JOURNAL OF NUMBER THEORY 26, 325–367 (1987)

Solving Exponential Diophantine Equations Using Lattice Basis Reduction Algorithms

B. M. M. DE WEGER*

Mathematisch Instituut, Rijks Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

Communicated by M. Waldschmidt

Received June 5, 1986

Let S be the set of all positive integers with prime divisors from a fixed finite set of primes. Algorithms are given for solving the diophantine inequality $0 < x - y < y^{\delta}$ in $x, y \in S$ for fixed $\delta \in (0, 1)$, and for the diophantine equation $x + y = z$ in $x, y, z \in S$. The method is based on multi-dimensional diophantine approximation, in the real and p-adic case, respectively. The main computational tool is the L^3-Basis Reduction Algorithm. Elaborate examples are presented.

1. INTRODUCTION

In 1981, L. Lovász invented an algorithm for computing a reduced (i.e., nearly orthogonal) basis of an arbitrary lattice in $\mathbb{R}^n$ from a known basis of the lattice. It has a surprisingly good theoretical complexity (polynomial time), and also performs very well in practice. This algorithm, together with an application to the factorization of polynomials, is described in Lenstra *et al.* [9]. It has several other interesting applications, such as in public-key cryptography (cf. Lagarias and Odlyzko [8]), and in the disproof of the Mertens conjecture (cf. Odlyzko and te Riele [13]). We shall refer to the algorithm as the "L^3-Basis Reduction Algorithm," (L^3-BRA).

The L^3-BRA can also be used for solving multi-dimensional diophantine approximation problems, as Lenstra *et al.* already indicated [9, p. 525]. In the present paper it is shown that this enables us to find all solutions of certain exponential diophantine equations and inequalities in a routine manner. As is well known, many types of diophantine problems are associated to linear forms in logarithms of algebraic numbers (see, e.g., Baker [3, Chap. 4], Shorey and Tijdeman [18], Stroeker and Tijdeman [20, pp. 343–353]). Namely, for any large solution of the diophantine problem some linear form in logarithms is extremely close to zero. The Gelfond–Baker method provides effectively computable (and in many cases

* Present address: Department of Applied Mathematics, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands.

0022-314X/87 $3.00

explicitly computed) lower bounds for the absolute values of such linear forms. Thus, explicit upper bounds for the solutions of many diophantine problems can be obtained. The bounds that are found in this way are so large that enumeration of the remaining possibilities is practically impossible. However, it is generally assumed that the bounds are far from the actual largest solution. Therefore it is worthwile to search for methods to reduce the found upper bounds.

If the linear form in logarithms under consideration has only two terms, a simple method applies, based on continued fractions. For example, Cijsouw, Korlaar, and Tijdeman (Appendix to Stroeker and Tijdeman [20]) found in this way all solutions of the diophantine inequality

$$|p^x - q^y| < p^{\delta x} \tag{1.1}$$

for all primes p, q with $p < q < 20$, and $\delta = \frac{1}{2}$. In Section 4.B we extend this result for many more values of p, q, and $\delta = \frac{9}{10}$.

A natural generalization of (1.1) is the following problem. Let S be the set of all positive integers composed of primes from a fixed finite set $\{p_1, ..., p_t\}$, where $t \geqslant 2$, and let $\delta \in (0, 1)$. Then find all solutions of the diophantine inequality

$$0 < x - y < y^{\delta} \tag{1.2}$$

in x, $y \in S$. Putting $x/y = p_1^{x_1} \cdots p_t^{x_t}$, the corresponding linear form in logarithms is

$$\Lambda = x_1 \log p_1 + \cdots + x_t \log p_t.$$

The continued fraction method applies only for $t = 2$. For $t \geqslant 3$, multidimensional continued fraction algorithms are available (cf. Brentjes [5]), but they are not useful for our purposes. In Section 4.C we shall show that the L^3-BRA leads to substantial improvements of the upper bounds for (1.2). Usually the new bound is of the size of the logarithm of the initial bound. For $t = 6$, $\{p_1, ..., p_6\} = \{2, 3, 5, 7, 11, 13\}$, $\delta = \frac{1}{2}$, we show in detail how (1.2) can be solved completely with this method.

If the linear form is inhomogeneous of the form

$$\Lambda = x_1 \log \alpha_1 + \cdots + x_n \log \alpha_n + \log \alpha_{n+1},$$

it can of course be made homogeneous by introducing the variable x_{n+1} as coefficient of the last term. We may then solve this $(n+1)$-dimensional approximation problem, and select all solutions with $x_{n+1} = 1$. There is, however, a different approach, which may be faster. See Baker and Davenport [4] for $n = 2$, and Ellison [6] for $n > 2$. It is then needed to find good simultaneous approximations p_i/q to $\log \alpha_i / \log \alpha_n$ $(i = 1, ..., n-1)$. Lenstra *et al.* [9, p. 525] have indicated how the L^3-BRA can be used to find such approximations. We do not work this out in the present paper.

Up to now we have only considered real linear forms in logarithms. There is a p-adic counterpart of the Gelfond–Baker theory, which provides lower bounds for the p-adic values of linear forms in p-adic logarithms of algebraic numbers. It is therefore a natural problem to devise p-adic analogues of the diophantine approximation methods sketched above. The simplest case is that of an inhomogeneous form with only one variable, such as

$$\Lambda = x \log_p \alpha_1 + \log_p \alpha_2.$$

Then it suffices to compute the p-adic expansion of $\log_p \alpha_2 / \log_p \alpha_1$ far enough. See Wagstaff [21], Pethö and de Weger [14], and de Weger [24].

In the case of a form with two terms, such as

$$\Lambda = x_1 \log_p \alpha_1 + x_2 \log_p \alpha_2$$

a practical p-adic analogue of the real continued fraction algorithm is needed. Such an algorithm was first formulated by Mahler [11, Chap. 4]. A similar algorithm has been studied by de Weger [23] in the context of p-adic approximation lattices. See Agrawal *et al.* [1] for an application to a Thue–Mahler equation. We shall show in Section 5.C how to solve

$$p_1^{x_1} + p_2^{x_2} = w p_3^{x_3} \tag{1.3}$$

for fixed p_1, p_2, p_3, w using this algorithm. A natural generalization of (1.3) is the diophantine equation

$$x + y = z \tag{1.4}$$

in $x, y, z \in S$, with S as above. We may assume $\gcd(x, y, z) = 1$. Put $p = p_t$, and suppose $p \mid z$. Then $p \nmid xy$. Put $x/y = p_1^{x_1} \cdots p_{t-1}^{x_{t-1}}$. Then we have the p-adic linear form in logarithms

$$\Lambda = x_1 \log_p p_1 + \cdots + x_{t-1} \log_p p_{t-1}.$$

The concept of approximation lattices of p-adic numbers, as introduced in [23], can be generalized to the multi-dimensional case, as we shall see in Section 5.B. Then we can apply the L^3-BRA. In Section 5.D we show how this can be used to solve (1.4) explicitly. We give details for $t = 6$, $\{p_1, ..., p_6\} = \{2, 3, 5, 7, 11, 13\}$. This generalizes the results of Alex [2], who gave a complete solution of (1.4) for $t = 4$, $\{p_1, ..., p_4\} = \{2, 3, 5, 7\}$ by elementary arguments. The case where z has only one prime divisor was treated by Rumsey and Posner [16], also by elementary means.

Many diophantine equations, such as the Thue equation, the Thue–

Mahler equation, the hyperelliptic equation and the Mordell equation, lead to linear forms in logarithms similar to those described above. These equations differ from our examples (1.2) and (1.4) in that the path from the equation to the linear form in logarithms is not as straightforward; it leads through some algebraic number theory. This clearly does not affect the applicability of our approximation methods for reducing upper bounds, since they are based only on the linear forms themselves.

2. Bounds for Linear Forms in Logarithms

In this section we quote the results that we use from the theory of linear forms in logarithms. We do not quote the theorems in full generality, since we apply them only for logarithms of rational integers, and for rational coefficients. The results provide lower bounds for linear forms in logarithms in the real and p-adic cases. We chose results that give completely explicit constants and lead to convenient upper bounds for the solutions of the diophantine problems we want to solve. We stress that our methods for reducing these bounds are in principle independent of the size of the bounds.

Let $p_1,\ldots, p_n$ $(n \geqslant 2)$ be rational integers such that $2 \leqslant p_1 < \cdots < p_n$, and $[\mathbb{Q}(p_1^{1/2},\ldots, p_n^{1/2})\colon \mathbb{Q}] = 2^n$. Let $b_1,\ldots, b_n \in \mathbb{Z}$, and put $B = \max_{1 \leqslant i \leqslant n} |b_i|$. In the real case we have the following result.

Lemma 2.1. (Waldschmidt). *Let*

$$\Lambda = b_1 \log p_1 + \cdots + b_n \log p_n$$

be nonzero. Put

$$V_i = \max(1, \log p_i) \qquad (i = 1,\ldots, n),\ \Omega = V_1 \cdots V_n,$$

$$C_1 = 2^{9n+26} n^{n+4} \Omega \log(eV_{n-1}), \qquad C_2 = C_1 \log(eV_n).$$

Then

$$|\Lambda| > \exp\{-(C_1 \log B + C_2)\}.$$

This lemma was proved by Waldschmidt [22]. In the case $n = 2$ a sharper bound was given by Mignotte and Waldschmidt [12]. In the p-adic case we have the following result:

Lemma 2.2. (van der Poorten). *Let p be a prime with $p \nmid p_i$ $(i = 1,\ldots, n)$. Let*

$$\Lambda = b_1 \log_p p_1 + \cdots + b_n \log_p p_n$$

be nonzero. Choose μ, κ *with* $2/(n+1) \leqslant \mu \leqslant 2$, $0 < \kappa < \mu/2$. *Put*

$$V_i = \max(e, \log p_i) \qquad (i = 1, ..., n),\ \Omega = V_1 \cdots V_n,$$

$$G_p = \begin{cases} p(p-1) & \textit{if} \ \ p = 2, 3 \\ p-1 & \textit{if} \ \ p \geqslant 5, \end{cases}$$

$$\varepsilon = (\mu - \kappa)/(1+\kappa)(1+\mu)(n+1),$$

$$k = \max\{(16n)^{(1+1/\kappa)(n+1)}, (8/\varepsilon)^{(1+\mu)(n+1)}, 16^{1/\varepsilon}\},$$

$$C_3 = 4(n+1)^{(n+1)} k^{(1+\mu)} (G_p/\log p)\, \Omega.$$

Then $B \leqslant 7$, *or*

$$\mathrm{ord}_p(\Lambda) \leqslant C_3 (\log B)^2.$$

This lemma follows from the proof of Theorem 2 of van der Poorten [15]. Note that we omitted the factor $n(2D^2)^{n+1}$, since $D = 1$; cf. van der Poorten [15, p. 35]. To save computation time we may choose μ, κ as a function of n such that C_3 is minimal, for van der Poorten's estimate $(16(n+1))^{12(n+1)}$ for $4(n+1)^{(n+1)} k^{(1+\mu)}$ (with $\mu = 2$, $\kappa = \frac{1}{2}$) is rather crude. Note that for $n = 2$ a sharper bound was by Schinzel [17]. It is expected that the constant C_3 of Lemma 2.2 can be sharpened considerably (van der Poorten, private communication).*

We also need the following simple lemma. For its proof, see Pethö and de Weger [14, Lemma 2.2].

LEMMA 2.3. *Let* $a \geqslant 0$, $h \geqslant 1$, $b > (e^2/h)^h$, *and let* $x \in \mathbb{R}$ *satisfy* $x \leqslant a + b(\log x)^h$. *Then*

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

3. THE L^3-BASIS REDUCTION ALGORITHM

In this section we describe how we use the L^3-BRA. All lattices that appear in this paper are integral lattices, that is, sublattices of $\mathbb{Z}^n$. In the algorithm as stated in [9, Fig. 1, p. 521], non-integral rationals may occur, even if the input consists of rational integers only. We now describe a variant of the L^3-BRA in which only integers occur. This has the advantage of avoiding rounding-off errors.

Let $\Gamma \subset \mathbb{Z}^n$ be a lattice with basis vectors $\mathbf{b}_1, ..., \mathbf{b}_n$. Define $\mathbf{b}_i^*$, $\mu_{i,j}$, d_i as in [9], (1.2), (1.3), (1.24), respectively. The d_i can be used as denominators

* *Note added in proof.* Recently, K. R. Yu has obtained such an improvement, to be published in the Proceedings of the 1986 Durham Conference. His results lead (in Section 5) to bounds less than the square root of the bounds we derived using Lemma 2.2.

for all numbers that appear in the original algorithm [9, p. 523]. Thus, put for all relevant i, j,

$$\mathbf{c}_i = d_{i-1}\mathbf{b}_i^*, \tag{3.1}$$

$$\lambda_{i,j} = d_j \mu_{i,j}. \tag{3.2}$$

They are integral, by [9], (1.28), (1.29). Note that, with $B_i = |\mathbf{b}_i^*|^2$,

$$d_i = d_{i-1} B_i. \tag{3.3}$$

We can now rewrite the L^3-BRA in terms of $\mathbf{c}_i$, d_i, $\lambda_{i,j}$ instead of $\mathbf{b}_i^*$, B_i, $\mu_{i,j}$, thus eliminating all non-integral rationals. We give this variant of the algorithm in Table I. All the lines in this variant are evident from applying

