', which means that for $p = p_l$ there is no need for a reduction process such as described below. In view of this, the following linear form in p_l-adic logarithms is well defined for $l = 1, \ldots, v$ (cf. (12)):

$$\Lambda_l = \log_{p_l}(\lambda + 1) = \log_{p_l}\delta_1 + \sum_{i=1}^{v} n_i \log_{p_l} \frac{\pi_i^{(k)}}{\pi_i^{(j)}} + \sum_{i=1}^{r} a_i \log_{p_l} \frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}$$

(δ_1 has been defined immediately after (12)). Further, in view of Section 10, we will also deal with the following linear forms: in the real case with

$$\Lambda_0 = \log(\lambda + 1) = \log|\delta_1| + \sum_{i=1}^{v} n_i \log \left|\frac{\pi_i^{(k)}}{\pi_i^{(j)}}\right| + \sum_{i=1}^{r} a_i \log \left|\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right|,$$

and in the complex case with

$$\Lambda_0 = \frac{1}{i}\operatorname{Log}(\lambda+1) = \operatorname{Arg}(\delta_1) + \sum_{i=1}^{v} n_i \operatorname{Arg}\left(\frac{\pi_i^{(k)}}{\pi_i^{(j)}}\right) + \sum_{i=1}^{r} a_i \operatorname{Arg}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right) + a_0 \cdot 2\pi.$$

In dealing with Λ_l for $l = 1, \ldots, v$, all three indices i_0, j, k are fixed, as noted immediately before Lemma 3. However, in case of Λ_0, we have no prior knowledge of i_0, which is defined by (19), and thus depends on the presupposed solution (x, y). Therefore in this case we must consider all possible values for i_0, and for each one of them fix j, k, according to the rules given after Proposition 9.

For convenience, let us write

$$\Lambda_l = \rho_l + \sum_{i=1}^{v} n_i \lambda_{li} + \sum_{i=1}^{r} a_i \mu_{li} (+ a_0 2\pi)$$

for $l = 1, \ldots, v, 0$, where the definitions of $\rho_l, \lambda_{li}, \mu_{li}$ are obvious. Note that in the totally complex case we have only $l = 1, \ldots, v$. In fact, in the totally complex case any upper bound for N immediately gives rise to a good upper bound for A, by Propositions 7 and 9, namely $A \leqslant \max\{c_{18} + c_{17}N, N, c_{12}\}$ (note that c_{17} and c_{18} are 'small' numbers).

Lemma 12 guarantees that when n_l is large enough, an important property of λ is carried over to Λ_l, namely that its p_l-adic order can be expressed in terms of n_l. Put

$$v_l = \operatorname{ord}_{p_l}(\delta_2).$$

LEMMA 13. *If*

$$n_l > \frac{1}{h_l}\left(\frac{1}{p-1} - v_l\right)$$

then

$$\operatorname{ord}_{p_l}(\Lambda_l) = n_l h_l + v_l.$$

Proof of Lemma 13. Obvious from (12), (13) and Lemma 12. □

12[Ex] In this section we give approximations of the p-adic values for $p = 2, 3, 5, 7, \infty$ of the numbers appearing in the linear forms Λ_l ($l = 1, 2, 3, 4, 0$). When applying the reduction process, we will of course need much higher precision. We give first the p-adic field $K_{\mathfrak{p}}$ in which K is considered embedded (cf. the lines following the proof of Lemma 12), the choice of indices i_0, j, k, and for $l = 1, 2, 3, 4$ the value of v_l (see the Table in Section 7[Ex]). The above information is given for each p separately. Note that $h_1 = h_2 = h_3 = h_4 = 1$.

$p_1 = 2$: $K \hookrightarrow K_{\mathfrak{p}_{22}} = \mathbb{Q}_2(\theta)$, $v_1 = 0$, $\theta^{(1)} = 0.0001000110\ldots$, $\theta^{(2)}$, $\theta^{(3)}$ roots of $t^2 + 0.1000111010\ldots t + 0.1011000010\ldots$. We put $\theta^{(2)} = \theta$, so that $\theta^{(3)} = -\theta - 0.1000111010\ldots$. Then with $(i_0, j, k) = (1, 2, 3)$ we have

$$\rho_1 = \log_2 \delta_1 = \begin{cases} \log_2 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} & \text{in Case I} \\ \log_2 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} \dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}} & \text{in Case III,} \quad \lambda_{11} = \log_2 \dfrac{\pi_{21}^{(3)}}{\pi_{21}^{(2)}}, \quad \lambda_{12} = \log_2 \dfrac{\pi_{31}^{(3)}}{\pi_{31}^{(2)}}, \\ \log_2 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} \dfrac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}} & \text{in Case V} \end{cases}$$

$$\lambda_{13} = \begin{cases} \log_2 \dfrac{\pi_{51}^{(3)}}{\pi_{51}^{(2)}} & \text{in Case I} \\ \log_2 \dfrac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}} & \text{in Case III,} \quad \lambda_{14} = \log_2 \dfrac{\pi_{71}^{(3)}}{\pi_{71}^{(2)}}, \quad \mu_{11} = \log_2 \dfrac{\varepsilon_1^{(3)}}{\varepsilon_1^{(2)}}, \quad \mu_{12} = \log_2 \dfrac{\varepsilon_2^{(3)}}{\varepsilon_2^{(2)}}. \\ \log_2 \dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}} & \text{in Case V} \end{cases}$$

	Case I	Case III	Case V
ρ_1	$0.0011010000\cdots + 0.0001101110\cdots\theta$	$0.0010001101\cdots + 0.0001000001\cdots\theta$	$0.0000100010\cdots + 0.0000010000\cdots\theta$
λ_{11}	$0.0010010001\cdots + 0.0001001100\cdots\theta$		
λ_{12}	$0.0000111010\cdots + 0.0000011100\cdots\theta$		
λ_{13}	$0.0010000100\cdots + 0.0001000110\cdots\theta$	$0.0010011100\cdots + 0.0001001001\cdots\theta$	$0.0001100101\cdots + 0.0000110000\cdots\theta$
λ_{14}	$0.0011111100\cdots + 0.0001111010\cdots\theta$		
μ_{11}	$0.0000111101\cdots + 0.0000011111\cdots\theta$		
μ_{12}	$0.0010111010\cdots + 0.0001011010\cdots\theta$		

$p_2 = 3$: $K \hookrightarrow K_{\mathfrak{p}_{32}} = \mathbb{Q}_3(\theta)$, $v_2 = 0$, $\theta^{(1)} = 0.0210020022\ldots$, $\theta^{(2)}$, $\theta^{(3)}$ roots of $t^2 + 0.1022210022\cdots t + 0.2021111120\ldots$. We put $\theta^{(2)} = \theta$, so that $\theta^{(3)} = -\theta - 0.1022210022\ldots$. Then with $(i_0, j, k) = (1, 2, 3)$ we have

$$\rho_2 = \log_3 \delta_1 = \begin{cases} \log_3 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} & \text{in Case I} \\ \log_3 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} \dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}} & \text{in Case III,} \quad \lambda_{21} = \log_3 \dfrac{\pi_{21}^{(3)}}{\pi_{21}^{(2)}}, \quad \lambda_{22} = \log_3 \dfrac{\pi_{31}^{(3)}}{\pi_{31}^{(2)}}, \\ \log_3 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} \dfrac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}} & \text{in Case V} \end{cases}$$

$$\lambda_{23}=\begin{cases}\log_3\dfrac{\pi_{51}^{(3)}}{\pi_{51}^{(2)}} & \text{in Case I}\\ \log_3\dfrac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}} & \text{in Case III,}\\ \log_3\dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}} & \text{in Case V}\end{cases}\quad \lambda_{24}=\log_3\frac{\pi_{71}^{(3)}}{\pi_{71}^{(2)}},\quad \mu_{21}=\log_3\frac{\varepsilon_1^{(3)}}{\varepsilon_1^{(2)}},\quad \mu_{22}=\log_3\frac{\varepsilon_2^{(3)}}{\varepsilon_2^{(2)}}.$$

	Case I	Case III	Case V
ρ_2	$0.0020121210\cdots+$ $0.0011001020\cdots\theta$	$0.0102202221\cdots+$ $0.0200020000\cdots\theta$	$0.0122101111\cdots+$ $0.0211220202\cdots\theta$
λ_{21}	$0.0110110222\cdots+0.0222121112\cdots\theta$		
λ_{22}	$0.0122212011\cdots+0.0211122022\cdots\theta$		
λ_{23}	$0.0112000120\cdots+$ $0.0220110102\cdots\theta$	$0.0102012120\cdots+$ $0.0200222111\cdots\theta$	$0.0111110011\cdots+$ $0.0221212202\cdots\theta$
λ_{24}	$0.0111021201\cdots+0.0221000010\cdots\theta$		
μ_{21}	$0.0101001221\cdots+0.0201112121\cdots\theta$		
μ_{22}	$0.0000110001\cdots+0.0000222220\cdots\theta$		

$p_3=5$: $K\hookrightarrow\mathbb{Q}_5$, $v_3=\begin{cases}1 & \text{in Case I}\\ -1 & \text{in Cases III, V}\end{cases}$, $\theta^{(1)}=0.4320132113\ldots$, $\theta^{(2)}=0.2212320101\ldots$, $\theta^{(3)}=0.2312041230\ldots$. We have with (Case, i_0, j, k) = (I, 1, 2, 3), (III, 2, 1, 3), (V, 3, 1, 2):

$$\rho_3=\log_5\delta_1=\begin{cases}\log_5\dfrac{\theta^{(1)}-\theta^{(2)}}{\theta^{(1)}-\theta^{(3)}} & \text{in Case I}\\ \log_5\dfrac{\theta^{(2)}-\theta^{(1)}}{\theta^{(2)}-\theta^{(3)}}\dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(1)}} & \text{in Case III,}\\ \log_5\dfrac{\theta^{(3)}-\theta^{(1)}}{\theta^{(3)}-\theta^{(2)}}\dfrac{\pi_{52}^{(2)}}{\pi_{52}^{(1)}} & \text{in Case V}\end{cases}\quad \lambda_{31}=\log_5\frac{\pi_{21}^{(k)}}{\pi_{21}^{(j)}},\quad \lambda_{32}=\log_5\frac{\pi_1^{(k)}}{\pi_{31}^{(j)}},$$

$$\lambda_{33}=\log_5\frac{\pi_{5i_0}^{(k)}}{\pi_{5i_0}^{(j)}},\quad \lambda_{34}=\log_5\frac{\pi_{71}^{(k)}}{\pi_{71}^{(j)}},\quad \mu_{31}=\log_5\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}},\quad \mu_{32}=\log_5\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}.$$

	Case I	Case III	Case V
ρ_3	$0.0303104024\cdots$	$0.0120010441\cdots$	$0.0210213301\cdots$
λ_{31}	$0.0104134430\cdots$	$0.0012340332\cdots$	$0.0403111341\cdots$
λ_{32}	$0.0020143404\cdots$	$0.0041022031\cdots$	$0.0021423022\cdots$
λ_{33}	$0.0013303302\cdots$	$0.0434331122\cdots$	$0.0000432440\cdots$
λ_{34}	$0.0104244122\cdots$	$0.0340230124\cdots$	$0.0241430441\cdots$
μ_{31}	$0.0221312110\cdots$	$0.0344013144\cdots$	$0.0123240034\cdots$
μ_{32}	$0.0034434443\cdots$	$0.0143020221\cdots$	$0.0114030222\cdots$

$p_4 = 7$: $K \hookrightarrow K_{p_{72}} = \mathbb{Q}_7(\theta)$, $v_4 = 0$, $\theta^{(1)} = 0.1544035230\ldots$, $\theta^{(2)}$, $\theta^{(3)}$ roots of $t^2 + 0.6144035230\cdots t + 0.4421630235\ldots$. We put $\theta^{(2)} = \theta$, so that $\theta^{(3)} = -\theta - 0.6144035230\ldots$. Then with $(i_0, j, k) = (1, 2, 3)$ we have

$$\rho_4 = \log_7 \delta_1 = \begin{cases} \log_7 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} & \text{in Case I} \\ \log_7 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} \dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}} & \text{in Case III,} \quad \lambda_{41} = \log_7 \dfrac{\pi_{21}^{(3)}}{\pi_{21}^{(2)}}, \quad \lambda_{42} = \log_7 \dfrac{\pi_{31}^{(3)}}{\pi_{31}^{(2)}}, \\ \log_7 \dfrac{\theta^{(1)} - \theta^{(2)}}{\theta^{(1)} - \theta^{(3)}} \dfrac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}} & \text{in Case V} \end{cases}$$

$$\lambda_{43} = \begin{cases} \log_7 \dfrac{\pi_{51}^{(3)}}{\pi_{51}^{(2)}} & \text{in Case I} \\ \log_7 \dfrac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}} & \text{in Case III,} \quad \lambda_{44} = \log_7 \dfrac{\pi_{71}^{(3)}}{\pi_{71}^{(2)}}, \quad \mu_{41} = \log_7 \dfrac{\varepsilon_1^{(3)}}{\varepsilon_1^{(2)}}, \quad \mu_{42} = \log_7 \dfrac{\varepsilon_2^{(3)}}{\varepsilon_2^{(2)}}. \\ \log_7 \dfrac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}} & \text{in Case V} \end{cases}$$

	Case I	Case III	Case V
ρ_4	$0.0661663355\cdots + 0.0245233564\cdots\theta$	$0.0402523333\cdots + 0.0636604432\cdots\theta$	$0.0534630416\cdots + 0.0401066250\cdots\theta$
λ_{41}	$0.0013364046\cdots + 0.0053662346\cdots\theta$		
λ_{42}	$0.0602344653\cdots + 0.0221636026\cdots\theta$		
λ_{43}	$0.0324004651\cdots + 0.0143562346\cdots\theta$	$0.0632043030\cdots + 0.0232423452\cdots\theta$	$0.0500626644\cdots + 0.0460440634\cdots\theta$
λ_{44}	$0.0513104013\cdots + 0.0444550354\cdots\theta$		
μ_{41}	$0.0504012336\cdots + 0.0466505033\cdots\theta$		
μ_{42}	$0.0650302255\cdots + 0.0264153356\cdots\theta$		