TABLE I

Variant of the L^3-Basis Reduction Algorithm

$$
\begin{array}{lll}
\text{(A)} & & \left.\begin{array}{l}
d_0 := 1; \\
\mathbf{c}_i := \mathbf{b}_i; \\
\left.\begin{array}{l}
\lambda_{i,j} := (\mathbf{b}_i, \mathbf{c}_j); \\
\mathbf{c}_i := (d_j \mathbf{c}_i - \lambda_{i,j}\mathbf{c}_j)/d_{j-1}
\end{array}\right\} \text{for } j = 1, \ldots, i-1; \\
d_i := (\mathbf{c}_i, \mathbf{c}_i)/d_{i-1} \\
k := 2;
\end{array}\right\} \text{for } i = 1, \ldots, n; \\
& (1) & \text{perform } (*) \text{ for } l = k-1; \\
& & \text{if } 4d_{k-2}d_k < 3d_{k-1}^2 - 4\lambda_{k,k-1}^2, \text{ go to } (2); \\
& & \text{perform } (*) \text{ for } l = k-2, \ldots, 1; \\
& & \text{if } k = n, \text{ terminate}; \\
& & k := k+1; \\
& & \text{go to } (1); \\
& (2) & \begin{pmatrix} \mathbf{b}_{k-1} \\ \mathbf{b}_k \end{pmatrix} := \begin{pmatrix} \mathbf{b}_k \\ \mathbf{b}_{k-1} \end{pmatrix}; \begin{pmatrix} \mathbf{u}_{k-1} \\ \mathbf{u}_k \end{pmatrix} := \begin{pmatrix} \mathbf{u}_k \\ \mathbf{u}_{k-1} \end{pmatrix}; \\
& & \begin{pmatrix} \lambda_{k-1,j} \\ \lambda_{k,j} \end{pmatrix} := \begin{pmatrix} \lambda_{k,j} \\ \lambda_{k-1,j} \end{pmatrix} \text{ for } j = 1, \ldots, k-2; \\
\text{(B)} & & \begin{pmatrix} \lambda_{i,k-1} \\ \lambda_{i,k} \end{pmatrix} := \left(\lambda_{i,k-1}\begin{pmatrix} \lambda_{k,k-1} \\ d_k \end{pmatrix} + \lambda_{i,k}\begin{pmatrix} d_{k-2} \\ -\lambda_{k,k-1} \end{pmatrix}\right) \Big/ d_{k-1} \text{ for } i = k+1, \ldots, n; \\
\text{(C)} & & d_{k-1} := (d_{k-2}d_k + \lambda_{k,k-1}^2)/d_{k-1}; \\
& & \text{if } k > 2, \text{ then } k := k-1; \\
& & \text{go to } (1); \\
& (*) & \text{if } 2\,|\lambda_{k,l}| > d_l, \text{ then} \\
& & \left\{\begin{array}{l}
r := \text{integer nearest to } \lambda_{k,l}/d_l; \\
\mathbf{b}_k := \mathbf{b}_k - r\mathbf{b}_l; \ \mathbf{u}_k := \mathbf{u}_k - r\mathbf{u}_l; \\
\lambda_{k,j} := \lambda_{k,j} - r\lambda_{l,j} \text{ for } j = 1, \ldots, l-1; \\
\lambda_{k,l} := \lambda_{k,l} - rd_l.
\end{array}\right.
\end{array}
$$

(3.1), (3.2), and (3.3) to the corresponding lines in the original algorithm, except the lines (A), (B), and (C), which will be explained below.

We added a few lines to the algorithm, in order to compute the matrix of the transformation from the initial to the reduced basis. Let C be the matrix with column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ (we say: the matrix associated to the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$), and let B be the matrix associated to the reduced basis computed by the algorithm. Then we define this transformation matrix V by $B = CV$. More generally, let U be the matrix of a transformation from some C_0 to C, so $C = C_0 U$. Denote the column vectors of U by $\mathbf{u}_1, \ldots, \mathbf{u}_n$. All manipulations in the algorithm done on $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are also done on $\mathbf{u}_1, \ldots, \mathbf{u}_n$. Then the algorithm gives as output matrices B and U', such that B is associated to a reduced basis, $B = CV$, and $U' = UV$. (Note that V is not computed explicitly). Hence $B = CU^{-1}U' = C_0 U'$, so U' is the matrix of the transformation from C_0 to B. In particular, if $U = I$, then $C = C_0$ and $U' = V$.

We now explain lines (A), (B), and (C).

(A) From [9], (1.2) it follows that

$$\mathbf{c}_i = d_{i-1}\mathbf{b}_i - \sum_{k=1}^{i-1} \frac{d_{i-1}}{d_{k-1}d_k} \lambda_{i,k}\mathbf{c}_k.$$

Define for $j = 0, 1, \ldots, i-1$,

$$\mathbf{c}_i(j) = d_j\mathbf{b}_i - \sum_{k=1}^{j} \frac{d_j}{d_{k-1}d_k} \lambda_{i,k}\mathbf{c}_k.$$

Then $\mathbf{c}_i(0) = \mathbf{b}_i$, and $\mathbf{c}_i(i-1) = \mathbf{c}_i$. The $\mathbf{c}_i(j)$ is exactly the vector computed in (A) at the jth step, since

$$\begin{aligned}&(d_j\mathbf{c}_i(j-1) - \lambda_{i,j}\mathbf{c}_j)/d_{j-1}\\ &\quad = d_j\mathbf{b}_i - \sum_{k=1}^{j-1} \frac{d_j}{d_{k-1}d_k} \lambda_{i,k}\mathbf{c}_k - \frac{d_j}{d_{j-1}d_j} \lambda_{i,j}\mathbf{c}_j = \mathbf{c}_i(j).\end{aligned}$$

This explains the recursive formula in line (A). It remains to show that the occurring vectors $\mathbf{c}_i(j)$ are integral. This follows from

$$d_j \sum_{k=1}^{j} \frac{1}{d_{k-1}d_k} \lambda_{i,k}\mathbf{c}_k = d_j \sum_{k=1}^{j} \mu_{i,k}\mathbf{b}_k^*,$$

which is integral by [9, p. 523, l. 11].

(B), (C) Note that the third and fourth line, starting from label (2), in the original algorithm are independent of the first, second, and fifth line. Thus a permutation of these lines is allowed. We rewrite the first, second, and fifth line as follows, where we indicate variables that have been changed by a prime,

$$B'_{k-1} := B_k + \mu^2_{k,k-1} B_{k-1}; \tag{3.4}$$

$$B'_k := B_{k-1} B_k / B'_{k-1}; \tag{3.5}$$

$$\mu'_{k,k-1} := \mu_{k,k-1} B_{k-1} / B'_{k-1}; \tag{3.6}$$

$$\left.\begin{aligned} \mu'_{i,k-1} &:= \mu'_{k,k-1}\mu_{i,k-1} + (1 - \mu_{k,k-1}\mu'_{k,k-1})\,\mu_{i,k}; \quad (3.7) \\ \mu'_{i,k} &:= \mu_{i,k-1} - \mu_{k,k-1}\mu_{i,k} \quad (3.8) \end{aligned}\right\} \text{for } i = k+1, \dots, n.$$

The d_i remain unchanged for $i = 0, 1, \dots, k-2$, and by (3.5) also for $i = k$. Now, (3.4) is equivalent to

$$\frac{d'_{k-1}}{d_{k-2}} = \frac{d_k}{d_{k-1}} + \frac{\lambda^2_{k,k-1}}{d^2_{k-1}} \frac{d_{k-1}}{d_{k-2}}, \tag{3.9}$$

which explains (C). From (3.6) we find

$$\frac{\lambda'_{k,k-1}}{d'_{k-1}} = \frac{\lambda_{k,k-1}}{d_{k-1}} \frac{d_{k-1}}{d_{k-2}} \frac{d'_{k-2}}{d'_{k-1}},$$

hence $\lambda_{k,k-1}$ remains unchanged. From (3.7) we obtain

$$\frac{\lambda'_{i,k-1}}{d'_{k-1}} = \frac{\lambda_{k,k-1}}{d'_{k-1}} \frac{\lambda_{i,k-1}}{d_{k-1}} + \left(1 - \frac{\lambda_{k,k-1}}{d_{k-1}} \frac{\lambda_{k,k-1}}{d'_{k-1}}\right) \frac{\lambda_{i,k}}{d_k},$$

whence, by multiplying by $d_{k-1} d'_{k-1}$ and using (3.9),

$$\begin{aligned} d_{k-1}\lambda'_{i,k-1} &= \lambda_{k,k-1}\lambda_{i,k-1} + (d_{k-1}d'_{k-1} - \lambda^2_{k,k-1}) \frac{\lambda_{i,k}}{d_k} \\ &= \lambda_{k,k-1}\lambda_{i,k-1} + d_{k-2}\lambda_{i,k}. \end{aligned}$$

Finally, from (3.8) we see

$$\frac{\lambda'_{i,k}}{d_k} = \frac{\lambda_{i,k-1}}{d_{k-1}} - \frac{\lambda_{k,k-1}}{d_{k-1}} \frac{\lambda_{i,k}}{d_k},$$

and (B) follows.

In our applications we often have a lattice Γ, of which a basis is given such that the associated matrix, A say, has the special form

$$A = \begin{pmatrix} 1 & & 0 \\ 0 & \ddots & 1 \\ \theta_1 & \cdots & \theta_n \end{pmatrix},$$

where the θ_i are large integers (they may have several hundreds of digits). We can compute a reduced basis of this lattice directly, using the matrix A itself as input for the L^3-BRA. But it may save time and space to split up the computation into several steps with increasing accuracy, as follows.

Let k be a natural number (the number of steps), and let l be a natural number such that the θ_i have about kl (decimal) digits. For $i=1,\ldots,n$, $j=1,\ldots,k$, put

$$\theta_i^{(j)}=[\theta_i/10^{l(k-j)}],$$

and define $\psi_i^{(j)}$ by

$$\theta_i^{(j+1)}=10^l\,\theta_i^{(j)}+\psi_i^{(j)}.$$

Thus, the $\psi_i^{(j)}$ are blocks of l consecutive digits of θ_i. Define for the relevant j,

$$A_j=\begin{pmatrix} 1 & & 0 \\ 0 & \ddots & 1 \\ \theta_1^{(j)} & \cdots & \theta_n^{(j)} \end{pmatrix}, \qquad \Psi_j=\begin{pmatrix} & 0 & \\ \psi_1^{(j)} & \cdots & \psi_n^{(j)} \end{pmatrix},$$

$$E=\begin{pmatrix} 1 & & & 0 \\ 0 & \ddots & 1 & \\ & & & 10^l \end{pmatrix}.$$

Then it follows at once that

$$A_{j+1}=EA_j+\Psi_j.$$

Note that $A_k=A$, since $\theta_i^{(k)}=\theta_i$. Put $U_0=I$, $C_1=A_1$. For some $j\geqslant 1$ let C_j and U_{j-1} be known matrices. Then we apply the L^3-BRA to $C=C_j$, $U=U_{j-1}$. We thus find matrices B_j and U_j such that

$$B_j=C_jU_{j-1}^{-1}U_j.$$

Now put

$$C_{j+1}=EB_j+\Psi_jU_j.$$

By induction the matrices B_j, C_j, and U_j are well defined for $j=1,\ldots,k$. Note that

$$C_{j+1}U_j^{-1}=EC_jU_{j-1}^{-1}+\Psi_j,$$

so the $C_j U_{j-1}^{-1}$ satisfy the same recursive relation as the A_j. Since $C_1 U_0^{-1} = A_1$, we have $C_j U_{j-1}^{-1} = A_j$ for all j. Hence

$$B_j = C_j U_{j-1}^{-1} U_j = A_j U_j,$$

and it follows that B_k and A_k are associated to bases of the same lattice, which is Γ. Moreover, since B_k is output of the L^3-BRA, it is associated to a reduced basis of Γ.

Let us now analyse the computation time. For a matrix M we denote by $L(M)$ the maximal number of (decimal) digits of its entries. If the L^3-BRA is applied to a matrix C, with as output a matrix B, then according to the experiences of Lenstra, Odlyzko (cf. Lenstra [10, p. 7]) and ourselves, the computation time is proportional to $L(C)^3$ in practice. Since B is associated to a reduced basis, we have

$$L(B) \simeq {}^{10}\log(\det(\Gamma))/n.$$

In our situation, $L(A_j) \simeq lj$, $L(\Psi_j) \simeq l$, and since $\det(B_j) = \det(A_j) = \theta_n^{(j)}$, we have $L(B_j) \simeq lj/n$. Put $B_j = (b_{i,h}^{(j)})$, $U_j = (u_{i,h}^{(j)})$. Then by $B_j = A_j U_j$ and the special shape of A_j we have $b_{i,h}^{(j)} = u_{i,h}^{(j)}$ for $i = 1, ..., n-1$, $h = 1, ..., n$, and

$$u_{n,h}^{(j)} = (-b_{1,h}^{(j)}\theta_1^{(j)} - \cdots - b_{n-1,h}^{(j)}\theta_{n-1}^{(j)} + b_{n,h}^{(j)})/\theta_n^{(j)}.$$

It follows that $L(U_j) \simeq L(B_j)$. So

$$L(C_j) \simeq \max(L(EB_{j-1}), L(\Psi_{j-1} U_{j-1})) \simeq l + l(j-1)/n.$$

Instead of applying the L^3-BRA once with A as input, we apply it k times, with $C_1, ..., C_k$ as input. Thus we reduce the computation time by a factor

$$\frac{L(A)^3}{\sum_{j=1}^{k} L(C_j)^3} \simeq \frac{(lk)^3}{\sum_{j=1}^{k} l^3(1+(j-1)/n)^3} = \frac{k^3 n^3}{\sum_{j=0}^{k-1} (n+j)^3}.$$

For k between $2.5n$ and $3n$ this expression is maximal, about $0.4n^2$. So the reduction in computation time is considerable. The storage space that is required is also reduced, since the largest numbers that appear in the input have $l(1+((k-1)/n))$ digits.

We use the L^3-BRA for finding a lower bound for the length of the non-zero vectors of a lattice Γ. Let $|\cdot|$ denote the euclidean length on $\mathbb{R}^n$. Put

$$l(\Gamma) = \min_{0 \neq \mathbf{x} \in \Gamma} |\mathbf{x}|.$$

Then the following inequality holds (cf. [9, (1.11)]).

LEMMA 3.1. (Lenstra *et al.*). *Let* $\mathbf{b}_1,\ldots,\mathbf{b}_n$ *be a reduced basis of the lattice* Γ. *Then*

$$l(\Gamma) \geqslant 2^{-(n-1)/2}\,|\mathbf{b}_1|.$$

In some applications we want to compute all vectors in a lattice with length bounded by a given constant. To do this we employ a recent algorithm of Fincke and Pohst [7], in combination with the L^3-BRA.

4. A DIOPHANTINE INEQUALITY

Let $p_1 < \cdots < p_t$ be prime numbers, where $t \geqslant 2$. Let S be the set of all positive integers composed of these primes only, so

$$S = \{p_1^{x_1} \cdots p_t^{x_t} : x_i \in \mathbb{Z},\ x_i \geqslant 0 \text{ for } i = 1,\ldots, t\}.$$

Let $0 < \delta < 1$ be a fixed real number. We study the diophantine inequality

$$0 < x - y < y^{\delta} \tag{4.1}$$

in $x, y \in S$. For a solution x, y of (4.1), the finitely many $z \in \mathbb{N}$ for which zx, zy is also a solution of (4.1) can be found without any difficulty. Therefore we may assume that $(x, y) = 1$. Put

$$X = \max_{1 \leqslant i \leqslant t} \operatorname{ord}_{p_i}(xy).$$

Tijdeman showed that there exists a computable number c, depending on p_t only, such that for all $x, y \in S$ with $x > y \geqslant 3$,

$$x - y > y/(\log y)^c$$

(cf. Shorey and Tijdeman [18, Theorem 1.1]). Thus, for any solution of (4.1) a bound for X can be computed, and we do so in Section 4.A. In Sections 4.B and 4.C we show how to reduce such an upper bound, in the cases $t = 2$ and $t \geqslant 3$ respectively.