$p_0 = \infty$: $K \hookrightarrow \mathbb{R}$, $\theta^{(1)} = -0.9028831934\ldots$, $\theta^{(2)} = 1.1692597799\ldots$, $\theta^{(3)} = 22.7336234134\ldots$. We have with $(i_0, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$:

$$\rho_0 = \log|\delta_1| = \begin{cases} \log \left| \dfrac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \right| & \text{in Case I} \\ \log \left| \dfrac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \dfrac{\pi_{53}^{(k)}}{\pi_{53}^{(j)}} \right| & \text{in Case III,} \quad \lambda_{01} = \log \left| \dfrac{\pi_{21}^{(k)}}{\pi_{21}^{(j)}} \right|, \quad \lambda_{02} = \log \left| \dfrac{\pi_{31}^{(k)}}{\pi_{31}^{(j)}} \right|, \\ \log \left| \dfrac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \dfrac{\pi_{52}^{(k)}}{\pi_{52}^{(j)}} \right| & \text{in Case V} \end{cases}$$

$$\lambda_{03} = \begin{cases} \log \left|\dfrac{\pi_{51}^{(k)}}{\pi_{51}^{(j)}}\right| & \text{in Case I} \\ \log \left|\dfrac{\pi_{52}^{(k)}}{\pi_{52}^{(j)}}\right| & \text{in Case III,} \quad \lambda_{04} = \log \left|\dfrac{\pi_{71}^{(k)}}{\pi_{71}^{(j)}}\right|, \quad \mu_{01} = \log \left|\dfrac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right|, \quad \mu_{02} = \log \left|\dfrac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}\right|. \\ \log \left|\dfrac{\pi_{53}^{(k)}}{\pi_{53}^{(j)}}\right| & \text{in Case V} \end{cases}$$

$i_0 = 1$	Case I	Case III	Case V
ρ_0	−2.4342090823···	12.9846875535···	−8.8270472842···
λ_{01}	−5.8088635875···		
λ_{02}	20.3940649170···		
λ_{03}	−9.0260584338···	−6.3928382019···	15.4188966358···
λ_{04}	4.8551811120···		
μ_{01}	11.4185651918···		
μ_{02}	−2.3198675688···		

$i_0 = 2$	Case I	Case III	Case V
ρ_0	2.3424587957···	1.7095054351···	0.6315809180···
λ_{01}	0.3777789841···		
λ_{02}	−4.3593440764···		
λ_{03}	2.3438312383···	−1.7108778777···	−0.6329533606···
λ_{04}	−2.4354903211···		
μ_{01}	−7.8425648244···		
μ_{02}	−22.8149748950···		

$i_0 = 3$	Case I	Case III	Case V
ρ_0	0.0917502865···	−14.6941929886···	8.1954663662···
λ_{01}	5.4310846034···		
λ_{02}	−16.0347208405···		
λ_{03}	6.6822271954···	8.1037160796···	−14.7859432751···
λ_{04}	−2.4196907908···		
μ_{01}	−3.5760003674···		
μ_{02}	25.1348424639···		

13. The reduction strategy

Let K_0 be the upper bound for H that is given by Theorem 10, and let N_0 be the upper bound for N that is given by Theorem 10 or its corollary. Our reduction strategy is the following. For every $i = 1, \ldots, v$ we apply to the linear form Λ_i the so-called p-adic reduction step (with $p = p_i$; see Sections 14 and 15) in order to obtain an upper bound for n_i, which is very small in comparison with the initial upper bound N_0 for n_i; in fact it can be expected to be of the size of $(v + r)\dfrac{\log K_0}{\log p_i}$. Thus the maximum of these reduced upper bounds for $n_1, \ldots, n_v$ gives us a new upper bound N_1 for N, which is considerably smaller than N_0. Using this we can in turn find a new upper bound A_1 for A, which also is of the size of $(v + r)\dfrac{\log K_0}{\log p_i}$. Indeed, we have the following cases:

Case 1. $A \leqslant N$

Case 2. $N < A$ $\begin{cases} \text{Case 2.1: } A < c_{18} + c_{17}N \\ \text{Case 2.2: } c_{18} + c_{17}N \leqslant A \end{cases}$ $\begin{cases} \text{Case 2.2.1: } A \leqslant c_{22} \\ \text{Case 2.2.2: } A > c_{22} \end{cases}$

In all cases but Case 2.2.2 we immediately have for A an upper bound of the desired size (note that c_{17}, c_{18}, c_{22} are small compared to K_0 and N_0). In Case 2.2.2 we have

$$c_{18} + c_{17}N \leqslant A \quad \text{and} \quad A > c_{22} \quad \text{and} \quad N < A.$$

The first inequality implies, in view of Proposition 7, that we are in Case 3 (Section 10). Moreover, the third inequality, Proposition 9 and the definition of c_{22} (see after (22)) show that we cannot have $s = 0$, therefore we are in the real or complex case. Now the second and third inequality, in combination with (23) in the real case and (27) in the complex case, imply that

$$0 < |\Lambda_0| < c_{27}e^{-c_{16}A}, \tag{29}$$

where

$$c_{27} = \begin{cases} 1.39c_{21} & \text{in the real case} \\ 1.02c_{21} & \text{in the complex case} \end{cases}.$$

This inequality plays an important role in the so called real reduction step, which we apply to Λ_0 in Section 16. In that step use is made of both $A \leqslant K_0$ and $N \leqslant N_1$.

The whole reduction process can be repeated with N_1 in place of N_0 and $K_1 = \max\{A_1, N_1\}$ in place of K_0. Thus we will find in the second p-adic reduction step a bound $N_2 < N_1$ for N, that can be used in the second real reduction step to find a bound $A_2 < A_1$ for A. As long as a good reduction is achieved this way, we can go further with a third, fourth, etc. reduction step (see Section 17).

14. Preliminaries for the p-adic reduction step

In this section we give some preliminary remarks for the p-adic reduction step, that will be treated in the next section. For every $i \in \{1, \dots, v\}$ we consider the linear form Λ_i. We have (cf. Lemma 13)

$$\operatorname{ord}_{p_i}(\Lambda_i) = n_i h_i + v_i.$$

In general, ρ_i, λ_{il} $(l = 1, \dots, v)$, μ_{il} $(l = 1, \dots, r)$ and Λ_i belong to some finite extension $\mathbb{Q}_{p_i}(\phi)$ of $\mathbb{Q}_{p_i}$. For convenience in our notation we put

$$(\alpha_0, \alpha_1, \dots, \alpha_{v+r}) = (\rho_0, \lambda_{i1}, \dots, \lambda_{iv}, \mu_{i1}, \dots, \mu_{ir}).$$

Let $s = [\mathbb{Q}_{p_i}(\phi) : \mathbb{Q}_{p_i}]$, and let $G(t) \in \mathbb{Q}_{p_i}[t]$ be the minimal polynomial of ϕ over $\mathbb{Q}_{p_i}$. Then for $l = 0, 1, \dots, v + r$ we can write

$$\alpha_l = \alpha_{l0} + \alpha_{l1}\phi + \cdots + \alpha_{l,s-1}\phi^{s-1}, \quad \alpha_{l0}, \dots, \alpha_{l,s-1} \in \mathbb{Q}_{p_i},$$

and consequently

$$\Lambda_i = \Lambda_{i0} + \Lambda_{i1}\phi + \cdots + \Lambda_{i,s-1}\phi^{s-1}, \tag{30}$$

where for $k = 0, \dots, s - 1$

$$\Lambda_{ik} = \alpha_{0k} + \sum_{l=1}^{v} n_l \alpha_{lk} + \sum_{l=1}^{r} a_l \alpha_{v+l,k} \in \mathbb{Q}_{p_i}.$$

Now we consider the s p_i-adic conjugates of (30) and note that $\operatorname{ord}_{p_i}(\Lambda_i^{(l)})$ does not depend on l (see Section 4). We have

$$\begin{bmatrix} \Lambda_i^{(1)} \\ \vdots \\ \Lambda_i^{(s)} \end{bmatrix} = \begin{bmatrix} 1 & \phi^{(1)} & \cdots & \phi^{(1)s-1} \\ \vdots & \vdots & & \vdots \\ 1 & \phi^{(s)} & \cdots & \phi^{(s)s-1} \end{bmatrix} \begin{bmatrix} \Lambda_{i0} \\ \vdots \\ \Lambda_{i,s-1} \end{bmatrix}.$$

Hence there are γ_{lm} with $\mathrm{ord}_{p_i}(\gamma_{lm}) \geqslant 0$ such that

$$\begin{bmatrix} \Lambda_{i0} \\ \vdots \\ \Lambda_{i,s-1} \end{bmatrix} = \frac{1}{\prod\limits_{1 \leqslant m < l \leqslant s} (\phi^{(l)} - \phi^{(m)})} \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1s} \\ \vdots & & \vdots \\ \gamma_{s1} & \cdots & \gamma_{ss} \end{bmatrix} \begin{bmatrix} \Lambda_i^{(1)} \\ \vdots \\ \Lambda_i^{(s)} \end{bmatrix}.$$

It follows that

$$\mathrm{ord}_{p_i}(\Lambda_{il}) \geqslant \mathrm{ord}_{p_i}(\Lambda_i) - u_i, \tag{31}$$

where

$$u_i = \mathrm{ord}_{p_i}\left(\prod_{1 \leqslant m < l \leqslant s} (\phi^{(l)} - \phi^{(m)}) \right) = \frac{1}{2} \mathrm{ord}_{p_i}(\mathrm{discr}\, G(t)).$$

Hence, if $\mathrm{ord}_{p_i}(\Lambda_i)$ is large, then so are $\mathrm{ord}_{p_i}(\Lambda_{ik})$ for all $k = 0, 1, \ldots, s-1$. Now fix an arbitrary $l \in \{0, \ldots, s-1\}$, and let us proceed with Λ_{il}, which has the nice property of being in $\mathbb{Q}_{p_i}$ itself, instead of in the extension $\mathbb{Q}_{p_i}(\phi)$ (we owe this remark to J.-H. Evertse). Define $\xi_i \in \{\alpha_{1l}, \ldots, \alpha_{v+r,l}\}$ by

$$\mathrm{ord}_{p_i}(\xi_i) = \min_{1 \leqslant m \leqslant v+r} \mathrm{ord}_{p_i}(\alpha_{ml})$$

(if more than one choice is possible, any one will do; it will be convenient in the sequel to take ξ_i as one of the μ's). Note that $\mathrm{ord}_{p_i}(\alpha_{0l}) \geqslant \mathrm{ord}_{p_i}(\xi_i)$ is true when $\mathrm{ord}_{p_i}(\Lambda_{il}) \geqslant \mathrm{ord}_{p_i}(\xi_i)$. Put

$$\Lambda_i' = \frac{1}{\xi_i} \Lambda_{il},$$

and note that Λ_i' is a linear form with p_i-adic integral coefficients (in $\mathbb{Q}_{p_i}$), one of which is 1, involving the same unknown integers as Λ_i. Thus we can write

$$\Lambda_i' = -\beta_0 - b_1\beta_1 - \cdots - b_{v+r-1}\beta_{v+r-1} + b_{v+r},$$

where $(b_1, \ldots, b_{v+r})$ is a permutation of $(n_1, \ldots, n_v, a_1, \ldots, a_r)$, $\beta_0 = -\alpha_{0l}/\xi_i$, and each of $\beta_1, \ldots, \beta_{v+r-1} \in \mathbb{Z}_{p_i}$ is equal to a number of the form $-\alpha_{kl}/\xi_i$ for the proper index k. It is convenient to choose the permutation as follows: if $\xi_i = \mu_{ik}$, then take $(b_1, \ldots, b_{v+r}) = (n_1, \ldots, n_v, a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_r, a_k)$, and if $\xi_i = \lambda_{ik}$ then take $(b_1, \ldots, b_{v+r}) = (n_1, \ldots, n_{k-1}, n_{k+1}, \ldots, n_v, a_1, \ldots, a_r, n_k)$. In the former case let $v' = v$, in the latter case let $v' = v - 1$. Note that in view of (31) we have

$$\mathrm{ord}_{p_i}(\Lambda_i') \geqslant n_i h_i + l_i, \tag{32}$$

for $i = 1, \ldots, v$, with $l_i = v_i - u_i - \mathrm{ord}_{p_i}(\xi_i)$.

To conclude this section we like to point out and discuss two special cases. At the beginning of Section 6 we have assumed that $\mathscr{P}_i$ is nonempty, since otherwise the exponent z_i in (1) would be necessarily 'small'. This is equivalent to the fact that at least one of the polynomials $g_i(t) \in \mathbb{Q}_{p_i}[t]$ (see Section 3) is of the first degree.

The first special case is when at least three of the polynomials $g_i(t)$ have degree 1. Then we have chosen i_0, j, k in such a way that all the numbers that are involved in Λ_i are in $\mathbb{Q}_{p_i}$ itself (cf. Section 7). For the above discussion this implies $s = 1$, and thus $\Lambda_i = \Lambda_{i0}$. Thus in this case we don't need to work in a nontrivial extension $\mathbb{Q}_{p_i}(\phi)$ of $\mathbb{Q}_{p_i}$.

The second special case is when at most two of the polynomials $g_i(t)$ are of degree 1, but there is one of degree 2. Then we choose indices j, k such that $\theta^{(j)}$, $\theta^{(k)}$ are roots of that quadratic polynomial over $\mathbb{Q}_{p_i}$ (cf. Section 7). In such a case, $\mathbb{Q}_{p_i}(\phi) = \mathbb{Q}_{p_i}(\theta^{(j)}) = \mathbb{Q}_{p_i}(\theta^{(k)})$.

In this second special case, for any $\alpha, \beta \in \mathbb{Q}_{p_i}(\phi)$ we have

$$\log_{p_i} \frac{\alpha^{(k)}}{\alpha^{(j)}} \Big/ \log_{p_i} \frac{\beta^{(k)}}{\beta^{(j)}} \in \mathbb{Q}_{p_i}. \tag{33}$$

This follows from the fact that the nontrivial automorphism of $\mathbb{Q}_{p_i}(\phi)$, which interchanges j and k, multiplies the logarithms by -1. So their quotient is fixed by this automorphism, and this implies (33).