4.A. *Upper Bounds*

THEOREM 4.1. *In the above notation, put*

$$C_4 = 2^{9t+26} t^{t+4} \max\left(1, \frac{1}{\log p_1}\right) \log p_2 \cdots \log p_t \log(e \log p_{t-1})/(1-\delta),$$

$$C_5 = 2 \log 2/\log p_1 + 2C_4 \log(eC_4 \log p_t).$$

Then the solutions of (4.1) *satisfy* $X < C_5$.

Proof. If $y \leqslant \frac{1}{2}x$, then $y^{\delta} > x - y \geqslant y$, which contradicts $y \geqslant 1$. So $y > \frac{1}{2}x$. Put $\Lambda = \log(x/y)$, then

$$0 < \Lambda < x/y - 1 < y^{-(1-\delta)} < (\tfrac{1}{2}x)^{-(1-\delta)}. \tag{4.2}$$

By $x = \max(x, y) \geqslant p_1^X$, we obtain

$$0 < \Lambda < 2^{1-\delta} p_1^{-(1-\delta)X}. \tag{4.3}$$

We apply Lemma 2.1 to Λ, with $n = t$, $q = 2$. Since $p_i \geqslant 3$ we have $V_i = \log p_i$ for $i \geqslant 2$. Thus

$$\Lambda > \exp\{-(\log X + \log(e \log p_t))\, C_4 (1 - \delta) \log p_1\}.$$

Combining this with (4.3) we find

$$X < C_4 \log(e \log p_t) + \log 2/\log p_1 + C_4 \log X.$$

The result now follows from Lemma 2.3, since $C_4 > e^2$. ∎

Examples. With $t = 2$, $2 \leqslant p_i \leqslant 199$ and $\delta = \frac{9}{10}$ we have $C_4 < 2.30 \times 10^{17}$ and $C_5 < 1.97 \times 10^{19}$. With $t = 6$, $2 \leqslant p_i \leqslant 13$ and $\delta = \frac{1}{2}$ we find $C_4 < 8.37 \times 10^{33}$ and $C_5 < 1.35 \times 10^{36}$.

4.B. *The Case $t = 2$*

In this section we work out the example $t = 2$, $2 \leqslant p_i \leqslant 199$ and $\delta = \frac{9}{10}$. We find all solutions of (4.1) with these parameters, thus extending a result of Cijsouw, Korlaar, and Tijdeman (Appendix to Stroeker and Tijdeman [20]). We write

$$\Lambda = |x_1 \log p_1 - x_2 \log p_2|,$$

where x_1, x_2 are both positive integers. We assume that

$$p_1^X > 10^{25}, \tag{4.4}$$

since it is easy to find the remaining solutions. Let $\log p_1/\log p_2$ have the simple continued fraction expansion

$$\log p_1/\log p_2 = [0; a_1, a_2, \ldots],$$

and let the convergents r_n/q_n be defined by

$$r_{-1} = 1, \qquad r_0 = 0, \qquad r_n = a_n r_{n-1} + r_{n-2},$$
$$q_{-1} = 0, \qquad q_0 = 1, \qquad q_n = a_n q_{n-1} + q_{n-2} \qquad (n = 1, 2, \ldots).$$

It is well known that r/q is a convergent of a real number α if

$$|\alpha - r/q| < 1/2q^2,$$

and that all convergents r_n/q_n of $\alpha = [a_0; a_1, a_2, \ldots]$ satisfy

$$1/(a_{n+1}+2)\, q_n^2 < |\alpha - r_n/q_n| < 1/a_{n+1} q_n^2. \tag{4.5}$$

We may assume that $(x_1, x_2) = 1$. We now have the following criteria.

LEMMA 4.2. *Assume* (4.4).

(a) *If* (4.3) *holds for some* x_1, x_2, *then* $x_2 = r_k$, $x_1 = q_k$ *for some* $k \leqslant 92$, *and*

$$a_{k+1} + 2 > p_1^{q_k/10} \frac{1}{q_k} \frac{\log p_2}{2^{1/10}}.$$

(b) *If for some* k

$$a_{k+1} > p_1^{q_k/10} \frac{1}{q_k} \frac{\log p_2}{2^{1/10}},$$

then (4.3) *holds for* $x_2 = r_k$, $x_1 = q_k$.

Proof. First we show that $x_1 \geqslant x_2$, hence $X = x_1$. Namely, if $x_1 < x_2$, then

$$\Lambda = x_2 \log p_2 - x_1 \log p_1 > X(\log p_2 - \log p_1) \geqslant X \log \frac{199}{197} > 0.0101\, X.$$

From (4.3) and (4.4) we infer

$$0.0101 \leqslant 0.0101\, X < \Lambda < 2^{1/10} 10^{-5/2} < 0.0034,$$

which is contradictory. Next we prove that

$$p_1^{X/10} > 3.1\, X. \tag{4.6}$$

Namely, suppose the contrary. Then $2^{X/10} \leqslant 3.1\, X$, and it follows that $X \leqslant 80$. This contradicts $3.1\, X \geqslant p_1^{X/10} > 10^{5/2}$. Now, (4.3) is equivalent to

$$\left| \frac{x_2}{X} - \frac{\log p_1}{\log p_2} \right| < \frac{2^{1/10}}{\log p_2} p_1^{-X/10} \frac{1}{X}. \tag{4.7}$$

TABLE II (Theorem 4.3a)

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
2	3	8	3	2	9	0.00000
3	3	27	5	2	25	0.21534
2	5	32	3	3	27	0.48832
5	3	125	11	2	121	0.28906
2	7	128	11	2	121	0.40575
2	7	128	5	3	125	0.22754
2	8	256	3	5	243	0.46694
7	3	343	19	2	361	0.49512
2	9	512	23	2	529	0.45416
3	7	2187	13	3	2197	0.29941
3	7	2187	47	2	2209	0.40194
13	3	2197	47	2	2209	0.32293
19	3	6859	83	2	6889	0.38504
31	3	29791	173	2	29929	0.47828
2	15	32768	181	2	32761	0.18716
13	7	627 48517	89	4	627 42241	0.48703
2	50	1 12589 99068 42624	47	9	1 11913 04731 02767	0.85259
7	18	1 62841 35979 10449	149	7	1 63043 64614 03549	0.80898
19	12	2 21331 49190 66161	83	8	2 25229 22321 39041	0.88568
2	51	2 25179 98136 85248	19	12	2 21331 49190 66161	0.88532
2	51	2 25179 98136 85248	83	8	2 25229 22321 39041	0.76159
5	22	2 38418 57910 15625	157	7	2 35124 32775 37493	0.87942
13	14	3 93737 63856 99289	89	8	3 93658 88057 02081	0.76282
17	13	9 90457 80329 05937	193	7	9 97473 03260 05057	0.86560
7	19	11 39889 51853 73143	197	7	11 51499 04768 98413	0.87594
61	9	11 69414 60928 34141	197	7	11 51499 04768 98413	0.88743
5	23	11 92092 89550 78125	61	9	11 69414 60928 34141	0.89343
5	23	11 92092 89550 78125	29	11	12 20050 97657 05829	0.89862
29	11	12 20050 97657 05829	199	7	12 35866 42791 61399	0.88268
23	12	21 91462 44320 20321	43	10	21 61148 23132 84249	0.88656
11	16	45 94972 98635 72161	71	9	45 84850 07184 49031	0.84059
5	24	59 60464 47753 90625	73	9	58 87158 67082 67913	0.88642
37	11	177 91762 17794 60413	53	10	174 88747 03655 13049	0.89785
29	12	353 81478 32054 69041	89	9	350 35640 37074 85209	0.88568
23	13	504 03636 19364 67383	163	8	498 31141 43181 21121	0.89040
23	13	504 03636 19364 67383	59	10	511 11675 33006 41401	0.89536
11	17	505 44702 84992 93771	163	8	498 31141 43181 21121	0.89580

11	17	505 44702 84992 93771	23	13	504 03636 19364 67383	0.85578
11	17	505 44702 84992 93771	59	10	511 11675 33006 41401	0.88985
7	21	558 54586 40832 84007	41	11	550 32903 17162 48441	0.89708
19	14	799 00668 57828 84121	31	12	787 66278 37885 49761	0.89710
19	14	799 00668 57828 84121	173	8	802 35917 84760 91681	0.86722
2	60	1152 92150 46068 46976	181	8	1151 93665 78235 00641	0.83013
67	10	1822 83780 45517 61449	107	9	1838 45921 24201 54507	0.88680
47	11	2472 15921 50840 12303	199	8	2459 37419 15531 18401	0.87580
13	17	8650 41591 93813 37933	127	9	8594 75474 86093 97887	0.88441
2	63	9223 37203 68547 75808	53	11	9269 03592 93721 91597	0.87844
3	41	36472 99637 71707 86403	149	9	36197 31987 96201 91349	0.89170
2	65	36893 48814 74191 03232	5	28	37252 90298 46191 40625	0.89721
2	66	73786 97629 48382 06464	97	10	73742 41268 94928 26049	0.83799
3	42	1 09418 98913 15123 59209	101	10	1 10462 21254 11204 51001	0.89916
2	68	2 95147 90517 93528 25856	29	14	2 97558 23267 57994 63481	0.89800
113	10	3 39456 73899 22223 14849	191	9	3 38298 68155 95733 17311	0.87990
53	12	4 91258 90425 67261 54641	199	9	4 89415 46411 90705 61799	0.88284
5	30	9 31322 57461 54785 15625	41	13	9 25103 10231 50136 29321	0.89638
19	17	54 80386 85778 48021 85939	47	13	54 60999 70612 05831 77327	0.88730
23	16	61 32610 41568 09986 48961	151	10	61 62677 95033 67185 14001	0.89400
2	73	94 44732 96573 92904 27392	7	26	93 87480 33764 77543 05649	0.89920
2	75	377 78931 86295 71617 09568	181	10	377 38596 84695 57044 99801	0.86840
2	75	377 78931 86295 71617 09568	41	14	379 29227 19491 55588 02161	0.89368
41	14	379 29227 19491 55588 02161	181	10	377 38596 84695 57044 99801	0.89828
3	49	2392 99329 23061 75295 90083	17	19	2390 72435 68515 13248 47153	0.87071
13	21	2470 64529 07345 03927 04413	89	12	2469 90403 56526 21403 03521	0.84941
103	12	14257 60886 84617 89454 47841	157	11	14285 52404 46318 60195 25093	0.88788
3	51	21536 93963 07555 77663 10747	163	11	21580 60662 62396 00904 07387	0.88933
7	29	32199 05755 81317 97268 37607	13	22	32118 38877 95485 51051 57369	0.89390
11	24	98497 32675 80761 10947 11841	61	14	98768 32533 36131 80951 12441	0.89755
37	16	1 23375 11914 21716 63622 74241	191	11	1 23414 74201 97479 41888 22591	0.86078
2	84	1 93428 13113 83406 67952 98816	199	11	1 93813 41794 57931 33178 02199	0.89319
2	84	1 93428 13113 83406 67952 98816	3	53	1 93832 45667 68001 98967 96723	0.89402
3	53	1 93832 45667 68001 98967 96723	199	11	1 93813 41794 57931 33178 02199	0.84151
7	30	2 25393 40290 69225 80878 63249	31	17	2 25501 16774 16274 31786 82911	0.86903
2	90	123 79400 39285 38027 48991 24224	181	12	123 63541 71303 11583 51179 80561	0.89326
43	17	587 44031 06360 42001 88795 53643	71	15	587 32059 59385 49335 38673 30551	0.86709
2	99	63382 53001 14114 70074 83516 02688	97	15	63325 11891 36789 38604 32759 54593	0.89791
2	102	5 07060 24009 12917 60598 68128 21504	83	16	5 07282 02989 53863 75247 83563 99681	0.89060
13	28	15 50293 28026 62396 21526 95351 05521	89	16	15 49673 14251 78936 43509 93277 30561	0.89106

TABLE III (Theorem 4.3b)

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
2	3	8	3	2	9	.00000
3	3	27	5	2	25	0.21534
2	5	32	3	3	27	0.48832
2	5	32	6	2	36	0.40000
5	3	125	11	2	121	0.28906
2	7	128	11	2	121	0.40575
2	7	128	5	3	125	0.22754
6	3	216	15	2	225	0.40876
2	8	256	3	5	243	0.46694
7	3	343	19	2	361	0.49512
2	9	512	23	2	529	0.45416
2	10	1024	10	3	1000	0.46007
6	4	1296	11	3	1331	0.49607
12	3	1728	42	2	1764	0.48070
2	11	2048	45	2	2025	0.41184
3	7	2187	13	3	2197	0.29941
3	7	2187	47	2	2209	0.40194
13	3	2197	47	2	2209	0.32293
15	4	50625	37	3	50653	0.30762
6	7	2 79936	23	4	2 79841	0.36309
2	50	1 12589 99068 42624	47	9	1 11913 04731 02767	0.85259
2	50	1 12589 99068 42624	18	12	1 15683 13814 26176	0.89628
24	11	1 52168 11431 69024	33	10	1 53157 89852 64449	0.85597
15	13	1 94619 50683 59375	50	9	1 95312 50000 00000	0.83986
2	51	2 25179 98136 85248	19	12	2 21331 49190 66161	0.88532
6	20	3 65615 84400 62976	26	11	3 67034 44869 87776	0.84507
11	15	4 17724 81694 15651	20	12	4 09600 00000 00000	0.89095
28	11	8 29350 94674 71872	39	10	8 14040 60851 91601	0.89154
10	16	10 00000 00000 00000	17	13	9 90457 80329 05937	0.87396
5	23	11 92092 89550 78125	29	11	12 20050 97657 05829	0.89862
2	54	18 01439 85094 81984	30	11	17 71470 00000 00000	0.89096
23	12	21 91462 44320 20321	43	10	21 61148 23132 84249	0.88656
6	21	21 93695 06403 77856	23	12	21 91462 44320 20321	0.81690
6	21	21 93695 06403 77856	43	10	21 61148 23132 84249	0.88845
2	55	36 02879 70189 63968	24	12	36 52034 74360 56576	0.88735

19	13	42 05298 34622 57059	46	10	42 42074 74827 76576	0.87619
3	35	50 03154 50989 99707	33	11	50 54210 65137 26817	0.88076
13	15	51 18589 30140 90757	33	11	50 54210 65137 26817	0.88656
26	12	95 42895 66616 82176	35	11	96 54915 73730 46875	0.88631
35	11	96 54915 73730 46875	50	10	97 65625 00000 00000	0.88575
14	15	155 56809 55578 12224	21	13	154 47237 77391 19461	0.87497
11	17	505 44702 84992 93771	23	13	504 03636 19364 67383	0.85578
7	21	558 54586 40832 84007	41	11	550 32903 17162 48441	0.89708
6	23	789 73022 30536 02816	31	12	787 66278 37885 49761	0.85579
6	23	789 73022 30536 02816	19	14	799 00668 57828 84121	0.89216
19	14	799 00668 57828 84121	31	12	787 66278 37885 49761	0.89710
26	13	2481 15287 32037 36576	47	11	2472 15921 50840 12303	0.86739
28	13	6502 11142 24979 47648	37	12	6582 95200 58400 35281	0.89872
15	16	6568 40835 57128 90625	28	13	6502 11142 24979 47648	0.89414
15	16	6568 40835 57128 90625	37	12	6582 95200 58400 35281	0.85892
2	65	36893 48814 74191 03232	5	28	37252 90298 46191 40625	0.89721
37	13	2 43569 22421 60813 05397	50	12	2 44140 62500 00000 00000	0.87101
2	68	2 95147 90517 93528 25856	29	14	2 97558 23267 57994 63481	0.89800
11	20	6 72749 99493 25600 09201	40	13	6 71088 64000 00000 00000	0.87486
5	30	9 31322 57461 54785 15625	41	13	9 25103 10231 50136 29321	0.89638
35	14	41 39545 12236 93847 65625	46	13	41 29065 87698 35408 01536	0.87993
19	17	54 80386 85778 48021 85939	47	13	54 60990 70612 05831 77327	0.88730
6	28	61 40942 21446 48154 97216	23	16	61 32610 41568 09986 48961	0.86842
2	73	94 44732 96573 92904 27392	7	26	93 87480 33764 77543 05649	0.89920
20	17	131 07200 00000 00000 00000	38	14	130 90925 53986 67734 38464	0.86863
2	74	188 89465 93147 85808 54784	39	14	188 32349 19413 17426 09041	0.88695
2	75	377 78931 86295 71617 09568	41	14	379 29227 19491 55588 02161	0.89368
3	49	2392 99329 23061 75295 90083	17	19	2390 72435 68515 13248 47153	0.87071
15	20	3325 25673 00796 50878 90625	37	15	3334 46267 95181 53070 88493	0.89126
19	19	19784 19655 66031 35891 23979	33	16	19779 85201 46255 88779 34081	0.84943
7	29	32199 05755 81317 97268 37607	13	22	32118 38877 95485 51051 57369	0.89390
2	84	1 93428 13113 83406 67952 98816	3	53	1 93832 45667 68001 98967 96723	0.89402
7	30	2 25393 40290 69225 80878 63249	31	17	2 25501 16774 16274 31786 82911	0.86903
11	25	10 83470 59433 88372 20418 30251	34	17	10 84280 35605 96593 23542 07744	0.87991
14	23	22 95856 92886 98149 54822 20544	18	21	22 94682 51895 12940 71398 72768	0.87516
23	20	171 61558 31334 58634 29238 95201	40	17	171 79869 18400 00000 00000 00000	0.89088
6	35	171 90707 99748 42259 10286 58176	23	20	171 61558 31334 58634 29238 95201	0.89829
6	35	171 90707 99748 42259 10286 58176	40	17	171 79869 18400 00000 00000 00000	0.88250
15	25	25251 16829 40423 48861 69433 59375	43	18	25259 93335 73498 06081 18208 06649	0.88234

It follows from (4.6) that

$$\left|\frac{x_2}{X} - \frac{\log p_1}{\log p_2}\right| < \frac{2^{1/10}}{\log 2} \frac{1}{3.1\, X^2} < \frac{1}{2\, X^2},$$

hence x_2/X is a convergent of $\log p_1/\log p_2$, say $x_2 = r_k$, $X = q_k$. Since q_k is at least the $(k+1)$th Fibonacci number, and by $X < 1.97 \times 10^{19}$ (from the examples at the end of Sect. 4.A), we obtain $k \leqslant 92$. The lemma now follows from (4.5) and (4.7). ∎

To solve (4.1), we computed the continued fraction expansions and the convergents of $\log p_1/\log p_2$ exactly, up to the index n such that $q_{n-1} \leqslant 1.97 \times 10^{19} < q_n$. Lemma 4.2 guarantees that $n \leqslant 93$. Doing so, we obtained the result,

THEOREM 4.3. (a) *The diophantine inequality*

$$|p_1^{x_1} - p_2^{x_2}| < \min(p_1^{x_1}, p_2^{x_2})^{\delta} \tag{4.8}$$

with p_1, p_2 primes such that $p_1 < p_2 < 200$, and

$$x_1, x_2 \in \mathbb{Z},\ x_1 \geqslant 2,\ x_2 \geqslant 2, \textit{ and either } \delta = \tfrac{1}{2}$$
$$\textit{or } \delta = \tfrac{9}{10} \textit{ and } \min(p_1^{x_1}, p_2^{x_2}) > 10^{15} \tag{4.9}$$

has only the 77 solutions listed in Table II.

(b) *The diophantine inequality* (4.8) *with p_1, p_2 non-powers such that $2 \leqslant p_1 < p_2 \leqslant 50$ and conditions* (4.9), *has only the 74 solutions listed in Table III.*

In Tables II and III, the column "delta" gives the real number with $|p_1^{x_1} - p_2^{x_2}| = \min(p_1^{x_1}, p_2^{x_2})^{\text{delta}}$. Note that in Theorem 4.3 we do not demand $(x_1, x_2) = 1$. The numerous solutions of (4.8) with $\delta = \frac{9}{10}$ and $\min(p_1^{x_1}, p_2^{x_2}) \leqslant 10^{15}$ can be found without much effort. The computations for the proof of the theorem took 35 sec. We computed approximations of $\log p_i$ by writing it as a suitable linear combination of numbers of the form $\log(1+x)$ for small x, and evaluating $\log(1+x)$ by a Taylor series, taking care to avoid mistakes by rounding-off procedures. Thus we computed explicit rational numbers θ_1, θ_2 with

$$\theta_1 < \log p_1/\log p_2 < \theta_2 < \theta_1 + \varepsilon$$

for a small enough ε. Then as far as the partial quotients of the continued fraction expansions of θ_1 and θ_2 coincide, they coincide with the partial quotients a_i of $\log p_1/\log p_2$. It appeared to be sufficient to take $\varepsilon = 10^{-50}$.

Note that Lemma 4.2. does not yield a decision if

$$a_{k+1} \leqslant p_1^{q_k/10} \frac{1}{q_k} \frac{\log p_2}{2^{1/10}} < a_{k+1} + 2.$$

Since this gap is relatively small, this situation is unlikely to occur. We met only one such a coincidence, namely for $p_1 = 15$, $p_2 = 23$. Here, $\log 15/\log 23 = [0; 1, 6, 2, 1, 51,...]$, so that $a_5 = 51$, $r_4 = 19$, $q_4 = 22$, and $15^{22/10} \frac{1}{22} \log 19/2^{1/10} = 51.4... \in [51, 53)$. We have further $\Lambda = 0.002714... < 0.002771... = 2^{1/10} 15^{-22/10}$, so (4.3) holds. But (4.1) does not hold, since $\log(15^{22} - 23^{19})/\log(23^{19}) = 0.9008...$. This example illustrates that (4.3) is weaker than (4.1). Therefore all found solutions of (4.3) have been checked for (4.1) as well.

4.C. *The Case* $t \geqslant 3$

In this section we show how the L^3-BRA can be used to reduce an upper bound for the solutions of (4.1) in the multi-dimensional case. This will enable us to find all solutions of (4.1) for given $t \geqslant 3$, $p_1,..., p_t$ and δ.

Let x, y be a solution of (4.1). Put $x_i = \operatorname{ord}_{p_i}(x/y)$ $(i = 1,..., t)$, and $X = \max_{1 \leqslant i \leqslant t} |x_i|$. Let C be an upper bound for X, for example, $C = C_5$ (cf. Theorem 4.1). Choose a positive constants $\gamma \in \mathbb{Z}$, $C_0 \in \mathbb{R}$, and put

$$\theta_i = [\gamma C_0 \log p_i] \qquad (i = 1,..., t). \tag{4.10}$$

Consider the lattice $\Gamma \subset \mathbb{Z}^t$, generated by the column vectors of the matrix

$$A = \begin{pmatrix} \gamma & & 0 \\ 0 & \ddots & \gamma \\ \theta_1 & \cdots & \theta_t \end{pmatrix}.$$

Put $\lambda = x_1\theta_1 + \cdots + x_t\theta_t$. Then

$$\mathbf{y} = A \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_t \end{pmatrix} = \begin{pmatrix} \gamma x_1 \\ \vdots \\ \gamma x_{t-1} \\ \lambda \end{pmatrix} \in \Gamma.$$

With this notation we have the following useful lemma.

LEMMA 4.4. *Suppose that for a solution of* (4.1)

$$|\lambda| > \sum_{i=1}^{t} |x_i| \tag{4.11}$$

holds. Then, for $i=1,\ldots,t$,

$$|x_i| < \log\left(2^{1-\delta}\gamma C_0 \Big/ \left(|\lambda| - \sum_{i=1}^{t} |x_i|\right)\right) \Big/ (1-\delta)\log p_i. \tag{4.12}$$

COROLLARY 4.5. *Let* X_0 *be a positive number such that*

$$l(\Gamma) \geqslant (4t^2 + (t-1)\gamma^2)^{1/2} X_0. \tag{4.13}$$

Then (4.1) *has no solutions with for* $i=1,\ldots,t$,

$$\log(2^{1-\delta}\gamma C_0/tX_0)/(1-\delta)\log p_i \leqslant |x_i| \leqslant X_0. \tag{4.14}$$

Proof of Lemma 4.4. Put $\Lambda = \log(x/y) = \sum_{i=1}^{t} x_i \log p_i$. Then

$$|\lambda - \gamma C_0 \Lambda| = \left|\sum_{i=1}^{t} x_i([\gamma C_0 \log p_i] - \gamma C_0 \log p_i)\right| \leqslant \sum_{i=1}^{t} |x_i|,$$

whence, by (4.11),

$$|\Lambda| \geqslant \left(|\lambda| - \sum_{i=1}^{t} |x_i|\right) \Big/ \gamma C_0 > 0.$$

By (4.2) we infer

$$x < 2\,|\Lambda|^{-1/(1-\delta)} \leqslant \left(2^{1-\delta}\gamma C_0 \Big/ \left(|\lambda| - \sum_{i=1}^{t} |x_i|\right)\right)^{1/(1-\delta)}.$$

Now (4.12) follows, since $p_i^{|x_i|} \leqslant \max(x, y) = x$. ∎

Proof of Corollary 4.5. By $x \neq y$ we have $\mathbf{y} \neq \mathbf{0}$. Suppose that $|x_i| \leqslant X_0$ for all i. Then

$$l(\Gamma)^2 \leqslant |\mathbf{y}|^2 = \gamma^2 \sum_{i=1}^{t-1} x_i^2 + \lambda^2 \leqslant (t-1)\gamma^2 X_0^2 + \lambda^2.$$

By (4.3) it follows that

$$\lambda^2 \geqslant l(\Gamma)^2 - (t-1)\gamma^2 X_0^2 \geqslant 4t^2 X_0^2,$$

and we infer

$$|\lambda| - \sum_{i=1}^{t} |x_i| \geqslant 2tX_0 - tX_0 = tX_0.$$

Now apply Lemma 4.4, and the result follows at once. ∎

We use the corollary to reduce the upper bound C for X as follows. Choose C_0 somewhat larger than $(tC)^t$. The parameter γ is used to keep the "rounding-off error" $|\gamma C_0 \log p_i - \theta_i|$ relatively small. (If C_0 is large, then this error is already so small compared to C_0 that it is safe to take $\gamma = 1$.) The θ_i are integers, and are computed exactly. By the L^3-BRA we can compute a lower bound for $l(\Gamma)$ (cf. Lemma 3.1). We may expect that this bound is of size $(\det(\Gamma))^{1/t}$, which is about $\gamma t C$. Thus we may expect that (4.13) holds with $X_0 = C$. Otherwise we may try some larger C_0. If (4.13) holds, then (4.14) gives bounds for $|x_i|$, and thus for X, of size $\log(C_0/C)$, which is of size $\log C$. Hence the reduction of the upper bound is considerable indeed. Lemma 4.4 is more precise than its corollary, and therefore more suitable for reducing a small bound C.