Because of property (33) we do not have to work with one of Λ_{i0}, Λ_{i1} (remember that $s = 2$), but we can work with Λ_i itself. Namely, now choose $\xi_i \in \{\lambda_{i1}, \ldots, \lambda_{iv}, \mu_{i1}, \ldots, \mu_{ir}\}$ with minimal p_i-adic order, and define $\Lambda_i' = (1/\xi_i)\Lambda_i$. In view of (33) and the definitions of ρ_i, the λ's and μ's (which indeed are p_i-adic logarithms of the quotient of a quadratic number over $\mathbb{Q}_{p_i}$ and its conjugate), the coefficients of Λ_i' are in $\mathbb{Z}_{p_i}$, and we can work with this Λ_i' as in the general case.

Note that if $n = 3$ we necessarily have one of the two special cases. In both special cases we can replace (32) by

$$\operatorname{ord}_{p_i}(\Lambda_i') = n_i h_i + l_i, \tag{34}$$

where $l_i = v_i - \operatorname{ord}_{p_i}(\xi_i)$.

14^{Ex} We took $\xi_1 = \mu_{12}$ (for $p_1 = 2$), and $\xi_i = \mu_{i1}$ for $p_i = 3, 5, 7$, so always $v' = v = 4$. Then $\operatorname{ord}_2(\xi_1) = 2$ and $\operatorname{ord}_{p_i}(\xi_i) = 1$ for $p_i = 3, 5, 7$. In view of (34) we have $\operatorname{ord}_{p_i}(\Lambda_i') = n_i + l_i$ for $i = 1, \ldots, 4$, with $l_1 = -2$, $l_2 = -1$, $l_3 = \begin{cases} 0 & \text{in Case I} \\ -2 & \text{in Cases III, V} \end{cases}$, $l_4 = -1$, under the condition $\operatorname{ord}_{p_i}(\Lambda_i') \geqslant 2$ for $i = 1$, $\operatorname{ord}_{p_i}(\Lambda_i') \geqslant 1$ for $i = 2, 3, 4$. From the Tables in Section 12^{Ex} we compute $\beta_0, \ldots, \beta_5$ in all the cases (which should be done to a much greater precision than presented here). For $i = 1$, so $p_1 = 2$, we have

$$\beta_0 = -\frac{\rho_1}{\mu_{12}}, \quad \beta_l = -\frac{\lambda_{1l}}{\mu_{12}} \ (l = 1, 2, 3, 4), \quad \beta_5 = -\frac{\mu_{11}}{\mu_{12}},$$

and for $i = 2, 3, 4$, so $p_i = 3, 5, 7$, we have

$$\beta_0 = -\frac{\rho_i}{\mu_{i1}}, \quad \beta_l = -\frac{\lambda_{il}}{\mu_{i1}} \ (l = 1, 2, 3, 4), \quad \beta_5 = -\frac{\mu_{i2}}{\mu_{i1}}.$$

Note that for $i = 1, 2, 4$ we are in the second special case, and for $i = 3$ we are in the first special case.

$p_1 = 2$	Case I	Case III	Case V
β_0	0.1110000100···	0.1010011010···	0.0010100011···
β_1	0.1011100010···		
β_2	0.0011000010···		
β_3	0.1010100100···	0.1011000101···	0.0111101100···
β_4	0.1101001001···		
β_5	0.0011011101···		

$p_2 = 3$	Case I	Case III	Case V
β_0	0.0202121002···	0.1012210010···	0.1212101101···
β_1	0.1122122101···		
β_2	0.1210012011···		
β_3	0.1112121212···	0.1010012002···	0.1100121201···
β_4	0.1102110002···		
β_5	0.0001121011···		

$p_3 = 5$	Case I	Case III	Case V
β_0	0.4302213223···	0.2123343114···	0.2241110022···
β_1	0.3403414014···	0.0213333412···	0.4204414122···
β_2	0.0140023031···	0.0312011101···	0.0223403411···
β_3	0.0331214022···	0.3002210013···	0.0004040304···
β_4	0.3401201111···	0.1024340340···	0.2004133143···
β_5	0.0402340030···	0.2030022001···	0.1420142114···

$p_4 = 7$	Case I	Case III	Case V
β_0	0.4522515064···	0.5540422123···	0.1246604142···
β_1	0.0332114423···		
β_2	0.4143654424···		
β_3	0.2334663553···	0.4314165054···	0.1025504035···
β_4	0.1354624005···		
β_5	0.4252341630···		

15. The p-adic reduction step

In this section $i \in \{1, \dots, v\}$ is fixed. Let $W_1, \dots, W_{v+r}$ be positive integers, called *weights*. Later in this section we will fix them. These weights are used to obtain an optimal balance between the various upper bounds for the different variables. We choose a positive integer m such that $p_i^m \prod_{j=1}^{v+r} W_j$ is of the size of K_0^{v+r}, but large enough (this 'large enough' will be explained after Proposition 15 below). For any $x \in \mathbb{Z}_{p_i}$ we denote by $x^{(m)}$ the unique rational integer in the interval $[0, p_i^m - 1]$ such that $\mathrm{ord}_{p_i}(x - x^{(m)}) \geqslant m$. We consider the lattice Γ_m generated by the column-vectors of the matrix

$$\mathscr{A}_m = \begin{bmatrix} W_1 & & \bigcirc & \\ & \ddots & & \\ \bigcirc & & W_{v+r-1} & \\ W_{v+r}\beta_1^{(m)} & \cdots & W_{v+r}\beta_{v+r-1}^{(m)} & W_{v+r}p_i^m \end{bmatrix}.$$

Put

$$\lambda = \frac{-\beta_0^{(m)} - b_1\beta_1^{(m)} - \cdots - b_{v+r-1}\beta_{v+r-1}^{(m)} + b_{v+r}}{p_i^m}$$

and

$$\mathbf{y} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ -W_{v+r}\beta_0^{(m)} \end{bmatrix} \in \mathbb{Z}^{v+r}.$$

LEMMA 14. *$n_i \geqslant (1/h_i)(m - l_i)$ if and only if*

$$\begin{bmatrix} W_1 b_1 \\ \vdots \\ W_{v+r} b_{v+r} \end{bmatrix} + \mathbf{y} \in \Gamma_m.$$

Proof of Lemma 14. Since

$$\mathscr{A}_m \begin{bmatrix} b_1 \\ \vdots \\ b_{v+r-1} \\ \lambda \end{bmatrix} = \begin{bmatrix} W_1 b_1 \\ \vdots \\ W_{v+r} b_{v+r} \end{bmatrix} + \mathbf{y},$$

this point is a lattice point if and only if $\lambda \in \mathbb{Z}$, which is equivalent to

$$\mathrm{ord}_{p_i}(-\beta_0^{(m)} - b_1\beta_1^{(m)} - \cdots - b_{v+r-1}\beta_{v+r-1}^{(m)} + b_{v+r}) \geqslant m.$$

In view of $\mathrm{ord}_{p_i}(\beta_j^{(m)} - \beta_j) \geqslant m$ for $j = 0, \ldots, v+r$ this is equivalent to

$$\mathrm{ord}_{p_i}(-\beta_0 - b_1\beta_1 - \cdots - b_{v+r-1}\beta_{v+r-1} + b_{v+r}) \geqslant m,$$

i.e. $\mathrm{ord}_{p_i}(\Lambda_i') \geqslant m$, which, by (32) (or (34) as the case may be) proves the lemma. □

Now put

$$l(\Gamma_m, \mathbf{y}) = \begin{cases} \min\limits_{\mathbf{x} \in \Gamma_m \setminus \{\mathbf{0}\}} |\mathbf{x}| & \text{if } \mathbf{y} = \mathbf{0} \\ \min\limits_{\mathbf{x} \in \Gamma_m} |\mathbf{x} - \mathbf{y}| & \text{if } \mathbf{y} \neq \mathbf{0} \end{cases}.$$

By the LLL-algorithm (see [LLL, Fig. 1], and [dW1, Fig. 1] for an 'integral version' of it), we can compute a so-called reduced basis $\mathbf{c}_1, \ldots, \mathbf{c}_{v+r}$ for Γ_m. Roughly speaking, this is an 'almost orthogonal' basis. We can also view it as a basis for $\mathbb{R}^{v+r}$, and, in case that $\mathbf{y} \neq 0$, we can express

$$\mathbf{y} = s_1\mathbf{c}_1 + \cdots + s_{v+r}\mathbf{c}_{v+r}, \quad s_1, \ldots, s_{v+r} \in \mathbb{R}.$$

For the actual computation of the s_j, see [dW1, Section 3.8], It can be proved that

$$l(\Gamma_m, \mathbf{y}) \geqslant \begin{cases} 2^{-(v+r-1)/2}|\mathbf{c}_1| & \text{if } \mathbf{y} = 0 \text{ ([LLL, Proposition 1.11])} \\ 2^{-(v+r-1)/2}\|s_{j_0}\|\,|\mathbf{c}_1| & \text{if } \mathbf{y} \neq 0 \text{ ([dW1, Lemma 3.5])} \end{cases}, \tag{35}$$

where $j_0 = \max\{j \in \{1, \ldots, v+r\} | s_j \notin \mathbb{Z}\}$, and $\|\cdot\|$ denotes the distance to the nearest integer. Note that the above set of indices j is not empty when $\mathbf{y} \neq 0$. Indeed, if it were, then $s_j \in \mathbb{Z}$ for every $j = 1, \ldots, v+r$, hence $\mathbf{y} \in \Gamma_m$ and rational integers $z_1, \ldots, z_{v+r}$ would exist such that

$$\mathbf{y} = \mathscr{A}_m \begin{bmatrix} z_1 \\ \vdots \\ z_{v+r} \end{bmatrix}.$$

But then $z_1 = \cdots = z_{v+r-1} = 0$ and $-\beta_0^{(m)} = z_{v+r}p_i^m$, and since by definition $\beta_0^{(m)} \in [0, p_i^m - 1]$, we would conclude $\beta_0^{(m)} = 0$, which contradicts $\mathbf{y} \neq 0$. Thus the lower bound for $l(\Gamma_m, \mathbf{y})$ given in (35) is always positive.

Now we fix the weights for the remainder of this section (but in later sections we might wish to make different choices for these weights):

$$W_1 = \cdots = W_{v'} = W, \quad W_{v'+1} = \cdots = W_{v+r-1} = 1,$$

$$W_{v+r} = \begin{cases} 1 & \text{if } v' = v \\ W & \text{if } v' = v-1 \end{cases},$$

where W is a convenient positive integer close to K_0/N_0 (e.g. with $K_0 = 10^{50}$ and $N_0 = 3 \times 10^{40}$ it is sufficient to take $W = 3 \times 10^9$). For the definition of v', see just before (32). Put

$$Q = vW^2N_0^2 + rK_0^2.$$

We have the following result.

PROPOSITION 15. *If* $l(\Gamma_m, \mathbf{y}) > \sqrt{Q}$ *then* $n_i < (1/h_i)(m - l_i)$.

Proof of Proposition 15. Suppose $n_i \geqslant (1/h_i)(m-l_i)$. Then, by Lemma 14,

$$\begin{bmatrix} W_1 b_1 \\ \vdots \\ W_{v+r} b_{v+r} \end{bmatrix} + \mathbf{y} \in \Gamma_m.$$

Therefore

$$W^2(b_1^2 + \cdots + b_{v'}^2) + b_{v'+1}^2 + \cdots + b_{v+r-1}^2 + W_{v+r}^2 b_{v+r}^2 \geqslant l(\Gamma_m, \mathbf{y})^2.$$

By the definitions of $b_1, \ldots, b_{v+r}$ and $W_1, \ldots, W_{v+r}$ for the two cases $v' = v$, $v-1$, and by the definitions of N_0 and K_0, we obtain

$$l(\Gamma_m, \mathbf{y})^2 \leqslant vW^2N_0^2 + rK_0^2 = Q,$$

which contradicts the hypothesis. □

Clearly one can prove a similar proposition when the weights are chosen differently. In practice one can expect that the hypothesis of Proposition 15 is highly probable if m is taken to be of the indicated size, and large enough. Indeed, the volume of the parallelepiped spanned by $\mathbf{c}_1, \ldots, \mathbf{c}_{v+r}$ is equal to $\det \mathscr{A}_m = p_i^m \prod_{j=1}^{v+r} W_j$. On the other hand, since $\mathbf{c}_1, \ldots, \mathbf{c}_{v+r}$ constitute an almost orthogonal basis, the above parallelepiped has a volume of the size of $|\mathbf{c}_1| \cdot \cdots \cdot |\mathbf{c}_{v+r}|$, which can be expected to be of the size of $|\mathbf{c}_1|^{v+r}$. Thus $|\mathbf{c}_1|^{v+r}$ is of the size of $\det \mathscr{A}_m$, which, by the choice of m, is of the size of K_0^{v+r}. From this we see that $|\mathbf{c}_1|$ is of the size of K_0. By (35) we see that also $l(\Gamma_m, \mathbf{y})$ is of that size, except in the case that $\|s_{j_0}\|$ is extremely small. This situation is unlikely to happen, but if it does, then one can apply [dW1, Lemma 3.6] in place of [dW1,

Lemma 3.5], which hopefully will give a better lower bound for $l(\Gamma_m, \mathbf{y})$ that is of the size of K_0.

In practice, we take m such that $p_i^m \prod_{j=1}^{v+r} W_j$ be somewhat larger than K_0^{v+r}, and if with the chosen value for m the hypothesis of Proposition 15 is not fulfilled, then we should take m somewhat larger than the previous one, and recompute the reduced basis for the new lattice Γ_m. Note that in such a case we can take advantage of the computations already done with the not large enough m, as follows. Suppose that we have computed, using the LLL-algorithm, the matrices $\mathscr{B}_m$, $\mathscr{U}_m$ for a certain m such that $\mathscr{B}_m = \mathscr{A}_m \mathscr{U}_m$, where the columns of $\mathscr{B}_m$ are a reduced basis for Γ_m, and suppose that we want a reduced basis for $\Gamma_{m'}$ with $m' > m$. Then we should use $\mathscr{A}_{m'} \mathscr{U}_m$ as input for the second application of the LLL-algorithm, rather than $\mathscr{A}_{m'}$. This will save a lot of computation time.

Note that the upper bound $(1/h_i)(m - l_i)$ for n_i is of the size of $(v+r)\log K_0/\log p_i$, as required. Thus, if we repeat the above reduction process for every $i = 1, \ldots, v$, then we get an upper bound N_1 for N, which is of the size of $\log K_0$. This usually is considerably smaller than N_0.

15[Ex] Based on $K_0 = N_0 = 9.844 \times 10^{49}$ we took $W_1 = \cdots = W_6 = 1$. We took m as in the following Table, and computed the $\beta_j \in \mathbb{Z}_{p_i}$ that constitute most of the input for the LLL-algorithm, to the desired precision. In order to be able to do this we had to compute many p-adic algebraic numbers and their logarithms to a high precision. These computations are straightforward but laborious (we used Hensel's Lemma = the p-adic Newton method, the power series expansion for the p-adic logarithm, and a multiple-precision package for p-adic computations written by ourselves). Then we applied the integral version [dW1, Fig. 1] of the LLL-algorithm to each of the 12 lattices, and obtained data as given in the following Table. Here, in all cases $j_0 = 6$.

i	p_i	m	$p_i^{m/6}$	Case	$\lvert c_1 \rvert >$	$\lVert s_6 \rVert >$	$l(\Gamma_m, \mathbf{y}) >$
1	2	1152	$6.27\cdots \times 10^{57}$	I	6.21609×10^{57}	0.36268	3.98541×10^{56}
				III	5.48328×10^{57}	0.00646	6.26946×10^{54}
				V	5.22452×10^{57}	0.46402	4.28559×10^{56}
2	3	672	$2.73\cdots \times 10^{53}$	I	3.05484×10^{53}	0.46487	2.51042×10^{52}
				III	2.29269×10^{53}	0.32858	1.33175×10^{52}
				V	2.14153×10^{53}	0.38535	1.45883×10^{52}
3	5	480	$8.27\cdots \times 10^{55}$	I	4.83786×10^{55}	0.40713	3.48191×10^{54}
				III	1.09351×10^{56}	0.48912	9.45521×10^{54}
				V	7.01884×10^{55}	0.22653	2.81079×10^{54}
4	7	384	$1.21\cdots \times 10^{54}$	I	1.16289×10^{54}	0.29605	6.08600×10^{52}
				III	9.57912×10^{53}	0.44165	7.47891×10^{52}
				V	8.63845×10^{53}	0.26302	4.01652×10^{52}

In all cases the hypothesis of Proposition 15, being $l(\Gamma_m, \mathbf{y}) \geqslant \sqrt{6} K_0 = 2.41127\cdots \times 10^{50}$, is amply fulfilled (in fact, we could have chosen somewhat smaller m's). Hence Proposition 15, with $l_1 = -2$, $l_2 = -1$, $l_3 = \begin{cases} 0 & \text{in Case I} \\ -2 & \text{in Cases III, V} \end{cases}$, $l_4 = -1$, $h_1 = h_2 = h_3 = h_4 = 1$, and m as in the Table above,

yields

$$n_1 \leqslant 1153,\ n_2 \leqslant 672,\ n_3 \leqslant 481,\ n_4 \leqslant 384,$$

and it follows that $N_1 = 1153$ is the new upper bound for N, replacing $N_0 = 9.844 \times 10^{49}$. Note that N_1 is indeed of the size of $6 \log K_0/\log 2 = 996.4\ldots$.

16. The real reduction step

As we have noted in Section 13, this step is not made in the totally complex case. Thus, we suppose that we are in the real or complex case, hence Λ_0 is defined (see also near the end of section 12). In Section 13 we have also noted that the real reduction step is essentially needed in practice only when

$$A > c_{22} \quad \text{and} \quad N < A \quad \text{and} \quad c_{18} + c_{17}N \leqslant A,$$

from which it follows (see (29)) that

$$0 < |\Lambda_0| < c_{27}e^{-c_{16}A}. \tag{36}$$

Thus in this section we suppose that all the above inequalities hold. Moreover, we are free to choose c_{16} different from earlier choices (such as in Section 11), as long as $0 < c_{16} < c_{15}/(n-1)$, and the constants depending on it (c_{17}, c_{18}, c_{22}) are changed accordingly.

Let $i_0 \in \{1, \ldots, s\}$ be fixed. In the real case, we again choose positive integers $W_1, \ldots, W_{v+r-1}$ as weights (note that now W_{v+r} is not defined). Let C be a positive integer such that $C \prod_{j=1}^{v+r-1} W_j$ is of the size of K_0^{v+r}, and C must be large enough (C is more or less the analogue of m of Section 15). Put

$$\phi_i = [C\lambda_{0i}]\ (i = 1, \ldots, v),\ \psi_i = [C\mu_{0i}]\ (i = 1, \ldots, r),\ \phi_0 = [C\rho_0],$$

where $[\cdot]$ denotes (e.g.) rounding off towards zero, i.e.

$$[x] = \begin{cases} \lfloor x \rfloor & \text{if } x \geqslant 0 \\ \lceil x \rceil & \text{if } x < 0 \end{cases}.$$

We consider the lattice Γ generated by the column vectors of the matrix

$$\mathscr{A} = \begin{bmatrix} W_1 & & & & & & \\ & \ddots & & & \bigcirc & & \\ \vdots & & W_v & & & & \\ & \bigcirc & & W_{v+1} & & & \\ \vdots & & \vdots & \vdots & \ddots & & \\ & & & & & W_{v+r-1} & \\ \phi_1 & \cdots & \phi_v & \psi_1 & \cdots & \psi_{r-1} & \psi_r \end{bmatrix}.$$

Its determinant is approximately $C\mu_{0,r}\prod_{j=1}^{v+r-1} W_j$, which is of the size of K_0^{v+r} in view of the choice of C. By the LLL-algorithm we compute a reduced basis $\mathbf{c}_1, \ldots, \mathbf{c}_{v+r}$ of Γ. We put

$$\mathbf{y} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ -\phi_0 \end{bmatrix} \in \mathbb{Z}^{v+r},$$

and as in Section 15 (but now with Γ in place of Γ_m) we define $l(\Gamma, \mathbf{y})$. Note that (35) still holds with Γ replaced by Γ_m. As explained in the remark following Proposition 15, it is reasonable to expect that $l(\Gamma, \mathbf{y})$ is of the size of K_0. If it is too small to fulfill the hypothesis of Proposition 16, we should try again with a somewhat larger value for C.

Now we fix the weights for the remainder of this section (but in later sections we might wish to make different choices for these weights):

$$W_1 = \cdots = W_v = W, \quad W_{v+1} = \cdots = W_{v+r-1} = 1,$$

where W is a convenient positive integer close to K_0/N_1. Thus C is of the size of $N_1^v K_0^r$. Let $\varepsilon = 0$ if $\rho_0 = 0$, and $\varepsilon = 1$ if $\rho_0 \neq 0$. Put

$$R = vN_1 + rK_0 + \varepsilon, \quad S = vW^2N_1^2 + (r-1)K_0^2.$$

Now we have the following result, which is the real analogue of Proposition 15.

PROPOSITION 16. *If* $l(\Gamma, \mathbf{y}) \geqslant \sqrt{R^2 + S}$ *then*

$$H = A \leqslant \frac{1}{c_{16}} \{\log c_{27} + \log C - \log(\sqrt{l(\Gamma, \mathbf{y})^2 - S} - R)\}.$$

Proof of Proposition 16. Consider the lattice point

$$\mathbf{x} = \mathscr{A} \begin{bmatrix} n_1 \\ \vdots \\ n_v \\ a_1 \\ \vdots \\ a_r \end{bmatrix}, \text{ with } \mathbf{x} - \mathbf{y} = \begin{bmatrix} Wn_1 \\ \vdots \\ Wn_v \\ a_1 \\ \vdots \\ a_{r-1} \\ \Phi \end{bmatrix},$$

where

$$\Phi = \phi_0 + n_1\phi_1 + \cdots + n_v\phi_v + a_1\psi_1 + \cdots + a_r\psi_r.$$

Then

$$|\Phi - C\Lambda_0| \leqslant |C\rho_0 - [C\rho_0]| + \sum_{i=1}^{v} n_i |C\lambda_{0,i} - [C\lambda_{0,i}]| + \sum_{i=1}^{r} |a_i||C\mu_{0,i} - [C\mu_{0,i}]| \leqslant R.$$

Hence, also in view of (36),

$$|\Phi| \leqslant Cc_{27}e^{-c_{16}A} + R. \tag{37}$$

Since $\mathbf{x} \in \Gamma$, we have, by the definition of $l(\Gamma, \mathbf{y})$, and in view of (37),

$$\begin{aligned} l(\Gamma, \mathbf{y})^2 &\leqslant |\mathbf{x} - \mathbf{y}|^2 = W^2(n_1^2 + \cdots + n_v^2) + a_1^2 + \cdots + a_{r-1}^2 + \Phi^2 \\ &\leqslant S + (Cc_{27}e^{-c_{16}A} + R)^2, \end{aligned}$$

from which the claimed upper bound for $H = A$ immediately follows. □

Clearly one can prove a similar result for different choices of the weights. The reduction process described above must be performed for all $i_0 = 1, \ldots, s$. The so obtained new upper bound for A is essentially of the size of $r \log K_0$, but holds only under the assumptions mentioned in the beginning of this section. Thus in the general situation we obtain the following upper bound A_1 for A, which will be considerably smaller than K_0:

$$A \leqslant A_1 = \max\{\text{upper bound from Proposition 16}, c_{18} + c_{17}N_1, c_{22}\}.$$

From this expression it is easy to choose an optimal value for the parameter c_{16}.

As a consequence of the reduced bounds for A and N we have a new upper bound K_1 for H, improving on K_0, namely

$$H \leqslant K_1 = \max\{N_1, A_1\},$$

which is expected to be of essentially the size of $\log K_0$.

In the complex case we work analogously. The only difference in this case is that, in view of the appearance of the variable a_0 (see Section 10 after (27)), we must work in a lattice of dimension $v + r + 1$, and K_0 must be replaced by $\frac{1}{2}(1 + v + r)K_0$. Note that here one needs to approximate $\pi = 3.14159\ldots$ to sufficiently high precision.

16^{Ex} Based on $K_0 = 9.844 \times 10^{49}$ and $N_1 = 1153$ we took $W_1 = \cdots = W_4 = 9 \times 10^{46}$, $W_5 = 1$, $C = 10^{132}$. We computed the input for the LLL-algorithm to the desired precision. In order to be

able to do this we had to compute many real algebraic numbers and their logarithms to a high precision. These computations are straightforward but laborious (we used the real Newton method, the power series expansion for $\log(1+x)$, and a multiple-precision package for real computations written by ourselves). Then we applied the integral version [dW1, Fig. 1] of the LLL-algorithm to each of the 9 lattices, and obtained data as given in the following Table. Here, in all cases $j_0 = 6$.

i_0	Case	$\|c_1\|>$	$\|s_6\|>$	$l(\Gamma, y)>$
1	I	1.71179×10^{53}	0.33615	1.01720×10^{52}
	III	1.63407×10^{53}	0.16228	4.68799×10^{51}
	V	2.01731×10^{53}	0.18308	6.52922×10^{51}
2	I	3.15947×10^{53}	0.26388	1.47383×10^{52}
	III	3.74556×10^{53}	0.44774	2.96465×10^{52}
	V	2.81549×10^{53}	0.31138	1.54981×10^{52}
3	I	3.13799×10^{53}	0.00946	5.24957×10^{50}
	III	3.00766×10^{53}	0.34886	1.85485×10^{52}
	V	2.80133×10^{53}	0.37839	1.87383×10^{52}

Either we have $H < c_{18} + c_{17}N_1 < \dfrac{28207.757}{5.812 - 2c_{16}}$, or we can apply Proposition 16. We have $R < 1.969 \times 10^{50}$, $S < 5.277 \times 10^{100}$, thus in all cases the hypothesis of Proposition 16 is fulfilled, since $l(\Gamma, y) > 3.026 \times 10^{50} > \sqrt{R^2 + S}$. Hence using $l(\Gamma, y) > 5.24957 \times 10^{50}$ we obtain from Proposition 16 that for this case $H < \dfrac{190.52800}{c_{16}}$. We find the optimal c_{16} from putting

$$\frac{28207.757}{5.812 - 2c_{16}} = \frac{190.52800}{c_{16}},$$

and this gives $c_{16} = 0.0387336\ldots$, and thus $H < 4918.928\ldots$. Hence the results from this and the preceding section yield $H \leqslant K_1 = 4918$.

17. Further reduction and the Fincke and Pohst method

As announced in Section 13, we can repeat the reduction process described in Sections 15 and 16, to reduce the upper bounds for N and A even further. It is often useful in the second and further reduction steps to be more careful in the estimations. Let us for simplicity assume that $v' = v$, since the case $v' = v - 1$ can be dealt with analogously. Then $(b_1, \ldots, b_{v+r}) = (n_1, \ldots, n_v, a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_r, a_k)$.

Assume that from the previous p-adic and real reduction steps, being the lth in succession, we have upper bounds $N_{l1}, \ldots, N_{lv}, A_l$ for $n_1, \ldots, n_v, A$ respectively. Then $N_l = \max_j N_{lj}$ is an upper bound for N, and $K_l = \max\{N_l, A_l\}$ is an upper

bound for H. To obtain bounds $N_{l+1,1},\dots,N_{l+1,v}$ we perform a p-adic reduction step for each $p = p_1,\dots,p_v$ as follows.

We choose weights as follows: for $j = 1,\dots,v$ let W_j be (e.g.) the nearest integer >0 to A_l/N_{lj}, and let $W_{v+1} = \cdots = W_{v+r} = 1$ (here the hidden assumption is that $A_l > N_{lj}$; if that is not the case then $W_{v+1},\dots,W_{v+r}$ should be adjusted such that a good balance is obtained). Let the lattice Γ_m and the vector $\mathbf{y}$ be defined as in Section 15, and now put

$$Q = W_1^2N_{l1}^2 + \cdots + W_v^2N_{lv}^2 + rA_l^2.$$

Then the statement of Proposition 15 is obviously true. The p-adic reduction step as described in Section 15, applied for $p = p_1,\dots,p_v$, now gives new upper bounds $N_{l+1,1},\dots,N_{l+1,v}$ for $n_1,\dots,n_v$. With small computational effort one can find for each p_i, by trying in a certain range, the smallest m such that the hypothesis of Proposition 15 is fulfilled. This gives the optimal upper bound for n_i.