We now proceed with an elaborate example. Let $t = 6$, $p_1, ..., p_6 = 2, ..., 13$, and $\delta = \frac{1}{2}$. By the example at the end of Section 4.A, we know that $X < C$ for $C = 1.35 \times 10^{36}$. We take $C_0 = 10^{240}$, $\gamma = 1$. The values of the θ_i were computed exactly. We applied the L^3-BRA to the corresponding lattice Γ_1, and found a reduced basis $\mathbf{c}_1, ..., \mathbf{c}_6$ with $|\mathbf{c}_1| > 9.40 \times 10^{39}$. So Lemma 3.1 yields

$$l(\Gamma_1) > 2^{-5/2} \times 9.40 \times 10^{39} > 1.66 \times 10^{39}.$$

This is larger than $\sqrt{149}\, C = 1.64... \times 10^{37}$, so (4.13) holds with $X_0 = C$. Hence, by Corollary 4.5,

$$X < \log(2^{1/2} \times 10^{240}/6 \times 1.35 \times 10^{36})/\tfrac{1}{2} \log 2 < 1350.4,$$

so $X \leqslant 1350$. Next we choose $C_0 = 10^{32}$, $\gamma = 1$, and $C = 1350$. The reduced basis of the corresponding lattice Γ_2 was computed, and we found $|\mathbf{c}_1| > 2.71 \times 10^5$. Hence $l(\Gamma_2) > 4.79 \times 10^4$, which is larger than $\sqrt{149}\, C = 1.64... \times 10^4$. So (4.13) holds for $X_0 = C$, and Corollary 4.5 yields

$$\begin{array}{lll} |x_1| \leqslant 187, & |x_2| \leqslant 118, & |x_3| \leqslant 80, \\ |x_4| \leqslant 66, & |x_5| \leqslant 54, & |x_6| \leqslant 50. \end{array} \tag{4.15}$$

Next we choose $C_0 = 10^{12}$, $\gamma = 10^4$. We use Lemma 4.4 as follows. If $|\lambda| > 10^6$ then (4.11) holds by (4.15), and (4.12) yields

$$\begin{array}{lll} |x_1| \leqslant 67, & |x_2| \leqslant 42, & |x_3| \leqslant 29, \\ |x_4| \leqslant 24, & |x_5| \leqslant 19, & |x_6| \leqslant 18. \end{array} \tag{4.16}$$

All vectors in Γ_3 satisfying (4.15) and $|\lambda| \leqslant 10^6$ can be computed with the algorithm of Fincke and Pohst [7] (we omit the details of the computations). We found that there exist only two such vectors, but they do not correspond to solutions of (4.1). Hence all solutions of (4.1) satisfy (4.16). Next we choose $C_0 = 10^8$, $\gamma = 10^4$. If $|\lambda| > 5 \times 10^5$, then (4.12) yields

$$|x_1| \leqslant 42, \quad |x_2| \leqslant 27, \quad |x_3| \leqslant 18,$$
$$|x_4| \leqslant 15, \quad |x_5| \leqslant 12, \quad |x_6| \leqslant 11. \tag{4.17}$$

TABLE IV (Theorem 4.6)

x_1	x_2	x_3	x_4	x_5	x_6	x	y	$x-y$
−1	−11	−1	0	6	0	17 71561	17 71470	91
0	4	5	1	−6	0	17 71875	17 71561	314
21	−2	−2	−1	−3	0	20 97152	20 96325	827
1	13	−1	−3	−1	−2	31 88646	31 88185	461
19	0	0	−8	1	0	57 67168	57 64801	2367
6	2	−1	1	−6	3	88 58304	88 57805	499
−2	15	−1	−2	−4	0	143 48907	143 48180	727
11	−15	0	2	1	1	143 50336	143 48907	1429
1	8	−1	−8	0	3	288 29034	288 24005	5029
−22	5	1	−1	1	3	293 62905	293 60128	2777
13	1	3	−1	1	−6	337 92000	337 87663	4337
1	2	9	−4	−4	0	351 56250	351 53041	3209
3	3	0	4	2	−7	627 52536	627 48517	4019
−26	1	0	5	3	0	671 10351	671 08864	1487
3	−13	10	−2	0	0	781 25000	781 21827	3173
8	−2	−10	4	1	1	878 95808	878 90625	5183
25	1	−4	0	−5	0	1006 63296	1006 56875	6421
−6	1	−2	−6	0	7	1882 45551	1882 38400	7151
8	−13	0	3	−2	3	1929 14176	1929 13083	1093
1	−13	−3	7	2	0	1992 97406	1992 90375	7031
−4	−1	−4	1	−4	7	4392 39619	4392 30000	9619
−4	2	−11	2	6	0	7812 58401	7812 50000	8401
16	−3	5	1	−1	−6	14336 00000	14335 62273	37727
−8	8	0	−8	3	2	14758 24779	14757 89056	35723
−5	−2	−5	11	0	−3	19773 26743	19773 00000	26743
−25	7	1	0	−2	5	40600 88955	40600 86272	2683
2	0	13	−9	−2	0	48828 12500	48827 86447	26053
−14	19	−2	−4	1	−1	1 27848 76137	1 27848 44800	31337
−24	−1	−2	12	−1	0	1 38412 87201	1 38412 03200	84001
−5	5	10	0	1	−8	2 61035 15625	2 61033 83072	1 32553
2	−4	−9	3	7	−2	2 67363 98612	2 67363 28125	70487
18	7	0	−13	0	2	9 68892 08832	9 68890 10407	1 98425
7	−5	3	−9	−3	8	1305 16915 36000	1305 16881 72831	33 63169
−10	10	−6	5	−6	4	2834 49801 04623	2834 49760 00000	41 04623

There are 143 vectors in Γ_4 satisfying (4.16) and $|\lambda| \leqslant 5 \times 10^5$. Of them, 2 correspond to solutions of (4.1), namely the vectors with

$$(x_1, ..., x_6) = (7, -5, 3, -9, -3, 8), \qquad \lambda = 257674,$$
$$(x_1, ..., x_6) = (-10, 10, -6, 5, -6, 4), \qquad \lambda = 144817.$$

Both also satisfy (4.17). Hence all solutions of (4.1) satisfy (4.17).

At this point it seems inefficient to choose appropriate parameters C_0, γ to repeat the procedure with. But the bounds of (4.17) are small enough to admit enumeration. Doing so, we found 605 solutions of (4.1). We cannot list them all here. Instead we give the following result, from which the reader should be able to find all solutions without much effort.

THEOREM 4.6. *The diophantine inequality*

$$0 < x - y < y^{1/2}$$

in x, $y \in S = \{2^{x_1} \cdots 13^{x_6} : x_i \in \mathbb{Z},\ x_i \geqslant 0\ (i = 1, ..., 6)\}$ *with* $(x, y) = 1$ *has exactly* 605 *solutions. Among those*, 571 *satisfy*

$$\mathrm{ord}_2(xy) \leqslant 19, \qquad \mathrm{ord}_3(xy) \leqslant 12, \qquad \mathrm{ord}_5(xy) \leqslant 8,$$
$$\mathrm{ord}_7(xy) \leqslant 7, \qquad \mathrm{ord}_{11}(xy) \leqslant 5, \qquad \mathrm{ord}_{13}(xy) \leqslant 5.$$

The remaining 34 *solutions are listed in Table IV.*

The computation of the reduced basis of Γ_1 took 113 sec, where we applied the L^3-BRA as we described it in Section 3, in 12 steps. The direct search for the solutions of (4.17) took 228 sec. The remaining computations (computation of the $\log p_i$ up to 250 decimal digits, of the reduced basis of Γ_2, and of the short vectors in Γ_3 and Γ_4) took 8 sec. Hence in total we used 349 sec. The numerical details can be obtained from the author.

5. A DIOPHANTINE EQUATION

Let $p_1 < \cdots < p_t$ be prime numbers, where $t \geqslant 3$, and let S be the set of all positive rational integers composed of those primes only. In this section we study the exponential diophantine equation

$$x + y = z \tag{5.1}$$

in x, y, $z \in S$. Without loss of generality we may assume that x, y, z are relatively prime. For any $a \in S$ we define

$$m(a) = \max_{1 \leqslant i \leqslant t} \mathrm{ord}_{p_i}(a).$$

It was proved by Mahler that $m(xyz)$ is bounded for the solutions of (5.1). An explicit bound can be computed (cf. Shorey and Tijdeman [18, Corollary 1.2]). We do so in Section 5.A. In Section 5.B we introduce multi-dimensional p-adic approximation lattices, and in Sections 5.C and 5.D we show how to reduce the found upper bound, and to solve (5.1) completely, in the cases $t=3$ and $t\geqslant 4$, respectively. We conclude with some remarks on a conjecture of Oesterlé and Masser, which is related to Eq. (5.1), in Section 5.E.

5.A. *Upper Bounds*

THEOREM 5.1. *In the above notation, put*

$$s=[2t/3], \qquad P=p_1\cdots p_t,$$

$$V_i=\max(e, \log p_i) \qquad (i=1,\dots,t),\ \Omega=V_{t-s+1}\cdots V_t,$$

$$G_2=2, \qquad G_3=6, \qquad G_{p_i}=p_i-1 \quad \text{if } p_i\geqslant 5, \qquad G=\max_{1\leqslant i\leqslant t} G_{p_i}/\log p_i,$$

$$C_6=2^{9s+26}s^{s+4}\Omega\log(eV_{t-1}).$$

Choose μ, κ *with* $2/(s+1)\leqslant\mu\leqslant 2$, $0<\kappa<\mu/2$, *and put*

$$\varepsilon=(\mu-\kappa)/(1+\kappa)(1+\mu)(s+1),$$

$$k=\max\{(16s)^{(1+1/\kappa)(s+1)}, (8/\varepsilon)^{(1+\mu)(s+1)}, 16^{1/\varepsilon}\},$$

$$C_7=4(s+1)^{(s+1)}k^{(1+\mu)}G\Omega, \qquad C_8=4(C_6+C_7\log(P/p_1))/\log p_1,$$

$$C_9=C_8(\log C_8)^2, \qquad C_{10}=\max(C_9, C_7(\log C_9)^2).$$

Then all solutions of (5.1) *satisfy* $m(xyz)<C_{10}$.

Proof. If we consider instead of (5.1) the equivalent equation

$$x\pm y=z, \tag{5.2}$$

then we may assume that xy has at most s prime divisors. Suppose that $m(xy)\leqslant 7$. Then

$$p_1^{m(z)}\leqslant z\leqslant 2\max(x,y)\leqslant 2(P/p_1)^7,$$

hence

$$m(z)\leqslant\log(2(P/p_1)^7)/\log p_1,$$

and it follows that $m(xyz)<C_{10}$. Now let $m(xy)\geqslant 8$, and suppose $m(z)\geqslant 2$. Then for some $p=p_i$,

$$m(z)=\mathrm{ord}_p(z)=\mathrm{ord}_p(\pm x/y-1)=\mathrm{ord}_p(\log_p(x/y)).$$

Put $x/y = p_{i_1}^{x_{i_1}} \cdots p_{i_s}^{x_{i_s}}$. *Then* $m(xy) = \max(|x_{i_1}|,..., |x_{i_s}|)$. On applying Lemma 2.2 we obtain

$$m(z) \leqslant C_7(\log m(xy))^2. \tag{5.3}$$

Obviously (5.3) is also true if $m(z) < 2$. If in (5.2) the plus sign holds, then

$$(P/p_1)^{m(z)} \geqslant z > \max(x, y) \geqslant p_1^{m(xy)}.$$

By (5.3) it then follows that

$$m(xy) < C_7 \frac{\log(P/p_1)}{\log p_1} (\log m(xy))^2. \tag{5.4}$$

If in (5.2) the minus sign holds, then we apply Lemma 2.1 as follows. Suppose that

$$m(xy) \log p_1 \geqslant (C_6 + C_7 \log(P/p_1))(\log m(xy))^2. \tag{5.5}$$

Then it follows that

$$C_7(\log m(xy))^2 \log(P/p_1) \leqslant m(xy) \log p_1 - \log 2.$$

Note that by (5.3)

$$\left|\frac{y}{x} - 1\right| = \frac{z}{x} = \frac{z}{\max(x, y)} \leqslant \frac{(P/p_1)^{m(z)}}{p_1^{m(xy)}} \leqslant \frac{(P/p_1)^{C_7(\log m(xy))^2}}{p_1^{m(xy)}},$$

so that $|y/x - 1| \leqslant \frac{1}{2}$. Hence

$$|\log(y/x)| \leqslant 2 \log 2 \left|\frac{y}{x} - 1\right| \leqslant 2 \log 2 \frac{(P/p_1)^{C_7(\log m(xy))^2}}{p_1^{m(xy)}}.$$

On the other hand, Lemma 2.1 yields

$$|\log(y/x)| > \exp\{-C_6(\log m(xy) + \log(eV_t))\}.$$

Thus we obtain

$$\begin{aligned} m(xy) \log p_1 < C_7(\log m(xy))^2 \log(P/p_1) + \log(2 \log 2) \\ + C_6(\log m(xy) + \log(eV_t)). \end{aligned}$$

Obviously,

$$C_6(\log m(xy))^2 > \log(2 \log 2) + C_6(\log m(xy) + \log(eV_t)),$$

and we have a contradiction with (5.5). So from (5.4) or from the negation of (5.5) we infer

$$m(xy) < \tfrac{1}{4} C_8 (\log m(xy))^2,$$

and from Lemma 2.3 we obtain $m(xy) < C_9$. Now the result follows from (5.3). ∎

EXAMPLES. With $t = 3$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ we find a minimal value for $k^{1+\mu}$ on taking $\mu = 1$, $\kappa = \frac{5}{13}$, namely $k^{1+\mu} = 2^{108}$. Then $C_{10} < 6.75 \times 10^{41}$. With $t = 6$, $p_1,..., p_6 = 2,..., 13$ we take $\mu = 1$, $\kappa = \frac{3}{7}$, and we find $C_{10} < 3.37 \times 10^{73}$.

5.B. *Approximation Lattices*

In [23] the concept of (2-dimensional) approximation lattices of a p-adic number was introduced. In this subsection we generalize this notion to multi-dimensional approximation lattices of a linear form of p-adic numbers. We confine ourselves to the particular lattices that we use for solving Eq. (5.2), and indicate how a basis of such a lattice can be computed explicitly.

Let p be any of the primes $p_1,..., p_t$. We may assume that $p \nmid xy$. Rename the other primes as $p_0,..., p_{t-2}$, such that $\operatorname{ord}_p(\log_p(p_0))$ is minimal. For $i = 1,..., t-2$ and $m \in \mathbb{N}$, put

$$\theta_i = -\log_p(p_i)/\log_p(p_0) = \sum_{l=1}^{\infty} u_{i,l}\, p^l, \qquad \theta_i^{(m)} = \sum_{l=1}^{m-1} u_{i,l}\, p^l,$$

where $u_{i,l} \in \{0, 1,..., p-1\}$. Then θ_i is a p-adic integer by the choice of p_0, and $\theta_i^{(m)}$ is the unique rational integer satisfying $\operatorname{ord}_p(\theta_i - \theta_i^{(m)}) \geq m$ and $0 \leq \theta_i^{(m)} < p^m$. The $\theta_i^{(m)}$ can be computed for the desired m by using the Taylor series for the p-adic logarithm,

$$\log_p(\chi) = \frac{1}{k} \log_p(1 + (\chi^k - 1)) = \frac{1}{k} \sum_{l=1}^{\infty} (-1)^{l+1} (\chi^k - 1)^l / l,$$

where k is the smallest positive integer such that $\operatorname{ord}_p(\chi^k - 1) \geq 1$.