Subsequently we perform a real reduction step. Choose the weights W_j for $j = 1,\dots,v$ to be the nearest integer >0 to $A_l/N_{l+1,j}$, and $W_{v+1} = \cdots = W_{v+r-1} = 1$. Then Proposition 16 with Γ, ε and $\mathbf{y}$ as in Section 16, and with

$$R = N_{l+1,1} + \cdots + N_{l+1,v} + rA_l + \varepsilon,$$
$$S = W_1^2N_{l+1,1}^2 + \cdots + W_v^2N_{l+1,v}^2 + (r-1)A_l^2,$$

is obviously true. Application of the real reduction step as described in Section 16 now gives a new upper bound A_{l+1} for A. Again, an optimal C can be found by trial and error.

In each reduction step the final upper bound K_{l+1} for H follows as indicated at the end of Section 16. Here, c_{16} can be chosen differently at each reduction step. The whole procedure can be repeated until no more improvement is accomplished.

It is possible to considerably reduce the bounds thus obtained even further by taking a much more detailed look at the approximation lattices Γ_m and Γ. A useful tool here is the algorithm of Fincke and Pohst [FP] for determining the lattice points in a given lattice within a certain distance from the origin. Since this much more refined reduction technique might use a large amount of computation time (a large number of lattice points might be found as candidates for solutions), it is advisable to use it only after the cruder but faster reduction steps as described above have been pursued until no further improvement is apparent.

For the p-adic reduction step the technique works as follows (again assuming $v' = v$). For the weights W_j for $j = 1,\dots,v$ we now take (e.g.) the integer nearest

to $2A_l/N_{lj}$, and further $W_{v+1} = \cdots = W_{v+r} = 1$. Put

$$\mathbf{y}' = \begin{bmatrix} \lfloor \frac{1}{2} W_1 N_{l1} \rfloor \\ \vdots \\ \lfloor \frac{1}{2} W_v N_{lv} \rfloor \\ 0 \\ \vdots \\ 0 \\ -\beta_0^{(m)} \end{bmatrix}.$$

Let $\mathbf{s} \in \mathbb{R}^{v+r}$ be defined by $\mathbf{y}' = \mathscr{B}\mathbf{s}$, where $\mathscr{B}$ is the matrix with the reduced basis $\mathbf{c}_1, \ldots, \mathbf{c}_{v+r}$ as columns. Choose $\mathbf{t} \in \mathbb{Z}^{v+r}$ such that $|t_i - s_i| = 1$ for every $i = 1, \ldots, v + r$ and $|\mathscr{B}\mathbf{t} - \mathbf{y}'|$ is minimal. Then most likely $\mathscr{B}\mathbf{t}$ is the lattice point nearest to $\mathbf{y}'$. With λ as in Section 15 and the conventions and notations as adopted just before (32), we have

$$\mathbf{z} = \mathscr{A}_m \begin{bmatrix} n_1 \\ \vdots \\ n_v \\ a_1 \\ \vdots\# \\ a_r \\ \lambda \end{bmatrix} = \begin{bmatrix} W_1 n_1 - \lfloor \frac{1}{2} W_1 N_{l1} \rfloor \\ \vdots \\ W_v n_v - \lfloor \frac{1}{2} W_v N_{lv} \rfloor \\ a_1 \\ \vdots\# \\ a_r \\ a_k \end{bmatrix} + \mathbf{y}'$$

(where $\#$ means: a_k omitted), which is a lattice point, since $\lambda \in \mathbb{Z}$ (cf. the first lines of the proof of Lemma 14). By $0 \leqslant n_i \leqslant N_{li}$ we have

$$|W_i n_i - \lfloor \tfrac{1}{2} W_i N_{li} \rfloor| \leqslant \lceil \tfrac{1}{2} W_i N_{li} \rceil.$$

Put $\mathbf{u} = \mathbf{z} - \mathscr{B}\mathbf{t}$, then also $\mathbf{u} \in \Gamma_m$, and

$$|\mathbf{u}| \leqslant \sqrt{\lceil \tfrac{1}{2} W_1 N_{l1} \rceil^2 + \cdots + \lceil \tfrac{1}{2} W_v N_{lv} \rceil^2 + r A_l^2} + |\mathscr{B}\mathbf{t} - \mathbf{y}'|.$$

Thus, upper bound for $|\mathbf{u}|$ is a constant, so the algorithm of Fincke and Pohst [FP] can be applied to find all the points $\mathbf{u}$ that satisfy this relation. For each $\mathbf{u}$ the corresponding $n_1, \ldots, n_v, a_1, \ldots, a_r$ can be easily found, and this candidate solution should be tested further (see below). After all the candidates have been tested, we can conclude that apart from a few explicitly known ones, the solutions satisfy $n_i < (1/h_i)(m - l_i)$, and we have found an improvement of the upper bound for n_i.

Note that in the above process, if we have performed the p-adic reduction step for some of the p_i, we can, instead of the old bound N_{li}, use the corresponding

improved bound $N_{l+1,i}$ for n_i in the subsequent applications of the process for the other p_i's.

In the real reduction step we may work as follows. Again let W_j for $j = 1, \ldots, v$ be the nearest integer > 0 to $2A_l/N_{l+1,j}$, and $W_{v+1} = \cdots = W_{v+r-1} = 1$, with all other notations below as in Section 16, if not explicitly redefined. Consider the lattice Γ for some C, and the vector

$$\mathbf{y}' = \begin{bmatrix} \lfloor \frac{1}{2} W_1 N_{l+1,1} \rfloor \\ \vdots \\ \lfloor \frac{1}{2} W_v N_{l+1,v} \rfloor \\ 0 \\ \vdots \\ 0 \\ -\phi_0 \end{bmatrix}.$$

Let $\mathbf{s}$, $\mathbf{t}$, $\mathscr{B}$ be as above. Consider the lattice point

$$\mathbf{z} = \mathscr{A} \begin{bmatrix} n_1 \\ \vdots \\ n_v \\ a_1 \\ \vdots \# \\ a_r \\ a_k \end{bmatrix} = \begin{bmatrix} W_1 n_1 - \lfloor \frac{1}{2} W_1 N_{l+1,1} \rfloor \\ \vdots \\ W_v n_v - \lfloor \frac{1}{2} W_v N_{l+1,v} \rfloor \\ a_1 \\ \vdots \# \\ a_r \\ \Phi \end{bmatrix} + \mathbf{y}'.$$

Put $\mathbf{u} = \mathbf{z} - \mathscr{B}\mathbf{t}$, which is a lattice point with

$$|\mathbf{u}| \leqslant |\mathbf{z} - \mathbf{y}'| + |\mathscr{B}\mathbf{t} - \mathbf{y}'|.$$

Let R be as before, and now let

$$S = \lceil \tfrac{1}{2} W_1 N_{l+1,1} \rceil^2 + \cdots + \lceil \tfrac{1}{2} W_v N_{l+1,v} \rceil^2 + (r-1) A_l^2 .$$

Let $D > \sqrt{R^2 + S}$ be some convenient number. We distinguish two cases.

- If $|\mathbf{z} - \mathbf{y}'| \leqslant D$ then all lattice points $\mathbf{u}$ satisfying the inequality $|\mathbf{u}| < D + |\mathscr{B}\mathbf{t} - \mathbf{y}'|$ can be computed by the algorithm of Fincke and Pohst, and tested.
- Otherwise we can apply Proposition 16, with $l(\Gamma, \mathbf{y})$ replaced by D and with S as given above, and thus obtain a new upper bound for A.

In this way we will find a new upper bound for H that holds for all solutions

apart from a few explicitly known ones. We may repeat the whole procedure, decreasing m (in the p-adic step) and C (in the real step) little by little (not too much at a time, in order to limit the number of lattice points to be tested), and hopefully we will reach a final upper bound for N and A that is small enough to admit e.g. enumeration techniques.

To conclude this section we describe how we can test a candidate solution in a way that rules out non-solutions at an early stage. We start by checking (34) for $i = 1, \ldots, v$, and in case of failure we take

$$\mathrm{ord}_{p_i}(\Lambda_i) = n_i h_i + v_i$$

for $i = 1, \ldots, v$ (compare Lemma 13). This test is easy in practice: the Λ_i can be easily computed up to the desired precision because all its ingredients have already been computed to a very high precision.

It is not guaranteed that all candidate solutions that pass this test are solutions. Therefore one subsequently has to perform another test, such as checking (12), or the vanishing of the coefficients of $\theta^2, \ldots, \theta^{n-1}$ in the right hand side of (11). Such a test can be performed up to a certain precision in p-adic and real form before it is applied with exact computations. Thus a series of tests is available, of increasing computational complexity, but hopefully needed for a rapidly decreasing number of candidates only.

17^{Ex} For the second p-adic reduction step we took $W_1 = 4$, $W_2 = 7$, $W_3 = 10$, $W_4 = 13$. We increased m with steps of 1, in the ranges indicated below, until $l(\Gamma_m, \mathbf{y}) > \sqrt{Q} = 11824.879\ldots$, since $Q = 4^2 1153^2 + 7^2 672^2 + 10^2 481^2 + 13^2 384^2 + 2 \cdot 4918^2$. We used the reduced basis of Γ_{m-1} to precompute the input for the reduction of the basis of Γ_m, as indicated near the end of Section 15. We found:

p	Case	range for m	$\lvert\mathbf{c}_1\rvert >$	$\lVert s_6 \rVert >$	$l(\Gamma_m, \mathbf{y}) >$
2	I	84– 97	334824	0.21192	12543
	III	84–104	303877	0.47593	25566
	V	84–100	386457	0.17618	12036
3	I	49– 60	308427	0.42982	23434
	III	49– 58	145737	0.46329	11935
	V	49– 60	220651	0.38291	14935
5	I	35– 42	230930	0.47395	19348
	III	35– 42	210908	0.37384	13938
	V	35– 40	182977	0.47108	15237
7	I	28– 35	253880	0.36187	16240
	III	28– 35	261805	0.27181	12579
	V	28– 34	144298	0.48438	12355

The conclusion is:

$$n_1 \leqslant 105, \quad n_2 \leqslant 60, n_3 \leqslant 43, n_4 \leqslant 35,$$

hence $N_2 = 105$.

For the second real reduction step we took $W_1 = 47$, $W_2 = 82$, $W_3 = 114$, $W_4 = 141$. We started with $C = 10^{21}$, increasing it by a factor 10 until we could find an upper bound for A for some optimal c_{16}, applying either $H < c_{18} + c_{17}N_2 = \dfrac{2578.917}{5.812 - 2c_{16}}$ or Proposition 16. We thus obtained:

i_0	Case	final C	$\lvert c_1\rvert >$	$\lVert s_6\rVert >$	$l(\Gamma, y) >$	c_{16}	$H \leqslant$
1	I	10^{24}	211427	0.43513	16263	0.10940…	461
	III	10^{28}	1052952	0.35472	66027	0.12154…	463
	V	10^{25}	363139	0.27984	17964	0.11258…	461
2	I	10^{23}	175905	0.48364	15039	0.10963…	461
	III	10^{26}	649285	0.34402	39486	0.11339…	461
	V	10^{24}	281100	0.44227	21977	0.10615…	460
3	I	10^{23}	236851	0.48709	20394	0.10182…	459
	III	10^{24}	310082	0.34395	18853	0.10728…	460
	V	10^{27}	861423	0.13577	20675	0.12092…	462

The conclusion is: $H \leqslant 463$.

For the third p-adic reduction step we took $W_1 = 4$, $W_2 = 7$, $W_3 = 10$, $W_4 = 13$. We increased m until $l(\Gamma_m, y) > \sqrt{Q} = 1083.265\ldots$, since $Q = 4^2105^2 + 7^260^2 + 10^243^2 + 13^235^2 + 2 \cdot 463^2$. We found:

p	Case	range for m	$\lvert c_1\rvert >$	$\lVert s_6\rVert >$	$l(\Gamma_m, y) >$
2	I	72–75	17469	0.44524	1375
	III	72–75	22927	0.39308	1593
	V	72–78	37980	0.31137	2090
3	I	42–45	13985	0.45183	1117
	III	42–54	79063	0.22715	3174
	V	42–48	26150	0.47372	2189
5	I	30–33	24452	0.35949	1553
	III	30–35	41524	0.37149	2727
	V	30–33	20656	0.32888	1200
7	I	24–26	14672	0.46797	1213
	III	24–26	16753	0.42145	1248
	V	24–30	52147	0.47753	4402

The conclusion is:

$$n_1 \leqslant 79, \quad n_2 \leqslant 54, \quad n_3 \leqslant 36, \quad n_4 \leqslant 30,$$

hence $N_3 = 79$.

For the third real reduction step we took $W_1 = 6$, $W_2 = 9$, $W_3 = 13$, $W_4 = 15$. We started with $C = 10^{18}$, increasing it by a factor 10 until we could find an upper bound for A for some optimal c_{16}, applying either $H < c_{18} + c_{17}N_3 = \dfrac{1943.087}{5.812 - 2c_{16}}$ or Proposition 16. We thus obtained:

i_0	Case	final C	$\lvert\mathbf{c}_1\rvert >$	$\lVert s_6\rVert >$	$l(\Gamma, \mathbf{y}) >$	c_{16}	$H \leqslant$
1	I	10^{24}	42528	0.41517	3121	0.14355···	351
	III	10^{24}	54327	0.47110	4524	0.14195···	351
	V	10^{25}	42622	0.37629	2835	0.15025···	352
2	I	10^{22}	19216	0.48374	1643	0.13800···	350
	III	10^{21}	20966	0.47450	1758	0.12979···	349
	V	10^{24}	52446	0.44227	4100	0.14234···	351
3	I	10^{23}	40201	0.42533	3022	0.13747···	350
	III	10^{23}	49989	0.34395	3039	0.13744···	350
	V	10^{24}	63098	0.30391	3389	0.14315···	351

The conclusion is: $H \leqslant 352$.

In the subsequent reduction steps we applied the algorithm of Fincke and Pohst [FP] to compute all lattice points in a sphere of a certain radius around the origin. We have for the fourth p-adic reduction step:

p	m	$n_1, n_2, n_3, n_4, A \leqslant$	W_1, W_2, W_3, W_4	Case	$\lvert\mathscr{B}\mathbf{t} - \mathbf{y}'\rvert \leqslant$	$\lvert\mathbf{u}\rvert \leqslant$	*	**	***
2	36	79, 54, 36, 30, 352	9, 13, 20, 23	I	294.93388	1158.86095	3312	22	0
				III	394.73914	1258.66621	5598	19	1
				V	279.97142	1143.89849	3172	14	0
3	21	37, 54, 36, 30, 352	19, 13, 20, 23	I	257.07978	1119.36628	8554	69	1
				III	173.62605	1035.91256	5344	71	4
				V	214.44349	1076.72999	6758	74	3
5	15	37, 21, 36, 30, 352	19, 34, 20, 23	I	323.10218	1187.84840	1570	11	2
				III	481.29621	1346.04243	3234	6	0
				V	299.41780	1164.16402	1414	6	0
7	12	37, 21, 16, 30, 352	19, 34, 44, 23	I	271.15118	1132.59766	1188	8	1
				III	302.54744	1163.99392	1462	10	0
				V	333.98644	1195.43292	1662	8	0

The * column gives the number of lattice points found in the sphere of radius the given bound for $\mathbf{u}$. The ** column gives the number of those points that satisfy the given bounds for n_i and A, as well as the condition $n_i + l_i \geqslant m$ for the i such that $p_i = p$. The *** column gives the number of these lattice points that correspond to solutions of $\mathrm{ord}_{p_i}(\Lambda_i') = n_i + l_i$ for only the prime $p_i = p$. The 12 such

solutions that were found were checked for $\mathrm{ord}_{p_i}(\Lambda_i') = n_i + l_i$ for the other three primes, and all failed. Thus the conclusion is:

$$n_1 \leqslant 37, \quad n_2 \leqslant 21, \quad n_3 \leqslant 16, \quad n_4 \leqslant 12,$$

hence, $N_4 = 37$.

At the fourth real reduction step we took $C = 10^{10}$ and $W_1 = 19$, $W_2 = 34$, $W_3 = 44$, $W_4 = 59$. Then $R = 791$ and $S = 624477$. We took $D = 1500$, which satisfies $D > \sqrt{R^2 + S} = 1118.1\ldots$. We found:

i_0	Case	$\lvert\mathscr{B}\mathbf{t}-\mathbf{y}'\rvert \leqslant$	*	**
1	I	464.29089	7656	3
	III	372.31576	5802	5
	V	205.23890	3238	1
2	I	647.46665	1316	1
	III	738.61362	1740	1
	V	630.15399	1284	1
3	I	707.31116	1424	1
	III	551.28128	926	3
	V	528.66156	864	2

Here the * column gives the number of lattice points in the sphere of radius D + the given bound for $|\mathscr{B}\mathbf{t}-\mathbf{y}'|$, and the ** column gives the number of those points inside the block given by the bounds for n_i found in the fourth p-adic reduction step, and the bound 352 for A found in the third real reduction step. These 18 candidate solutions did not pass the $\mathrm{ord}_{p_i}(\Lambda_i') = n_i + l_i$ test for the four primes. Now we have either $H \leqslant c_{18} + c_{17}N_4 = \dfrac{915.977}{5.812 - 2c_{16}}$, or we apply Proposition 16, which yields $H \leqslant \dfrac{19.571927}{c_{16}}$. The optimal c_{16} is 0.119097, that leads to the conclusion $H \leqslant 164$.

We performed three more reduction steps using the Fincke and Pohst method. We give the following data:

step	p/real	m/C	$n_1, n_2, n_3, n_4, A \leqslant$	W_1, W_2, W_3, W_4	R	S	D	*
fifth	2	24	37, 21, 16, 12, 164	9, 16, 21, 27				0
	3	14	25, 21, 16, 12, 164	13, 16, 21, 27				0
	5	10	25, 14, 16, 12, 164	13, 23, 21, 27				2
	7	8	25, 14, 11, 12, 164	13, 23, 30, 27				0
	real	10^9	25, 14, 11, 8, 164	13, 23, 30, 41	387	133507	750	0
sixth	2	21	25, 14, 11, 8, 113	9, 16, 21, 28				0
	3	12	22, 14, 11, 8, 113	10, 16, 21, 28				3
	5	9	22, 12, 11, 8, 113	10, 19, 21, 28				1
	7	7	22, 12, 10, 8, 113	10, 19, 23, 28				0
	real	10^8	22, 12, 10, 7, 113	10, 19, 23, 32	278	63634	600	0
seventh	2	18	22, 12, 10, 7, 99	9, 17, 20, 28				4
	3	11	19, 12, 10, 7, 99	10, 17, 20, 28				9
	5	7	19, 11, 10, 7, 99	10, 18, 20, 28				14
	7	6	19, 11, 8, 7, 99	10, 18, 25, 28				9
	real	10^7	19, 11, 8, 6, 99	10, 18, 25, 33	243	48428	500	3

Here the *-column gives the number of candidate-solutions that passed the test for $\mathrm{ord}_{p_i}(\Lambda_i') = n_i + l_i$ for the four primes. For these 45 candidate-solutions we computed (to a precision of about 15 decimal digits) as a subsequent test the real logarithms of the absolute values of the three conjugates of $\beta = \alpha\pi_{21}^{n_1}\pi_{31}^{n_2}\pi_5^{n_3}\pi_{71}^{n_4}\varepsilon_1^{a_1}\varepsilon_2^{a_2}$, and checked for

$$(\theta^{(2)} - \theta^{(3)})\beta^{(1)} + (\theta^{(3)} - \theta^{(1)})\beta^{(2)} + (\theta^{(1)} - \theta^{(2)})\beta^{(3)} = 0,$$

which is equivalent to (12). Only six candidates survived this, and appeared to correspond to solutions of (1) indeed. They are (of the pair $\pm(x, y)$ we give only the one with positive x)

n_1	n_2	n_3	n_4	a_1	a_2	Case	x	y	found at
18	0	12	0	−6	2	V	48632	−3729	fifth step, $p = 5$
0	13	2	0	−22	5	III	399	302	sixth step, $p = 3$
20	0	0	0	10	−3	I	56	55	seventh step, $p = 2$
0	2	2	1	−2	1	I	93	−103	seventh step, real
5	0	2	3	2	−1	III	1112	951	seventh step, real
2	0	8	0	3	−2	III	3388	149	seventh step, real

As in the fourth reduction step we conclude after the real reduction steps that we have for all but the above six exceptional solutions:

after step	c_{16}	$H \leqslant$
fifth	0.1577012···	113
sixth	0.1558846···	99
seventh	0.1562559···	86

The conclusion is that for all but the six exceptional solutions we have

$$n_1 \leqslant 19, \quad n_2 \leqslant 11, \quad n_3 \leqslant 8, \quad n_4 \leqslant 6, \quad A \leqslant 86.$$

Note that only the first three exceptional solutions do not satisfy these bounds. Carrying out further reduction in the same way caused the number of lattice points found by the Fincke and Pohst method to increase so dramatically that it turned out to be more efficient to apply the sieve method of the next section to find all the solutions below the bounds just obtained.

18. The final sieve

Now we are left with the 'very small' upper bounds $N_1, \ldots, N_v$ for $n_1, \ldots, n_v$ respectively, and A_0 for $A = \max|a_i|$. Thus we have $(N_1 + 1)\cdot\cdots\cdot(N_v + 1)\cdot(2A_0 + 1)^r$ possible tuples $(n_1, \ldots, n_v, a_1, \ldots, a_r)$ to check for relation (11), i.e. whether, if we express the right-hand side of (11) as a $\mathbb{Z}$-linear combination of an integral basis $1, \theta, \ldots$ of the order $\mathcal{O}$, all but the coefficients of 1 and θ turn out to be zero. Such a task might be difficult to accomplish by direct checking of every possible tuple. Therefore we propose the following, com-

putationally easier method, which constitutes a sieve of the set, in general very large, of possible (very small) tuples.

Let q be a rational prime, whose prime ideal factorization in K has at least three distinct first degree ideals, denoted by $\mathfrak{q}_i$ $(i = 1, 2, 3)$. Then

$$\theta \equiv m_i \pmod{\mathfrak{q}_i}$$

for some explicitly known $m_i \in \mathbb{Z}$ for $i = 1, 2, 3$. Hence for $i = 1, 2, 3$ rational integers $A_i, P_{i1}, \ldots, P_{iv}, E_{i1}, \ldots, E_{ir}$ can be easily computed such that (cf. (11))

$$\alpha \equiv A_i, \quad \pi_j \equiv P_{ij} (j = 1, \ldots, v), \quad \varepsilon_j \equiv E_{ij} \ (j = 1, \ldots, r) \pmod{\mathfrak{q}_i}.$$

It follows by (11) that

$$x - ym_i \equiv A_i \cdot P_{i1}^{n_1} \cdot \ldots \cdot P_{iv}^{n_v} \cdot E_{i1}^{a_1} \cdot \ldots \cdot E_{ir}^{a_r} \pmod{\mathfrak{q}_i} \ (i = 1, 2, 3),$$

and now both sides of the last congruence are rational integers, therefore each of the three congruences above holds modulo q as a congruence in $\mathbb{Z}$ as well. From these three congruences we can eliminate x and y, just as we did in deriving (12) from (11), to find a congruence of the form

$$\begin{aligned} &C_1 \cdot P_{11}^{n_1} \cdot \ldots \cdot P_{1v}^{n_v} \cdot E_{11}^{a_1} \cdot \ldots \cdot E_{1r}^{a_r} + C_2 \cdot P_{21}^{n_1} \cdot \ldots \cdot P_{2v}^{n_v} \cdot E_{21}^{a_1} \cdot \ldots \cdot E_{2r}^{a_r} \\ &\quad \equiv C_3 \cdot P_{31}^{n_1} \cdot \ldots \cdot P_{3v}^{n_v} \cdot E_{31}^{a_1} \cdot \ldots \cdot E_{3r}^{a_r} \pmod{q}. \end{aligned} \tag{38}$$

For several primes $q, q', q'', \ldots$ as above we can find analogous congruences. We start with checking all possible tuples $(n_1, \ldots, n_v, a_1, \ldots, a_r)$ for congruence (38) modulo q. Each tuple that survives this test is then checked for (38) modulo q', and so on. If a tuple does satisfy all the congruences (38) modulo $q, q', q'', \ldots$, then, and only then, this tuple is tested further, e.g. directly for (11), or by checking (12) seen as an equality in $\mathbb{R}$ with a certain precision (15 decimal digits usually will suffice). One expects that this last check has to be done for only a very few tuples that are not factual solutions of (11). In practice this is already the case when only a few primes $q, q', q'', \ldots$ are selected. Heuristically, one expects that only one out of every q random tuples satisfies (38) modulo q. Thus it is efficient to start the sieving with the largest prime selected.

18^{Ex} We have as bounds: $N_1 = 19, N_2 = 11, N_3 = 8, N_4 = 6, A_0 = 86$. The number of tuples to be checked in each of the three cases is thus $20 \cdot 12 \cdot 9 \cdot 7 \cdot 173^2 \approx 4.5 \times 10^8$. We chose four primes: $q = 401, 167, 89, 47$, that all split completely in K (note that $401 \cdot 167 \cdot 89 \cdot 47 \approx 2.8 \times 10^8$ is of the size of the number of tuples). Using the data as given in the Table below we performed the sieve for these four primes.

q	401			167			89			47		
i	1	2	3	1	2	3	1	2	3	1	2	3
m_i	−28	5	46	14	−75	−83	−34	−18	−14	3	−15	−12
C_i (Case I)	−41	74	33	8	70	78	−4	20	16	−3	−15	−18
C_i (Case III)	−9	−132	91	−75	−51	44	20	43	−24	−22	−16	16
C_i (Case V)	−116	140	77	−10	59	−39	−27	−21	38	−19	−4	−10
P_{i1}	−46	−35	134	−11	−40	−63	7	−35	−8	17	10	−21
P_{i2}	−19	138	39	−64	79	40	30	−24	−33	2	−12	6
P_{i3} (Case I)	126	192	3	−65	−72	−43	43	−31	42	9	14	16
P_{i3} (Case III)	−183	−139	136	−43	8	83	29	39	−31	22	−6	11
P_{i3} (Case V)	10	−121	−58	−72	78	−8	−5	−29	43	23	23	20
P_{i4}	29	−4	−45	−13	76	−83	35	19	15	−2	16	13
E_{i1}	143	188	−118	64	−50	−68	22	35	23	−10	−1	14
E_{i2}	63	−85	−48	−76	−56	−33	11	42	−21	22	17	−23

The results were as follows:

Case	initial # tuples	# tuples left after sieving with $q = 401$	$q = 167$	$q = 89$	$q = 47$
I	452526480	1128261	6767	87	20
III	452526480	1128603	6704	99	33
V	452526480	1128376	6764	121	29

The 82 tuples that were left were tested for (12) in 15 digit real precision. Three tuples did not satisfy this test, namely $(n_1, n_2, n_3, n_4, a_1, a_2, \text{Case}) = (9, 5, 5, 5, 48, 13, \text{III}), (10, 3, 1, 2, 18, -3, \text{III}), (10, 3, 1, 2, 18, -3, \text{V})$. The other 79 tuples come from solutions indeed. Among them there are 10 solutions counted twice, namely in Cases III and V with $n_3 = 1$. Thus there are 69 solutions satisfying the bounds given above, in addition to the 3 solutions not satisfying these bounds, that were found in the previous Section.

We do not give detailed information on the computation time, since we used different computers, which makes comparison difficult. Moreover, the computation times might say more about the complexity of our implementation of the algorithms than about the complexity of the algorithms themselves. Roughly speaking we used about 15% of the total time for the first reduction step (bringing the bound down from 9.844×10^{49} to 4918), about 5% on the second to fifth steps (from 4918 down to 113), about 45% on the sixth and seventh reduction step (from 113 down to 86, this large percentage being due to the very many lattice points detected by the Fincke and Pohst algorithm that had to be checked further), and about 30% for the final sieve. We estimate that the total computation time on a VAX 3100 workstation (the fastest computer we have used) would be about 100 hours.

We also performed an eighth and ninth reduction step using the Fincke and Pohst method, leading to a reduction of the bound from 86 down to 59 only, at the cost of 150 hours on the VAX 3100. It is thus clear that the sieve did this job much faster. This experience shows that the different reduction methods are in practice complementary. It also shows that the amount of work needed (by computer *and* programmer) for reducing the bound from, say, 1000 to 0, will in general be much larger than the time needed for the reduction from, say, 10^{50} to 1000.