Consider the lattice $\Gamma_m \subset \mathbb{Z}^{t-1}$ generated by the column vectors $\mathbf{b}_1,..., \mathbf{b}_{t-2}, \mathbf{b}_0$ of the matrix

$$\begin{pmatrix} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ \theta_1^{(m)} & \cdots & \theta_{t-2}^{(m)} & p^m \end{pmatrix}.$$

Put $m_0 = \operatorname{ord}_p(\log_p(p_0))$. Then

$$\begin{aligned}\Gamma_m &= \{(x_1,\dots, x_{t-2}, x_0) \in \mathbb{Z}^{t-1} : |x_1\theta_1 + \cdots + x_{t-2}\theta_{t-2} - x_0|_p \leqslant p^{-m}\}\\ &= \{(x_1,\dots, x_{t-2}, x_0) \in \mathbb{Z}^{t-1} : |\log_p(p_0^{x_0} \cdots p_{t-2}^{x_{t-2}})|_p \leqslant p^{-(m+m_0)}\}.\end{aligned}$$

We call such a lattice an approximation lattice of the p-adic linear form $x_1\theta_1 + \cdots + x_{t-2}\theta_{t-2}$. For $t=3$ we have exactly the approximation lattice of θ_1 in the sense of [23]. (Note that there is a different matrix notation there). Further, consider also the set

$$\Gamma_m^* = \{(x_1,\dots, x_{t-2}, x_0) \in \mathbb{Z}^{t-1} : |p_0^{x_0} \cdots p_{t-2}^{x_{t-2}} \pm 1|_p \leqslant p^{-(m+m_0)}\}.$$

It is clear that Γ_m^* is a sublattice of Γ_m. In general, the two are not equal, since $(x_1,\dots, x_{t-2}, x_0) \in \Gamma_m$ only implies $p_0^{x_0} \cdots p_{t-2}^{x_{t-2}} \equiv \zeta \pmod{p^{m+m_0}}$ for some $(p-1)$th root of unity ζ, not necessarily ± 1. (Recall that $\log_p(\zeta) = 0$ if and only if ζ is a root of unity). For $p = 2, 3$ the only roots of unity in $\mathbb{Q}_p$ are ± 1, so then $\Gamma_m^* = \Gamma_m$.

For $p \geqslant 3$ we show how a basis $\mathbf{b}_1^*,\dots, \mathbf{b}_{t-2}^*, \mathbf{b}_0^*$ of Γ_m^* can be computed from a known basis $\mathbf{b}_1,\dots, \mathbf{b}_{t-2}, \mathbf{b}_0$ of Γ_m. Let ζ be a primitive $(p-1)$th root of unity in $\mathbb{Q}_p$. For any $\mathbf{x} = (x_1,\dots, x_{t-2}, x_0) \in \Gamma_m$ we define $k(\mathbf{x}) \in \mathbb{Z}$ by

$$p_0^{x_0} \cdots p_{t-2}^{x_{t-2}} \equiv \zeta^{k(\mathbf{x})} \pmod{p^{m+m_0}}, \qquad 0 \leqslant k(\mathbf{x}) \leqslant p-2.$$

Then $k(\mathbf{x})$ is $(\operatorname{mod}(p-1))$ a linear function on Γ_m, and $\mathbf{x} \in \Gamma_m^*$ if and only if $\frac{1}{2}(p-1) \mid k(\mathbf{x})$. Put

$$k = \gcd(k(\mathbf{b}_0),\dots, k(\mathbf{b}_{t-2})),$$

and compute (by the euclidean algorithm) a basis $\mathbf{b}'_1,\dots, \mathbf{b}'_{t-2}, \mathbf{b}'_0$ of Γ_m such that $k(\mathbf{b}'_0) = k$. Put for $i = 1,\dots, t-2$,

$$\gamma_i \equiv k(\mathbf{b}'_i)/k \pmod{(p-1)/2}, \qquad |\gamma_i| \leqslant (p-1)/4,$$
$$\mathbf{b}_i^* = \mathbf{b}'_i - \gamma_i \mathbf{b}'_0.$$

Then $k(\mathbf{b}_i^*) \equiv k(\mathbf{b}'_i) - \gamma_i k(\mathbf{b}'_0) \equiv 0 \pmod{(p-1)/2}$ $(i = 1,\dots, t-2)$. Put

$$\gamma_0 = \operatorname{lcm}(k, (p-1)/2)/k,$$

which is the smallest positive integer such that $\gamma_0 k \equiv 0 \pmod{(p-1)/2}$. Every $\mathbf{x} \in \Gamma_m$ can be written as

$$\mathbf{x} = y_1\mathbf{b}_1^* + \cdots + y_{t-2}\mathbf{b}_{t-2}^* + y_0\mathbf{b}'_0, \qquad y_i \in \mathbb{Z},$$

since $\mathbf{b}_1^*,\dots, \mathbf{b}_{t-2}^*, \mathbf{b}'_0$ is a basis of Γ_m. Now,

$$k(\mathbf{x}) \equiv y_0 k \pmod{(p-1)/2}.$$

So $\mathbf{x} \in \Gamma_m^*$ if and only if $\gamma_0 \mid y_0$. Hence put

$$\mathbf{b}_0^* = \gamma_0 \mathbf{b}_0',$$

then it follows that $\mathbf{b}_1^*, \ldots, \mathbf{b}_{t-2}^*, \mathbf{b}_0^*$ is a basis of Γ_m^*. In practice it may occur that p_0 can be chosen such that it is a primitive root $(\bmod\, p)$. Then choose $\zeta \equiv p_0 \pmod p$, and it follows from $k(\mathbf{b}_0) = 1$ that $\mathbf{b}_i' = \mathbf{b}_i$ $(i = 0, \ldots, t-2)$. If $p_i \equiv p_0^{\alpha_i} \pmod p$, then

$$\gamma_i \equiv \alpha_i + \theta_i^{(m)} \equiv \alpha_i + \sum_{l=0}^{m-1} u_{i,l} \pmod{(p-1)/2} \qquad (i = 1, \ldots, t-2),$$

$$\gamma_0 = (p-1)/2.$$

So in this special case it is simple to find a basis of Γ_m^*.

For any solution x, y, z of (5.2) put $x/y = p_0^{x_0} \cdots p_{t-2}^{x_{t-2}}$, and consider the point $\mathbf{x} = (x_1, \ldots, x_{t-2}, x_0) \in \mathbb{Z}^{t-1}$. Suppose that $\operatorname{ord}_p(z) \geqslant 2$. Then

$$\begin{aligned} \operatorname{ord}_p(z) &= \operatorname{ord}_p(x/y \pm 1) = \operatorname{ord}_p(\log_p(x/y)) \\ &= \operatorname{ord}_p(x_1\theta_1 + \cdots + x_{t-2}\theta_{t-2} - x_0) + m_0. \end{aligned}$$

Hence $\mathbf{x} \in \Gamma_m^*$ for $m \leqslant \operatorname{ord}_p(z) - m_0$. With this notation we have the following useful lemma:

LEMMA 5.2. *Let $m \in \mathbb{N}$ and $X_0 > 0$ be constants such that*

$$l(\Gamma_m^*) > (t-1)^{1/2} X_0. \tag{5.6}$$

Then (5.2) *has no solutions x, y, z with*

$$m + m_0 \leqslant \operatorname{ord}_p(z) \leqslant m(xyz) \leqslant X_0. \tag{5.7}$$

Proof. Suppose (5.7) holds. By $\operatorname{ord}_p(z) \geqslant m + m_0$ we have $\mathbf{x} \in \Gamma_m^*$, $\mathbf{x} \neq \mathbf{0}$. Further, $|x_i| \leqslant m(xyz) \leqslant X_0$ $(i = 0, \ldots, t-2)$. Hence

$$l(\Gamma_m^*)^2 \leqslant |\mathbf{x}|^2 = \sum_{i=0}^{t-2} x_i^2 \leqslant (t-1)\, X_0^2,$$

which contradicts (5.6). ∎

Suppose that we know that $m(xyz) \leqslant X_0$. We may expect that $l(\Gamma_m^*)$ is of size $(\det(\Gamma_m^*))^{1/(t-1)}$, which is about $p^{m/(t-1)}$. Thus we may expect that it will suffice to take m somewhat larger than $(t-1)\log(\sqrt{t-1}\, X_0)/\log p$. If (5.6) does not hold then, we may try some larger m. If (5.6) holds, then (5.7) yields $\operatorname{ord}_p(z) \leqslant m + m_0$. We repeat this procedure for $p = p_1, \ldots, p_t$. Since (5.2) is invariant under permutation of x, y, z we find a new upper bound for $m(xyz)$, which is of size $m \simeq \log X_0$.

5.C. *The Case* $t=3$

We illustrate the use of the p-adic analogue of the one-dimensional continued fraction algorithm by solving the equation

$$x \pm y = wz, \tag{5.8}$$

where $x, y, z \in \{p^k : p = 2, 3, 5, k \in \mathbb{Z}, k \geqslant 0\}$, and $w \in \mathbb{Z}$, $|w| \leqslant 10^6$, $(w, z) = 1$. Put $X = \max_{p=2,3,5} \operatorname{ord}_p(xyz)$. The example at the end of Section 5.A shows that in the case $|w| = 1$ we have $X < 6.75 \times 10^{41}$. It can be checked without difficulties that the effect of the w with $|w| \leqslant 10^6$ can be neglected, so that for the solutions of (5.8) also $X < 6.75 \times 10^{41}$ holds. Put for $p = 2$, 3, or 5,

$$x/y = p_0^{x_0} p_1^{x_1}, \qquad z = p^u,$$

such that

$$\theta = -\log_p p_1 / \log_p p_0$$

is a p-adic integer. Then define the lattices Γ_m and Γ_m^* as in Section 5.B, so Γ_m is generated by

$$\mathbf{b}_1 = \begin{pmatrix} 1 \\ \theta^{(m)} \end{pmatrix}, \qquad \mathbf{b}_0 = \begin{pmatrix} 0 \\ p^m \end{pmatrix}.$$

For $p = 2$, 3, we have $\Gamma_m^* = \Gamma_m$, and for $p = 5$ a basis of Γ_m^* is

$$\mathbf{b}_1^* = \mathbf{b}_1 - \gamma \mathbf{b}_0, \qquad \mathbf{b}_0^* = 2\mathbf{b}_0,$$

where $\gamma = 0$ if $\theta^{(m)}$ is odd, $\gamma = 1$ if $\theta^{(m)}$ is even. Using the algorithm of [23, Sect. 3], we can compute a basis $\mathbf{c}_1$, $\mathbf{c}_2$ of Γ_m^* that is reduced in the sense that

$$\mathbf{c}_1 = \begin{pmatrix} c_{1,1} \\ c_{1,2} \end{pmatrix}$$

has minimal norm $\Phi(\mathbf{c}_1) = \max(|c_{1,1}|, |c_{1,2}|)$ in $\Gamma_m^* \setminus \{\mathbf{0}\}$. We choose p, p_0, p_1, and m as in the following table, where m is chosen so that p^m is somewhat larger than $(6.75 \times 10^{41})^2$:

p	p_0	p_1	m_0	m	γ	$\Phi(\mathbf{c}_1) >$	$u \leqslant$	W	$\lvert x_0\rvert \leqslant$	$\lvert x_1\rvert \leqslant$
2	3	5	2	297		2^{148}	298	$10^6 \times 2^{298}$	222	152
3	2	5	1	189		3^{94}	189	$10^6 \times 3^{189}$	354	152
5	2	3	1	135	0	5^{67}	135	$10^6 \times 5^{135}$	370	233

We give the values of $\theta^{(m)}$ in Table V, and the reduced bases of the Γ_m^* in Table VI. From this table we find the lower bounds for $\Phi(\mathbf{c}_1)$ given above.

TABLE V (Section 5C)

(p-adic notation: $0.abc... = a + b.p + c.p^2 + \cdots$)

theta = $-\log_2 5/\log_2 3$ =

0.10101 11101 00001 11110 11000 10101 00000 01001 11101 00010 10000 10011 10110 10000 01011 11100 00001 11010 00000 00001
00010 11100 11100 10111 01001 01101 11000 01010 01110 01010 11110 00000 00101 00110 00100 00011 01111 01110 01010 11101
10010 01001 00001 10100 00111 00001 11111 01111 00011 10110 00000 00101 01101 01100 00010 01110 11100 11101 11011 01011
10111 0....

theta = $-\log_3 5/\log_3 2$ =

0.11022 12121 22001 12010 21102 10210 10022 20210 20010 10112 22201 21021 21022 10000 22020 12012 02022 21001 00012 02020
21210 12202 12200 00000 10120 00211 12021 10120 02100 10222 22122 01201 21111 11121 11001 20222 10000 20121 22221....

theta = $-\log_5 3/\log_5 2$ =

0.33002 02003 04411 23120 44012 01011 00044 43204 30340 00023 14333 12413 43420 40302 10202 44104 32433 24432 03021 12311
34044 40231 04112 33230 00242 14232 14400 3110....