Finally we give the complete list of solutions of

$$x - y\theta = \pm \pi_{21}^{n_1} \pi_{31}^{n_2} \pi_5^{n_3} \pi_{71}^{n_4} \varepsilon_1^{a_1} \varepsilon_2^{a_2}$$

with $(x, y) = 1$ and $x \geqslant 0$. Note that the solutions of the Thue-Mahler equation

$$x^3 - 23x^2y + 5xy^2 + 24y^3 = \pm 2^{z_1}3^{z_2}5^{z_3}7^{z_4}$$

can be easily found from this Table, since $z_1 = n_1$, $z_2 = n_2$, $z_3 = n_3 + \begin{cases} 0 & \text{in Case I} \\ 1 & \text{in Cases III, V} \end{cases}$, $z_4 = n_4$.

x	y	n_1	n_2	n_3	n_4	a_1	a_2	Case
48632	−3729	18	0	12	0	−6	2	V
264	−1003	5	5	7	1	−4	0	III
267	−209	0	8	3	2	−14	3	III
137	−199	0	0	3	6	−2	0	III
96	−107	3	5	1	1	−8	2	III, V
93	−103	0	2	2	1	−2	1	I
88	−101	8	0	2	2	3	−1	III
73	−81	0	0	2	3	−3	1	V
24	−53	6	2	3	1	−4	1	V
31	−32	0	0	5	1	−6	2	V
28	−31	2	0	2	0	1	0	III
24	−29	7	3	2	0	0	0	I
132	−29	2	4	2	3	−9	2	V
24	−23	4	2	3	0	−1	0	III
3	−16	0	6	2	0	−12	3	V
19	−13	0	0	6	0	2	−1	III
24	−13	11	1	1	0	3	−1	III, V
48	−13	3	9	1	0	−13	3	I
4	−9	2	0	5	0	5	−1	I
6	−7	1	1	2	0	−3	1	V
3	−4	0	2	0	2	−4	1	I
4	−3	2	0	1	1	0	0	III, V
1	−2	0	0	2	0	0	0	III
51	−2	0	4	4	0	−6	1	III
1	−1	0	0	1	0	1	0	I
3	−1	0	2	1	0	−4	1	III, V
6	−1	1	1	2	1	0	0	I
8	−1	4	0	2	0	0	0	V
13	−1	0	0	2	2	−1	0	III
0	−1	3	1	0	0	0	0	I
1	0	0	0	0	0	0	0	I
1	1	0	0	0	1	0	0	I
2	1	1	0	1	0	0	0	III, V
8	1	7	0	0	1	3	−1	I
12	1	2	1	2	0	−1	0	III
15	1	0	5	0	1	−9	2	I
22	1	1	0	1	1	−1	0	III, V
24	1	4	2	1	0	−1	0	I
42	1	1	3	3	0	−8	2	V
3	2	0	3	1	0	−4	1	I

x	y	n_1	n_2	n_3	n_4	a_1	a_2	Case
9	2	0	1	2	1	−4	1	V
1	3	0	0	3	0	−3	1	V
10	3	1	0	0	4	−1	0	I
7	6	0	0	1	0	0	0	III, V
8	7	4	0	2	0	4	−1	I
9	7	0	1	3	0	−1	0	III
24	7	5	4	1	0	−5	1	III, V
159	7	0	3	2	0	−6	1	III
8	9	6	0	2	0	3	−1	III
128	9	3	0	4	2	−4	1	V
12	11	2	2	2	0	−4	1	V
32	11	3	0	4	1	2	−1	III
87	11	0	1	7	0	−10	3	V
6	13	1	3	2	1	−5	1	III
272	13	3	0	4	3	3	−1	I
296	13	6	0	3	0	−1	0	V
24	17	4	1	1	2	−1	0	III, V
744	37	6	3	3	2	−3	0	III
48	41	3	4	0	1	−5	1	I
56	43	5	0	5	0	−3	1	V
59	52	0	0	3	3	−4	1	V
56	55	20	0	0	0	10	−3	I
2184	97	14	5	1	0	−3	0	III, V
24	115	10	6	0	2	−6	1	I
152	131	10	0	2	1	3	−1	V
216	139	12	1	4	1	7	−2	I
3388	149	2	0	8	0	3	−2	III
399	302	0	13	2	0	−22	5	III
534	457	1	1	6	1	1	−1	III
984	827	7	8	3	0	−13	3	V
1112	951	5	0	2	3	2	−1	III
1656	1663	11	1	5	3	4	−2	III

Appendix A1. The absolute logarithmic height of an algebraic number

Let α be an algebraic number, $a_0 t^D + \cdots + a_D$ its minimal polynomial over $\mathbb{Z}$, and $\alpha^{(1)}, \ldots, \alpha^{(D)}$ the real or complex roots of this polynomial. The *absolute logarithmic height* of α is

$$h(\alpha) = \frac{1}{D} \log \left(a_0 \prod_{i=1}^{D} \max\{1, |\alpha^{(i)}|\} \right).$$

Note that even when we view α as a complex number (so that α coincides with some $\alpha^{(i)}$) rather than as an abstract algebraic number, $h(\alpha)$ is independent of the

specific numerical value of the conjugate of α that we are considering. For references and more information on the absolute logarithmic height we refer to [Wa, Section 2].

A1^{Ex} Below δ_1 is as defined in Section 7 (see also the Table in Section 6^{Ex}), where for (i_0, j, k) we have chosen some permutation of $(1, 2, 3)$. Referring to the notation of Appendix A1, we have computed the following Table.

α	$\frac{\theta^{(1)}-\theta^{(2)}}{\theta^{(1)}-\theta^{(3)}}$	$\frac{\theta^{(1)}-\theta^{(2)}}{\theta^{(1)}-\theta^{(3)}}\cdot\frac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}}$	$\frac{\theta^{(1)}-\theta^{(2)}}{\theta^{(1)}-\theta^{(3)}}\cdot\frac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}}$	$\frac{\pi_{21}^{(3)}}{\pi_{21}^{(2)}}$	$\frac{\pi_{31}^{(3)}}{\pi_{31}^{(2)}}$
D	6	6	6	6	6
a_0	1115525	1115525	1115525	4	9
$h(\alpha)<$	3.132209	7.218871	5.263156	2.167337	7.164226

α	$\frac{\pi_{51}^{(3)}}{\pi_{51}^{(2)}}$	$\frac{\pi_{52}^{(3)}}{\pi_{52}^{(2)}}$	$\frac{\pi_{53}^{(3)}}{\pi_{53}^{(2)}}$	$\frac{\pi_{71}^{(3)}}{\pi_{71}^{(2)}}$	$\frac{\varepsilon_1^{(3)}}{\varepsilon_1^{(2)}}$	$\frac{\varepsilon_2^{(3)}}{\varepsilon_2^{(2)}}$
D	6	6	6	6	6	6
a_0	25	25	25	49	1	1
$h(\alpha)<$	3.545166	3.237718	5.676112	2.267031	3.806189	8.378281

Appendix A2. A lower bound for linear forms in logarithms of algebraic numbers in the *p*-adic case

In this Appendix we refer to [Yu2, Section 0.2]. We have made several slight modifications to the notation in order to conform to (or to avoid confusion with) the notation of the present paper.

Let $\alpha_1, \ldots, \alpha_m$ $(m \geqslant 2)$ be nonzero algebraic numbers, and put $K_1 = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, $n_1 = [K_1 : \mathbb{Q}]$. Let p be a prime number. Set

$$(q, u) = \begin{cases} (2, 2) & \text{if } p > 2 \\ (3, 1) & \text{if } p = 2 \end{cases}.$$

Let K_2 be an extension of K_1 such that

$$i \in K_2 \quad \text{if } p > 2, \quad (i = \sqrt{-1}),$$

$$\omega \in K_2 \quad \text{if } p = 2, \quad \left(\omega = \frac{-1+\sqrt{-3}}{2}\right),$$

and $n_2 = [K_2 : \mathbb{Q}]$. Let $\mathfrak{p}_2$ be a prime ideal of K_2 over p with f_2 as residual degree.

For any algebraic number α of degree D and conjugates $\alpha^{(1)}, \ldots, \alpha^{(D)}$ in $\mathbb{C}$ we define

$$L(\alpha) = \max_{1 \leqslant i \leqslant D} |\mathrm{Log}\, \alpha^{(i)}|,$$

where Log denotes the principal complex algorithm. Now for every $j = 1, \ldots, m$ let

$$V_j \geqslant \max \left\{ h(\alpha_j), \frac{L(\alpha_j)}{2\pi n_2}, \frac{f_2 \log p}{n_2} \right\},$$

and

$$V = \max_{1 \leqslant j \leqslant m} V_j.$$

Finally put

$$\sigma = \frac{1}{2qf_2 \log p}.$$

Let $b_1, \ldots, b_m \in \mathbb{Z}$, and put

$$\lambda = \alpha_1^{b_1} \cdot \ldots \cdot \alpha_m^{b_m} - 1, \quad B = \max_{1 \leqslant j \leqslant m} |b_j|.$$

The following theorem is a slightly weakened version of [Yu2, Theorem 1].

THEOREM (Yu). *If* $\mathrm{ord}_{\mathfrak{p}_2}(\alpha_j) = 0$ *for* $j = 1, \ldots, m$ *and* $\lambda \neq 0$, *then*

$$\mathrm{ord}_{\mathfrak{p}_2}(\lambda) < C_0 \cdot (m+1)^{m+2} \cdot m^{m+\sigma} \cdot \frac{p^{f_2} - 1}{q^u} \cdot \left(\frac{2 + 1/(p-1)}{f_2 \log p} \right)^{m+2} \cdot n_2^{m+2} \cdot V_1 \cdot \ldots \cdot V_m \cdot$$
$$\cdot \max\{m \log(2^{10} qm(m+\sigma) n_2^2 V), f_2 \log p\} \cdot (\log B + 2 \log n_2),$$

where

$$C_0 = \begin{cases} 404746 \times 10^m & \text{if } p > 2 \\ 848625 \times 12^m & \text{if } p = 2 \end{cases}.$$

A2$^{\mathrm{Ex}}$ We refer to the notation of Appendix A2. In our case $p \in \{2, 3, 5, 7\}$, $m = 7$, $\alpha_1 = \delta_1$, $\alpha_2 = \frac{\pi_{21}^{(k)}}{\pi_{21}^{(j)}}$, $\alpha_3 = \frac{\pi_{31}^{(k)}}{\pi_{31}^{(j)}}$, $\alpha_4 = \frac{\pi_5^{(k)}}{\pi_5^{(j)}}$, $\alpha_5 = \frac{\pi_{71}^{(k)}}{\pi_{71}^{(j)}}$, $\alpha_6 = \frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}$, $\alpha_7 = \frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}$, K_1 is the normal closure of K, so that $n_1 = 6$, and $K_2 = K_1(\zeta)$ with $\zeta = i$ for $p = 3, 5, 7$ and $\zeta = \omega$ for $p = 2$. Since $K_1 \subset \mathbb{R}$ it is obvious that $n_2 = 12$.

We put $\mathfrak{p} = \mathfrak{p}_{p1}$ if $p = 2, 3, 7$, and $\mathfrak{p} = \mathfrak{p}_5$ if $p = 5$ (see the Table in Section 6^{Ex}). In Section 3^{Ex} we have seen that

$$e_{K/\mathbb{Q}}(\mathfrak{p}) = 1, f_{K/\mathbb{Q}}(\mathfrak{p}) = 1.$$

Let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be prime ideals over p of K_1 and K_2 respectively. Put

$$f_j = f_{K_j/\mathbb{Q}}(\mathfrak{p}_j)$$

for $j = 1, 2$ (note that f_2 agrees with the notation of Appendix A2). Since $\mathfrak{p}_2$ is over $\mathfrak{p}$ we obviously have $\mathrm{ord}_{\mathfrak{p}}(\lambda) \leqslant \mathrm{ord}_{\mathfrak{p}_2}(\lambda)$, therefore

$$\mathrm{ord}_p(\lambda) = \mathrm{ord}_{\mathfrak{p}}(\lambda) \leqslant \mathrm{ord}_{\mathfrak{p}_2}(\lambda). \tag{39}$$

By the relation between residual degrees of ideals in relative extensions (see [Na2, Proposition 4.3] or [Na1, p. 136]) we have

$$f_1 = f_{K_1/\mathbb{Q}}(\mathfrak{p}_1) = f_{K_1/K}(\mathfrak{p}_1) f_{K/\mathbb{Q}}(\mathfrak{p}) = f_{K_1/K}(\mathfrak{p}_1) \leqslant 2, \tag{40}$$

since $[K_1 : K] = 2$. By Yu's lemma (see [Yu2, Appendix]), for $p = 2, 3, 7$ we have $f_2 = \max\{f_1, 2\}$, while for $p = 5$ we have $f_2 = f_1$. Hence, by (40),

$$f_2 = 2 \quad \text{for} \quad p = 2, 3, 7, \qquad f_2 \leqslant 2 \quad \text{for} \quad p = 5. \tag{41}$$

Now we can apply the Theorem of Appendix A2, making use of (41), in order to find an upper bound for $\mathrm{ord}_{\mathfrak{p}}(\lambda)$, which, in view of (39), will give an upper bound for $\mathrm{ord}_p(\lambda)$. In our case, of course λ is given by the leftmost expression in (12), and $B = H$. Straightforward computations show that $V_j = h(\alpha_j)$ for $j = 1, \ldots, 7$. The upper bound for $\mathrm{ord}_p(\lambda)$ is of the form

$$\mathrm{ord}_p(\lambda) \leqslant c_{10}(p)(\log H + c_{11}(p)).$$

For every $p \in \{2, 3, 5, 7\}$ we can take

$$c_{11}(p) = 4.970 \geqslant 2 \log n_2 = 2 \log 12.$$

It is easy to see that the worst (=largest) upper bound given by the Theorem is obtained in Case V. Then $V_1 \cdot \cdots \cdot V_7 < 33534.769$, and $V = V_7 < 8.378281$. The following Table is useful for the computation of $c_{10}(p)$:

p	q	u	f_2	σ	$\dfrac{p^{f_2}-1}{q^u}$	$\dfrac{2+1/(p-1)}{f_2 \log p}$	C_0
2	3	1	2	$\dfrac{1}{12\log 2}$	1	$\dfrac{3}{2\log 2}$	848625×12^7
3	2	2	2	$\dfrac{1}{8\log 3}$	2	$\dfrac{5}{4\log 3}$	404746×10^7
5	2	2	2	$\dfrac{1}{8\log 5}$	6	$\dfrac{9}{8\log 5}$	404746×10^7
5	2	2	1	$\dfrac{1}{4\log 5}$	1	$\dfrac{9}{4\log 5}$	404746×10^7
7	2	2	2	$\dfrac{1}{8\log 7}$	12	$\dfrac{13}{12\log 7}$	404746×10^7

A straightforward computation shows that

$$c_{10}(2) = 1.020 \times 10^{47}, \quad c_{10}(3) = 8.051 \times 10^{43},$$
$$c_{10}(5) = 2.787 \times 10^{44}, \quad c_{10}(7) = 7.050 \times 10^{41}$$

(rounded up).