TABLE VI (Section 5C)

$p = 2$ (base-2 notation)

$$\mathbf{b}_1 = \begin{pmatrix} \begin{array}{r} -101\ 11001\ 00011\ 11100\ 10101\ 01010\ 01110\ 00101\ 11110 \\ 10000\ 11000\ 11100\ 10011\ 11001\ 01110\ 10000\ 10001\ 00011\ 11110\ 01100\ 10011\ 01101\ 01000\ 11110\ 01001\ 10111\ 10010\ 11001\ 10111 \\ -1010\ 11101\ 01011\ 00011\ 00000\ 00111\ 01001\ 11001\ 10010\ 10110 \\ 00111\ 00001\ 01100\ 11101\ 00011\ 01001\ 00100\ 10101\ 11011\ 10011\ 00011\ 01011\ 01011\ 00110\ 11111\ 11110\ 10100\ 01010\ 01101\ 00011 \end{array} \end{pmatrix}$$

$$\mathbf{b}_2 = \begin{pmatrix} \begin{array}{r} 1011\ 10001\ 10101\ 01101\ 10111\ 10101\ 01111\ 10111\ 00001\ 01010 \\ 11010\ 10001\ 10011\ 11111\ 01101\ 10110\ 01100\ 11001\ 00101\ 10000\ 00011\ 00100\ 01010\ 00101\ 01011\ 10000\ 00111\ 01100\ 10101\ 10110 \\ -1010\ 01101\ 01110\ 11110\ 10000\ 00000\ 10001\ 11000\ 10111\ 00100 \\ 01010\ 11000\ 11110\ 11101\ 10101\ 11110\ 00011\ 10101\ 01000\ 11010\ 01001\ 01100\ 10111\ 00110\ 10101\ 01110\ 11100\ 00010\ 11110\ 10010 \end{array} \end{pmatrix}$$

$p = 3$ (base-3 notation)

$$\mathbf{b}_1 = \begin{pmatrix} \begin{array}{r} 1110\ 00102\ 10211\ 22010\ 20100\ 10022\ 10001\ 20220\ 12202\ 01102\ 11202\ 11110\ 20112\ 22101\ 20022\ 22112\ 10020\ 10022\ 12000 \\ 2000\ 11110\ 21111\ 10112\ 10102\ 10210\ 22101\ 01021\ 10212\ 10020\ 11002\ 12222\ 20012\ 11101\ 01222\ 11211\ 01201\ 22201\ 02000 \end{array} \end{pmatrix}$$

$$\mathbf{b}_2 = \begin{pmatrix} \begin{array}{r} 2102\ 21112\ 02001\ 22101\ 01111\ 00222\ 12000\ 20022\ 02011\ 12200\ 21221\ 00200\ 00120\ 20210\ 01100\ 12210\ 10222\ 00022\ 20202 \\ -12001\ 10002\ 21010\ 00220\ 10200\ 02122\ 00221\ 22120\ 22100\ 10120\ 12020\ 20120\ 22012\ 10011\ 10022\ 01122\ 22222\ 22212\ 02001 \end{array} \end{pmatrix}$$

$p = 5$ (base-5 notation)

$$\mathbf{b}_1 = \begin{pmatrix} \begin{array}{r} -213\ 21041\ 20044\ 21011\ 03000\ 00420\ 40302\ 13144\ 33303\ 42143\ 22021\ 31233\ 42233\ 42314 \\ -140\ 01221\ 40144\ 10323\ 41221\ 10113\ 13410\ 44144\ 41032\ 21131\ 43034\ 40322\ 11323\ 43022 \end{array} \end{pmatrix}$$

$$\mathbf{b}_2 = \begin{pmatrix} \begin{array}{r} -200\ 20012\ 43403\ 13232\ 12424\ 44102\ 00032\ 42321\ 20012\ 14134\ 22130\ 20103\ 00020\ 13301 \\ 233\ 01424\ 42013\ 24004\ 43244\ 32120\ 30230\ 23141\ 22340\ 40304\ 31113\ 30442\ 33443\ 20012 \end{array} \end{pmatrix}$$

They are all larger than 6.75×10^{41}. Hence for the solutions of (5.8) we have $u \leqslant m + m_0$, and $|w| z \leqslant W$, as shown in the table above. We now find the new upper bounds for $|x_0|$, $|x_1|$ as follows. If in (5.8) the minus sign holds, then, on supposing that $\min(x, y) > W^{10/9}$, we infer

$$|x - y| = |w| z \leqslant W < \min(x, y)^{9/10}.$$

By Theorem 4.3a and Table II, the inequality $|x - y| < \min(x, y)^{9/10}$ has no solutions with $\min(x, y) > W$, since $W > 10^{100}$. Hence $\min(x, y) \leqslant W^{10/9}$, and we infer

$$\max(x, y) \leqslant \min(x, y) + |w| z \leqslant W^{10/9} + W.$$

If in (5.8) the plus sign holds, this inequality follows at once. So now the bounds for $|x_0|$, $|x_1|$ follow from

$$|x_i| \log p_i \leqslant \log \max(x, y) \leqslant \log(W^{10/9} + W).$$

We repeat the procedure with m as in the following table:

p	m	γ	$\Phi(\mathbf{c}_1) >$	$u \leqslant$	W	$\lvert x_0\rvert \leqslant$	$\lvert x_1\rvert \leqslant$
2	17		260	18	$10^6 \times 2^{18}$	31	21
3	13		531	13	$10^6 \times 3^{13}$	49	21
5	8	1	818	8	$10^6 \times 5^8$	49	31

The numbers are now so small that the computations can be performed by hand. For example, for $p = 5$ the lattice Γ_8^* is generated by

$$\mathbf{b}_1^* = \begin{pmatrix} 1 \\ -358107 \end{pmatrix}, \qquad \mathbf{b}_0^* = \begin{pmatrix} 0 \\ 781250 \end{pmatrix},$$

and a reduced basis is

$$\mathbf{c}_1 = \begin{pmatrix} -24 \\ 818 \end{pmatrix}, \qquad \mathbf{c}_2 = \begin{pmatrix} 949 \\ 207 \end{pmatrix}.$$

Now, in all three cases, $W^{10/9} < 10^{15}$. On supposing $\min(x, y) > 10^{15}$ we infer

$$|x - y| = |w| z \leqslant W < 10^{15 \times 9/10} < \min(x, y)^{9/10}.$$

By Theorem 4.3a and Table II we see that the inequality $|x - y| < \min(x, y)^{9/10}$ has only two solutions: $(x, y) = (2^{65}, 5^{28})$, $(2^{84}, 3^{53})$. However, both have $|x - y| > 10^{15 \times 9/10}$. So we infer $\min(x, y) \leqslant 10^{15}$, hence by $\max(x, y) \leqslant 10^{15} + W$ we obtain the bounds for $|x_0|$, $|x_1|$ as given above.

TABLE VII (Theorem 5.3)

$p=2,\ p_0=3,\ p_1=5$

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
2	9	10	9765625	−1	4	−610351
10	59049	10	9765625	−1	4	−606661
4	81	12	244140625	−1	9	−476837
6	729	10	9765625	−1	5	−305153
2	9	8	390625	−1	3	−48827
6	729	8	390625	−1	3	−48737
10	59049	8	390625	−1	3	−41447
14	4782969	10	9765625	−1	7	−38927
4	81	8	390625	−1	4	−24409
0	1	8	390625	−1	5	−12207
8	6561	8	390625	−1	6	−6001
0	1	6	15625	−1	3	−1953
4	81	6	15625	−1	3	−1943
8	6561	6	15625	−1	3	−1133
6	729	6	15625	−1	4	−931
2	9	4	625	−1	3	−77
2	9	6	15625	−1	8	−61
0	1	4	625	−1	4	−39
4	81	4	625	−1	5	−17
0	1	2	25	−1	3	−3
2	9	2	25	−1	4	−1
1	3	1	5	1	3	1
1	3	3	125	1	7	1
2	9	0	1	−1	3	1
3	27	1	5	1	5	1
4	81	0	1	−1	4	5
4	81	2	25	−1	3	7
6	729	2	25	−1	6	11
6	729	4	625	−1	3	13
3	27	3	125	1	3	19
5	243	3	125	1	4	23
5	243	1	5	1	3	31
7	2187	5	3125	1	6	83
6	729	0	1	−1	3	91
7	2187	1	5	1	4	137
11	177147	1	5	1	10	173
3	27	5	3125	1	4	197
8	6561	0	1	−1	5	205
7	2187	3	125	1	3	289
8	6561	4	625	−1	4	371

Table continued

TABLE VII (Theorem 5.3)—*Continued*

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
1	3	5	3125	1	3	391
5	243	5	3125	1	3	421
9	19683	3	125	1	5	619
8	6561	2	25	−1	3	817
10	59049	6	15625	−1	5	1357
5	243	7	78125	1	5	2449
9	19683	1	5	1	3	2461
9	19683	5	3125	1	3	2851
10	59049	2	25	−1	4	3689
12	531441	4	625	−1	7	4147
1	3	7	78125	1	4	4883
9	19683	7	78125	1	4	6113
13	1594323	7	78125	1	8	6533
10	59049	4	625	−1	3	7303
10	59049	0	1	−1	3	7381
12	531441	8	390625	−1	4	8801
3	27	7	78125	1	3	9769
7	2187	7	78125	1	3	10039
11	177147	5	3125	1	4	11267
3	27	9	1953125	1	7	15259
11	177147	3	125	1	3	22159
11	177147	7	78125	1	3	31909
12	531441	0	1	−1	4	33215
12	531441	6	15625	−1	3	64477
12	531441	2	25	−1	3	66427
11	177147	9	1953125	1	5	66571
13	1594323	3	125	1	4	99653
7	2187	9	1953125	1	4	122207
14	4782969	2	25	−1	5	149467
13	1594323	1	5	1	3	199291
13	1594323	5	3125	1	3	199681
1	3	9	1953125	1	3	244141
5	243	9	1953125	1	3	244171
9	19683	9	1953125	1	3	246601
14	4782969	6	15625	−1	4	297959
13	1594323	9	1953125	1	3	443431
15	14348907	5	3125	1	5	448501
14	4782969	8	390625	−1	3	549043
14	4782969	4	625	−1	3	597793
14	4782969	0	1	−1	3	597871
16	43046721	0	1	−1	6	672605
9	19683	11	48828125	1	6	763247
15	14348907	1	5	1	4	896807

Table continued

TABLE VII (Theorem 5.3)—*Continued*

$p = 3$, $p_0 = 2$, $p_1 = 5$						
x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
14	16384	10	9765625	−1	4	−120361
9	512	9	1953125	−1	3	−72319
4	16	8	390625	−1	3	−14467
12	4096	6	15625	−1	3	−427
7	128	5	3125	−1	4	−37
2	4	4	625	−1	3	−23
1	2	2	25	1	3	1
5	32	1	5	−1	3	1
6	64	3	125	1	3	7
11	2048	4	625	1	5	11
9	512	0	1	1	3	19
10	1024	2	25	−1	3	37
3	8	6	15625	1	4	193
15	32768	3	125	−1	4	403
14	16384	1	5	1	3	607
17	131072	7	78125	−1	3	1961
16	65536	5	3125	1	3	2543
8	256	7	78125	1	3	2903
19	524288	2	25	1	4	6473
18	262144	0	1	−1	3	9709
23	8388608	1	5	−1	6	11507
13	8192	8	390625	1	3	14771
22	4194304	8	390625	−1	5	15653
10	1024	11	48828125	1	7	22327
18	262144	9	1953125	1	4	27349
20	1048576	4	625	−1	3	38813
0	1	9	1953125	1	3	72338
21	2097152	6	15625	1	3	78251
5	32	10	9765625	1	3	361691
24	16777216	3	125	1	3	621383
23	8388608	10	9765625	1	3	672379
26	67108864	7	78125	1	4	829469

$p = 5$, $p_0 = 2$, $p_1 = 3$						
x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
12	4096	16	43046721	−1	3	−344341
5	32	15	14348907	−1	3	−114791
7	128	1	3	−1	3	1
6	64	8	6561	1	3	53
14	16384	2	9	−1	3	131
13	8192	9	19683	1	3	223
20	1048576	10	59049	1	3	8861
21	2097152	3	27	−1	3	16777

Those bounds are small enough to admit enumeration of the remaining cases. Thus we obtain the following result.

THEOREM 5.3. *The diophantine equation*

$$x \pm y = wz,$$

where $x = p_0^{x_0}$, $y = p_1^{x_1}$, $z = p^u$, $(p, p_0, p_1) = (2, 3, 5)$, $(3, 2, 5)$, *or* $(5, 2, 3)$, x_0, x_1, u *are nonnegative integers,* $w \in \mathbb{Z}$, $|w| \leqslant 10^6$, *and* $p \nmid w$ *has exactly* 291 *solutions for* $p = 2$, 412 *solutions for* $p = 3$, *and* 570 *solutions for* $p = 5$. *In Table VII all solutions with* $u \geqslant 3$ *are given.*

The computer calculations for the proof of this theorem took 3 sec.

5.D. *The Case* $t \geqslant 4$

In this section we present an elaborate example of the use of the L^3-BRA for solving an equation of type (5.2) in the multi-dimensional case. Let S be the set of positive integers composed of the primes 2, 3, 5, 7, 11, 13 only. In the example at the end of Section 5.A. we have seen that the solutions x, y, $z \in S$ of (5.2) satisfy $m(xyz) < 3.37 \times 10^{73}$. We show how to reduce this bound, and thus we are able to find all solutions. With the notation of Section 5.B we choose the following parameters:

p	p_0	p_1	p_2	p_3	p_4	m_0	m	γ_0	γ_1	γ_2	γ_3	γ_4
2	3	5	7	11	13	2	1320					
3	2	5	7	11	13	1	840					
5	2	3	7	11	13	1	600	2	1	0	0	1
7	3	2	5	11	13	1	480	3	0	0	−1	1
11	2	3	5	7	13	1	360	5	−2	−1	2	0
13	2	3	5	7	11	1	360	6	3	1	−2	1

We computed the six values of the $\theta_i^{(m)}$ $(i = 1, 2, 3, 4)$, and the reduced bases of the six lattices Γ_m^*. Thus we obtained

p	$l(\Gamma_m{}^*) \geqslant \|\mathbf{c}_1\|/4 >$	$\mathrm{ord}_p(xyz) \leqslant$
2	6.34×10^{79}	1321
3	2.50×10^{79}	840
5	2.02×10^{83}	600
7	2.39×10^{80}	480
11	2.28×10^{74}	360
13	4.23×10^{79}	360

These lower bounds for $l(\Gamma_m^*)$ are all larger than $\sqrt{5} \times 3.37 \times 10^{73}$. So we may apply Lemma 5.2 with $X_0 = 3.37 \times 10^{73}$, which is the theoretical upper bound for $m(xyz)$. For every p we thus find $\mathrm{ord}_p(z) \leqslant m + m_0$. Since Eq. (5.2) is invariant under permutations of x, y, z, we even have $\mathrm{ord}_p(xyz) \leqslant m + m_0$, as shown in the above table. Hence $m(xyz) \leqslant 1321$.

We repeated the procedure with $X_0 = 1321$ and m as in the following table. After computing the reduced bases of the six lattices Γ_m^* we found the following data (Note that in all cases $l(\Gamma_m^*) \geqslant \sqrt{5} \times 1321$.)

p	m	γ_0	γ_1	γ_2	γ_3	γ_4	$l(\Gamma_m^*) >$	$\mathrm{ord}_p(xyz) \leqslant$
2	77						8342	78
3	49						9026	49
5	35	2	0	1	1	0	22325	35
7	28	3	0	-1	1	0	14403	28
11	21	5	1	1	1	-2	5162	21
13	21	6	0	0	1	2	14779	21

Hence $m(xyz) \leqslant 78$. Next, we repeated the procedure with $X_0 = 78$, and m as in the following table. We found

p	m	γ_0	γ_1	γ_2	γ_3	γ_4	$l(\Gamma_m^*) >$	$\mathrm{ord}_p(xyz) \leqslant$
2	55						364	56
3	35						301	35
5	25	2	1	1	1	0	622	25
7	20	3	1	-1	1	0	693	20
11	15	5	1	2	-2	-2	192	15
13	15	6	1	0	3	2	658	15

Hence $m(xyz) \leqslant 56$.