Appendix A3. A lower bound for linear forms in logarithms of algebraic numbers in the real/complex case

In this section we state a recent result by Blass, Glass, Manski, Meronk and Steiner [BGMMS, Corollary 2], which considerably improves the lower bound for linear forms in logarithms of algebraic numbers given in a well known earlier paper of Waldschmidt [Wa]. Below we give a slightly modified (weakened) version of this result, though we believe it to be more useful for our application.

Let $\alpha_1, \ldots, \alpha_m$ ($m \geqslant 2$) be algebraic numbers, which we view as complex numbers, belonging to a field of absolute degree $D \geqslant 2$. For every $j = 1, \ldots, m$ we fix a determination of the logarithm of α_j, which we denote by $\log \alpha_j$. For $j = 1, \ldots, m$ we define

$$V_j = \max\left\{h(\alpha_j), \frac{|\log \alpha_j|}{D}, \frac{1}{D}\right\},$$

where we have supposed, without loss of generality, that the numbering of the α_j's is such that

$$V_1 \leqslant \cdots \leqslant V_m.$$

Further we define for $j = 1, \ldots, m$

$$V_j^+ = \max\{1, V_j\}, \quad \bar{V}_j = \max\{jV_j, 1\}, \quad a_j = \frac{DV_j}{|\log \alpha_j|}, \quad \bar{a}_j = \left(\frac{1}{j}\sum_{i=1}^{j}\frac{1}{a_i}\right)^{-1}.$$

We also consider positive numbers a, $\bar{a}$, E, $\bar{E}$ and $\bar{M}$ such that

$$a \leqslant \left(\frac{1}{m}\sum_{i=1}^{m}\frac{1}{a_i}\right)^{-1}, \quad \bar{a} \geqslant \left(\frac{1}{m}\sum_{i=1}^{m}\frac{1}{\bar{a}_i}\right)^{-1}, \quad E \leqslant \min\{e^{2DV_1}, 4Da\},$$
$$\bar{E} \geqslant \min\{e^{2DV_1}, 4\bar{a}\}, \quad \bar{M} \leqslant 2(2^8 mD\bar{V}_{m-1}E)^m.$$

Finally, let $b_1, \ldots, b_m \in \mathbb{Z}$. Put

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m, \quad B = \max_{1 \leqslant j \leqslant m} |b_j|.$$

THEOREM (Blass, Glass, Manski, Meronk and Steiner). *If* $\Lambda \neq 0$ *and*

$$B \geqslant \frac{V_m}{m+1} \max\{(2^7 mDV_m^+)^m, E, \bar{E}^{2/mD}\}$$

then

$$|\Lambda| > e^{-c_7(\log B + c_8)},$$

where

$$c_7 \geqslant \frac{(24e^2)^m 2^{20}}{(\log \bar{E})^{m+1}} \cdot D^{m+2} \cdot m \cdot V_1 \cdot \ldots \cdot V_m \cdot \log \bar{M}$$

and

$$c_8 \geqslant (m+1)^2 \log\left(\frac{6mD^3\bar{V}_m}{\log D}\right) + \frac{(m+1)^2}{m}\log(m!)$$
$$+ \log\left(\frac{m}{V_1} + \frac{1}{V_m} + 0.000025\right) + \frac{m+1}{m^2}\log m.$$

A3$^{\text{Ex}}$ The algebraic numbers $\alpha_1, \ldots, \alpha_7$ are those which appear in Appendix A2$^{\text{Ex}}$, but now the ordering of these numbers is not immaterial, in view of the condition $V_1 \leqslant \cdots \leqslant V_7$. Note that here Λ is the linear form Λ_0 appearing in Section 10. As stressed there we must consider three cases, depending on the value of i_0. Corresponding to those cases we have chosen (see Section 10$^{\text{Ex}}$) $(j, k) = (2, 3), (3, 1), (1, 2)$. In the notation of the Theorem of Appendix A3, $B = H$, and $D = 6$. In the case of our specific example, the Theorem is applied with $H = A$ (see Section 10, after (21)). For the computation of the numerical values of c_7 and c_8 it has been necessary to construct the following Tables:

Case	α_1	α_2	α_3	α_4	α_5	α_6	α_7
I	$\frac{\pi_{21}^{(k)}}{\pi_{21}^{(j)}}$	$\frac{\pi_{71}^{(k)}}{\pi_{71}^{(j)}}$	δ_1	$\frac{\pi_{51}^{(k)}}{\pi_{51}^{(j)}}$	$\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}$	$\frac{\pi_{31}^{(k)}}{\pi_{31}^{(j)}}$	$\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}$
III	$\frac{\pi_{21}^{(k)}}{\pi_{21}^{(j)}}$	$\frac{\pi_{71}^{(k)}}{\pi_{71}^{(j)}}$	$\frac{\pi_{52}^{(k)}}{\pi_{52}^{(j)}}$	$\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}$	$\frac{\pi_{31}^{(k)}}{\pi_{31}^{(j)}}$	δ_1	$\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}$
V	$\frac{\pi_{21}^{(k)}}{\pi_{21}^{(j)}}$	$\frac{\pi_{71}^{(k)}}{\pi_{71}^{(j)}}$	$\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}$	δ_1	$\frac{\pi_{53}^{(k)}}{\pi_{53}^{(j)}}$	$\frac{\pi_{31}^{(k)}}{\pi_{31}^{(j)}}$	$\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}$

Case	$V_1 \cdot \cdots \cdot V_7$	V_1	V_6	V_7
I	12464.805	2.167336…	7.164225…	8.378280…
III	26236.536	2.167336…	7.218870…	8.378280…
V	33534.769	2.167336…	7.164225…	8.378280…

Case I	$j=2, k=3$	$j=3, k=1$	$j=1, k=2$
a_1	2.238651…	34.422300…	2.394369…
a_2	2.801580…	5.584987…	5.621454…
a_3	7.720476…	8.022874…	204.830465…
a_4	2.356620…	9.075308…	3.183219…
a_5	2.000000…	2.911946…	6.386221…
a_6	2.107738…	9.860509…	2.680767…
a_7	21.669204…	2.203363…	2.000000…
$a<$	2.944	5.218	3.601
$\bar{a}>$	2.693	8.219	3.729
$E<$	70.645	125.223	86.412
$\bar{E}>$	10.774	32.877	14.918
$\log \bar{M}<$	121.639	125.810	123.213
c_7	6.076×10^{32}	2.889×10^{31}	2.202×10^{32}
c_8	885.955		
provided that $H>$	3.939×10^{32}		

Case III	$j=2, k=3$	$j=3, k=1$	$j=1, k=2$
a_1	2.238651…	34.422300…	2.394369…
a_2	2.801580…	5.584987…	5.621454…
a_3	3.038761…	11.354584…	2.397209…
a_4	2.000000…	2.911946…	6.386221…
a_5	2.107738…	9.860509…	2.680767…
a_6	3.335715…	25.336697…	2.947642…
a_7	21.669204…	2.203363…	2.000000…
$a<$	2.854	5.672	2.940
$\bar{a}>$	2.493	8.270	3.033
$E<$	68.485	136.108	70.542
$\bar{E}>$	9.973	33.083	12.133
$\log \bar{M}<$	121.639	126.447	121.846
c_7	1.663×10^{33}	6.034×10^{31}	8.658×10^{32}
c_8	885.955		
provided that $H>$	3.939×10^{32}		

Case V	$j=2, k=3$	$j=3, k=1$	$j=1, k=2$
a_1	2.238651···	34.422300···	2.394369···
a_2	2.801580···	5.584987···	5.621454···
a_3	2.000000···	2.911946···	6.386221···
a_4	3.577519···	49.999816···	3.853219···
a_5	2.208761···	53.805969···	2.303313···
a_6	2.107738···	9.860509···	2.680767···
a_7	21.669204···	2.203363···	2.000000···
$a<$	2.739	6.112	3.019
$\bar{a}>$	2.439	8.170	3.267
$E<$	65.715	146.678	72.451
$\bar{E}>$	9.757	32.682	13.068
$\log \bar{M}<$	121.297	126.917	121.980
c_7	2.289×10^{33}	7.948×10^{31}	8.765×10^{32}
c_8	885.955		
provided that $H>$	3.939×10^{32}		

Summing up we have in all cases:

If $H > 3.939 \times 10^{32}$ then $|\Lambda_0| > e^{-c_7(\log H + c_8)}$,

where $c_7 = 2.289 \times 10^3$ and $c_8 = 885.955$.

It is impressive that, on applying Waldschmidt's theorem on which the present theorem is based (cf. [Wa]), we find $c_7 \approx 7 \times 10^{54}$, $c_8 \approx 5$, unconditionally on H. As is seen in Section 10^{Ex}, the restriction $H > 3.939 \times 10^{32}$ is not essential.

Acknowledgements

We are indebted to A. Bremner and R. J. Stroeker for helping us to improve the style of our paper.

References

[ACHP] A. K. Agrawal, J. Coates, D. C. Hunt and A. J. van der Poorten, Elliptic curves of conductor 11, *Math. Comput.* 35 (1980), 991–1002.

[Be] W. E. H. Berwick, Algebraic number-fields with two independent units, *Proc. London Math. Soc.* 34 (1932), 360–378.

[BGMMS] J. Blass, A. M. W. Glass, D. K. Manski, D. B. Meronk and R. P. Steiner, Constants for lower bounds for linear forms in logarithms of algebraic numbers II. The homogeneous rational case, *Acta Arith.* 55 (1990), 15–22.

[Bi1] K. K. Billevič, On the units of algebraic fields of third and fourth degree (Russian), *Mat. Sb.* 40, 82 (1956), 123–137.

[Bi2] K. K. Billevič, A theorem on the units of algebraic fields of nth degree, (Russian), *Mat. Sb.* 64, 106 (1964), 145–152.

[BS] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, London, 1973.

[Bu1] J. Buchmann, The generalized Voronoi algorithm in totally real algebraic number fields, *Eurocal '85, Linz 1985, Vol. 2,* Lecture Notes in Comput. Sci. 204, Springer, Berlin, New York, 1985, pp. 479–486.

[Bu2] J. Buchmann, A generalization of Voronoi's unit algorithm I, *J. Number Th.* 20 (1986), 177–191.

[Bu3] J. Buchmann, A generalization of Voronoi's unit algorithm II, *J. Number Th.* 20 (1986), 192–209.

[Bu4] J. Buchmann, On the computation of units and class numbers by a generalization of Lagrange's algorithm, *J. Number Th.* 26 (1987), 8–30.

[Bu5] J. Buchmann, The computation of the fundamental unit of totally complex quartic orders, *Math. Comput.* 48 (1987), 39–54.

[DF] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Vol. 10, Transl. of Math. Monographs, Am. Math. Soc, Rhode Island, 1964.

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

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

[Ko] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer Verlag, New York, 1977.

[LLL] A. K. Lenstra, H. W. Lenstra jr. and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1983), 515–534.

[Ma] K. Mahler, Zur Approximation algebraischer Zahlen, I: Über den grössten Primteiler binärer Formen, *Math. Ann.* 107 (1933), 691–730.

[Na1] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, Warszawa, 1974.

[Na2] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd ed., Polish Scientific Publishers, Warszawa, 1990.

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

[PZ1] M. Pohst and H. Zassenhaus, On effective computation of fundamental units I, *Math. Comput.* 38 (1982), 275–291.

[PZ2] M. Pohst, P. Weiler and H. Zassenhaus, On effective computation of fundamental units II, *Math. Comput.* 38 (1982), 293–329.

[PZ3] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, 1989.

[Sm] J. Graf von Schmettow, KANT – a tool for computations in algebraic number fields, A. Pethö, M. Pohst, H. C. Williams and H. G. Zimmer, eds., *Computational Number Theory*, Walter de Gruyter & Co., Berlin, 1991, pp. 321–330.

[Sp] V. G. Sprindžuk, *Classical diophantine equations in two unknowns* (Russian), Nauka, Moskva, 1982.

[ST] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, Cambridge, 1986.

[Th] A. Thue, Über Annäherungswerten algebraischer Zahlen, *J. reine angew. Math.* 135 (1909), 284–305.

[TW1] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Th.* 31 (1989), 99–132.

[TW2] N. Tzanakis and B. M. M. de Weger, Solving a specific Thue-Mahler equation, *Math. Comput.* 57 (No. 196) (1991), 799–815.

[TW3] N. Tzanakis and B. M. M. de Weger, "On the practical solution of the Thue-Mahler equation, A. Pethö, M. Pohst, H. C. Williams and H. G. Zimmer, eds., *Computational Number Theory*, Walter de Gruyter & Co., Berlin, 1991, pp. 289–294.

[Wa] M. Waldschmidt, A lower bound for linear forms in logarithms, *Acta Arith.* 37 (1980), 257–283.

[dW1] B. M. M. de Weger, *Algorithms for diophantine equations*, CWI-Tract No. 65, Centre for Math. and Comp. Sci., Amsterdam, 1989.

[dW2] B. M. M. de Weger, On the practical solution of Thue-Mahler equations, an outline, K. Győry and G. Halász, eds., *Number Theory*, Coll. Math. Soc. János Bolyai, Vol. 51, Budapest, 1990, pp. 1037–1050.

[Yu1] Kunrui Yu, Linear forms in p-adic logarithms, *Acta Arith.* 53 (1989), 107–186.

[Yu2] Kunrui Yu, Linear forms in p-adic logarithms II, *Compositio Math.* 74 (1990), 15–113.