To find the solutions of (5.2) with $\mathrm{ord}_p(xyz)$ below the bounds given in the above table, we followed the following procedure. Suppose that we are at a certain moment interested in finding the solutions with $\mathrm{ord}_p(xyz) \leqslant f(p)$, where $f(p)$ is given for $p = 2, \ldots, 13$. Choose a p and an $m < f(p) - m_0$, and consider the lattice Γ_m^*. If a solution x, y, z of (5.2) exists with $\mathrm{ord}_p(z) \geqslant m + m_0$, then the vector

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_4 \\ x_0 \end{pmatrix}$$

TABLE VIII (Section 5D)

p	m	n	p	m	n
2	44	–	5	7	–
3	28	–	5	6	–
5	20	–	5	5	6
7	16	–	7	7	–
11	12	–	7	6	–
13	12	–	7	5	1
2	33	–	7	4	4
3	21	–	11	5	–
5	15	–	11	4	1
7	12	–	11	3	4
11	9	–	13	5	–
13	9	–	13	4	–
2	22	–	13	3	1
3	14	–	2	10	2
5	10	–	2	9	3
7	8	–	2	8	6
11	6	–	2	7	15
13	6	–	2	6	16
2	21	–	2	5	26
2	20	–	2	4	31
2	19	–	2	3	44
2	18	–	3	6	5
2	17	–	3	5	8
2	16	–	3	4	16
2	15	–	3	3	35
2	14	–	3	2	54
2	13	1	3	1	87
2	12	2	5	4	1
2	11	2	5	3	5
3	13	–	5	2	18
3	12	–	5	1	36
3	11	–	7	3	–
3	10	1	7	2	6
3	9	1	7	1	18
3	8	1	11	2	1
3	7	6	11	1	8
5	9	–	13	2	–
5	8	–	13	1	4

(n = number of solutions found.)

with $x_i = \mathrm{ord}_{p_i}(x/y)$ $(i=0,..., 4)$ is in the lattice. Its length is bounded by $(f(p_0)^2 + \cdots + f(p_4)^2)^{1/2}$. All vectors in Γ_m^* with length below this bound can be computed by the algorithm of Fincke and Pohst [7] (we omit details). Then all solutions of (5.2) corresponding to lattice points can be selected. Then we replace $f(p)$ by $m + m_0 - 1$, and we may repeat the procedure for newly chosen p, m.

We performed this procedure, starting with the bounds for $\mathrm{ord}_p(xyz)$ given in the above table for $f(p)$, and with p, m as in Table VIII. At the end we have $f(2) = 4$, $f(p) = 1$ for $p = 3,..., 13$. The remaining solutions can be found by hand. Thus we obtained the following result.

THEOREM 5.4. *The diophantine equation*

$$x + y = z$$

in $x, y, z \in S = \{2^{x_1} \cdots 13^{x_6}: x_i \in \mathbb{Z},\ x_i \geqslant 0\ (i = 1,..., 6)\}$ *with* $(x, y) = 1$ *and* $x \leqslant y$, *has exactly* 545 *solutions. Of them,* 514 *satisfy*

$$\mathrm{ord}_2(xyz) \leqslant 12, \qquad \mathrm{ord}_3(xyz) \leqslant 7, \qquad \mathrm{ord}_5(xyz) \leqslant 5,$$
$$\mathrm{ord}_7(xyz) \leqslant 4, \qquad \mathrm{ord}_{11}(xyz) \leqslant 3, \qquad \mathrm{ord}_{13}(xyz) \leqslant 3.$$

The remaining 31 *solutions are given in Table IX.*

The computer calculations for the proof of this theorem took 2856 sec, of which 2830 sec were used for the first reduction step. In this first step, we applied the L^3-BRA in 12 steps (cf. Sect. 3), which costed on average about 400 sec. The remaining 430 sec were mainly used for the computation of the 24 $\theta_i^{(m)}$'s. Full numerical details can be obtained from the author.

5.E. *Examples Related to the Oesterlé–Masser Conjecture*

Let x, y, z be positive integers. Put

$$G = \prod_{\substack{p \mid xyz \\ p \text{ prime}}} p.$$

For all x, y, z with $(x, y) = 1$ and

$$x + y = z$$

we define

$$c(x, y, z) = \log z / \log G.$$

TABLE IX (Theorem 5.4)

			$\mathrm{ord}_p(x)$						$\mathrm{ord}_p(y)$						$\mathrm{ord}_p(z)$					
x	y	z	$p=2$	3	5	7	11	13	$p=2$	3	5	7	11	13	$p=2$	3	5	7	11	13
2401	4160	6561	0	0	0	4	0	0	6	0	1	0	0	1	0	8	0	0	0	0
875	6561	7436	0	0	3	1	0	0	0	8	0	0	0	0	2	0	0	0	1	2
1183	6561	7744	0	0	0	1	0	2	0	8	0	0	0	0	6	0	0	0	2	0
1125	8192	9317	0	2	3	0	0	0	13	0	0	0	0	0	0	0	0	1	3	0
1183	8192	9375	0	0	0	1	0	2	13	0	0	0	0	0	0	1	5	0	0	0
16	14625	14641	4	0	0	0	0	0	0	2	3	0	0	1	0	0	0	0	4	0
81	14560	14641	0	4	0	0	0	0	5	0	1	1	0	1	0	0	0	0	4	0
1936	13689	15625	4	0	0	0	2	0	0	4	0	0	0	2	0	0	6	0	0	0
3718	11907	15625	1	0	0	0	1	2	0	5	0	2	0	0	0	0	6	0	0	0
5824	9801	15625	6	0	0	1	0	1	0	4	0	0	2	0	0	0	6	0	0	0
49	16335	16384	0	0	0	2	0	0	0	3	1	0	2	0	14	0	0	0	0	0
2695	13689	16384	0	0	1	2	1	0	0	4	0	0	0	2	14	0	0	0	0	0
8019	8788	16807	0	6	0	0	1	0	2	0	0	0	0	3	0	0	0	5	0	0
3584	14641	18225	9	0	0	1	0	0	0	0	0	0	4	0	0	6	2	0	0	0
1625	16807	18432	0	0	3	0	0	1	0	0	0	5	0	0	11	2	0	0	0	0
3993	16807	20800	0	1	0	0	3	0	0	0	0	5	0	0	6	0	2	0	0	1
49	28512	28561	0	0	0	2	0	0	5	4	0	0	1	0	0	0	0	0	0	4
12936	15625	28561	3	1	0	2	1	0	0	0	6	0	0	0	0	0	0	0	0	4
22000	6561	28561	4	0	3	0	1	0	0	8	0	0	0	0	0	0	0	0	0	4
15625	17303	32928	0	0	6	0	0	0	0	0	0	0	3	1	5	1	0	3	0	0
507	32768	33275	0	1	0	0	0	2	15	0	0	0	0	0	0	0	2	0	3	0
10985	41503	52488	0	0	1	0	0	3	0	0	0	3	2	0	3	8	0	0	0	0
10000	49049	59049	4	0	4	0	0	0	0	0	0	3	1	1	0	10	0	0	0	0
14641	46875	61516	0	0	0	0	4	0	0	1	6	0	0	0	2	0	0	1	0	3
7168	78125	85293	10	0	0	1	0	0	0	0	7	0	0	0	0	8	0	0	0	1
20449	97200	117649	0	0	0	0	2	2	4	5	2	0	0	0	0	0	0	6	0	0
13	151250	151263	0	0	0	0	0	1	1	0	4	0	2	0	0	2	0	5	0	0
12005	161051	173056	0	0	1	4	0	0	0	0	0	0	5	0	10	0	0	0	0	2
121	255879	256000	0	0	0	0	2	0	0	9	0	0	0	1	11	0	3	0	0	0
2197	583443	585640	0	0	0	0	0	3	0	5	0	4	0	0	3	0	1	0	4	0
91	1771470	1771561	0	0	0	1	0	1	1	11	1	0	0	0	0	0	0	0	6	0

TABLE X (Section 5E)

x	y	z	$c(x, y, z)$
$121 = 11^2$	$48234375 = 3^2 5^6 7^3$	$48234496 = 2^{21} 23$	1.62599
1	$4374 = 2\ 3^7$	$4375 = 5^4 7$	1.56789
$343 = 7^3$	$59049 = 3^{10}$	$59392 = 2^{11} 29$	1.54708
$198425 = 5^2 7937$	$96889010407 = 7^{13}$	$96889208832 = 2^{18} 3^7 13^2$	1.49762
$121 = 11^2$	$255879 = 3^9 13$	$256000 = 2^{11} 5^3$	1.48887
37	$32768 = 2^{15}$	$32805 = 3^8 5$	1.48291
$3200 = 2^7 5^2$	$4823609 = 7^6 41$	$4826809 = 13^6$	1.46192
1	$2400 = 2^5 3\ 5^2$	$2401 = 7^4$	1.45567
$702021632 = 2^{19} 13\ 103$	$1977326743 = 7^{11}$	$2679348375 = 3^{11} 5^3 11^2$	1.45261
1	$512000 = 2^{12} 5^3$	$512001 = 3^5 7^2 43$	1.44331
1	$19140624 = 2^4 3^7 547$	$19140625 = 5^8 7^2$	1.43906
$7168 = 2^{10} 7$	$78125 = 5^7$	$85293 = 3^8 13$	1.43501
3	$125 = 5^3$	$128 = 2^7$	1.42657
5	$177147 = 3^{11}$	$177152 = 2^{10} 173$	1.41268

Recently, Oesterlé posed the problem to decide whether there exists an absolute constant C such that $c(x, y, z) < C$ for all x, y, z. Masser conjectured the stronger assertion that $c(x, y, z) < 1 + \varepsilon$, when z exceeds some bound depending on ε only. For a survey of related results and conjectures see Stewart and Tijdeman [19].

It might be interesting to have some empirical results on $c(x, y, z)$, and to search for x, y, z for which it is large. From the preceding sections it may be clear that such x, y, z correspond to relatively short vectors in appropriate approximation lattices. As a byproduct of the proofs of Theorems 4.6 and 5.4 we computed the value of $c(x, y, z)$, corresponding to many short vectors that we came across in performing the algorithm of Fincke and Pohst. All examples that we found with $c(x, y, z) \geqslant 1.4$ are listed in Table X. Our search was rather unsystematic, so we do not guarantee that this list is complete in any sense. The largest value for $c(x, y, z)$ that occurred is 1.626, which was reached by

$$x = 11^2, \qquad y = 3^2 \times 5^6 \times 7^3, \qquad z = 2^{21} \times 23.$$

These results do not seem to yield any heuristical evidence for the truth or falsity of the above mentioned conjecture.

Acknowledgments

The author wishes to thank Professor R. Tijdeman and Dr. F. Beukers for their helpful remarks. He was supported by the Netherlands Foundation for Mathematics (SMC) with financial aid from the Netherlands Organization for the Advancement of Pure Research (ZWO). All machine computations were performed on the IBM-3083 computer at the Centraal Reken Instituut of the University of Leiden.

REFERENCES

1. M. K. AGRAWAL, J. H. COATES, D. C. HUNT, AND A. J. VAN DER POORTEN, Elliptic curves of conductor *11*, *Math. Comput.* **35** (1980), 991–1002.
2. L. J. ALEX, Diophantine equations related to finite groups, *Comm. Algebra* **4** (1976), 77–100.
3. A. BAKER, "Transcendental Number Theory," Cambridge Univ. Press, London, 1975.
4. A. BAKER AND H. DAVENPORT, The equations $3x^2-2=y^2$ and $8x^2-7=z^2$, *Quart. J. Math. Oxford (2)* **20** (1969), 129–137.
5. A. J. BRENTJES, "Multi-dimensional Continued Fraction Algorithms," Dissertation, University of Leiden, 1981.
6. W. J. ELLISON, "Recipes for Solving Diophantine Problems by Baker's Method," Sém. de Théorie des Nombres, Talence, 1970–1971, exp. No. 11.
7. 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.
8. J. C. LAGARIAS AND A. M. ODLYZKO, Solving low-density subset sum problems, *J. Assoc. Comput. Mach.* **32** (1985), 229–246.
9. A. K. LENSTRA, H. W. LENSTRA JR., AND L. LOVÁSZ, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.
10. A. K. LENSTRA, "Polynomial-Time Algorithms for the Factorization of Polynomials," Dissertation, University of Amsterdam, 1984.
11. K. MAHLER, "Lectures on Diophantine Approximations I, *g*-adic Numbers and Roth's Theorem," Univ. of Notre Dame Press, Notre Dame, 1961.
12. M. MIGNOTTE AND M. WALDSCHMIDT, Linear forms in two logarithms and Schneider's method, *Math. Ann.* **231** (1978), 241–267.
13. A. M. ODLYZKO AND H. J. J. TE RIELE, Disproof of the Mertens conjecture, *J. Reine Angew. Math.* **357** (1985), 138–160.
14. A. PETHŐ AND B. M. M. DE WEGER, Products of prime powers in binary recurrence sequences, Part I: the hyperbolic case, with an application to the generalized Ramanujan-Nagell equation, *Math. Comput.* **47** (1986), 713–727.
15. A. J. VAN DER POORTEN, Linear forms in logarithms in the *p*-adic case, *in* "Transcendence Theory: Advances and Applications" (A. Baker and D. W. Masser, Eds.), Chap. 2, Academic Press, New York, 1977.
16. H. RUMSEY AND E. C. POSNER, On a class of exponential equations, *Proc. Amer. Math. Soc.* **15** (1964), 974–978.
17. A. SCHINZEL, On two theorems of Gelfond and some of their applications, *Acta Arith.* **13** (1967), 177–236.
18. T. N. SHOREY AND R. TIJDEMAN, "Exponential Diophantine Equations," Cambridge Univ. Press, London, 1986.
19. C. L. STEWART AND R. TIJDEMAN, On the Oesterlé–Masser conjecture, *Monatsh. Math.* **102** (1986), 251–257.
20. R. J. STROEKER AND R. TIJDEMAN, Diophantine equations, *in* "Computational Methods in Number Theory" (H. W. Lenstra, Jr. and R. Tijdeman, Eds.), Part II, MC Tract No. 155, pp. 321–369, Mathematisch Centrum, Amsterdam, 1982.
21. S. S. WAGSTAFF, Solution of Nathanson's exponential congruence, *Math. Comput.* **33** (1979), 1097–1100.

22. M. Waldschmidt, A lower bound for linear forms in logarithms, *Acta Arith.* **37** (1980), 257–283.
23. B. M. M. De Weger, Approximation lattices of p-adic numbers, *J. Number Theory* **24** (1986), 70–88.
24. B. M. M. de Weger, "Products of prime powers in binary recurrence sequences. Part II: The elliptic case, with an application to a mixed quadratic-exponential equation, *Math. Comput.* **47** (1986), 729–739.