Indag. Mathem., N.S., 1 (2), 243-262 June 18, 1990

The weighted sum of two S-units being a square

by B.M.M. de Weger

Faculty of Applied Mathematics, University of Twente, P.O. Box 217, 7500 AE Enschede, the Netherlands

Communicated by Prof. R. Tijdeman at the meeting of October 30, 1989

1. INTRODUCTION

Let $p_1, \ldots, p_s$ ($s \geq 1$) be fixed distinct primes. The set $\mathscr{S} \subset \mathbb{Q}$ of *S-units* is defined as

$$\mathscr{S} = \{ \pm p_1^{x_1} \cdot \cdots \cdot p_s^{x_s} \mid x_i \in \mathbb{Z} \text{ for } i = 1, \ldots, s \}.$$

Let $a, b \in \mathbb{Q} \setminus \{0\}$ be fixed. We study the diophantine equation

$$a \cdot x + b \cdot y = z^2 \tag{1}$$

in $x, y \in \mathscr{S}$, and $z \in \mathbb{Q}$. We show that this equation has essentially only finitely many solutions. Moreover, we indicate how to find all the solutions of this equation for any given set of parameters $a, b, p_1, \ldots, p_s$. Our tools are the theory of p-adic linear forms in logarithms, and a computational p-adic diophantine approximation method. We actually have performed all the necessary computations for solving (1) completely for $p_1, \ldots, p_s = 2, 3, 5, 7$ and $a = b = 1$, and reported on this elsewhere (cf. de Weger [1989], Ch. 7). The type of equation (1) has applications in arithmetic algebraic geometry (cf. Setzer [1975], Pinch [1984]).

2. THE MAIN RESULTS

We start with the treatment of (1) by getting rid of the denominators. Put $S = \mathscr{S} \cap \mathbb{N}$ (with $\mathbb{N} = \{1, 2, 3, \ldots\}$), which is the set of positive rational integers with only $p_1, \ldots, p_s$ as possible prime divisors. Let $x, y \in \mathscr{S}$, $z \in \mathbb{Q}$ be a solution

of (1). There is a $d \in S$ such that $d \cdot |x|$, $d \cdot |y| \in S$, namely the least common multiple of the denominators of x and y. Put $d = d_1 \cdot d_2^2$, with $d_1, d_2 \in \mathbb{N}$ and d_1 squarefree. Then by $d \in S$ it follows that $d_1 \in S$, so there are only finitely many (namely 2^s) possibilities for d_1. Further, let $e \in \mathbb{Z}$ be the least common multiple of the denominators of a and b, so that $e \cdot a, e \cdot b \in \mathbb{Z}$. Put $e = e_1 \cdot e_2^2$, with $e_1, e_2 \in \mathbb{Z}$ and e_1 squarefree. Now put

$$a' = e \cdot e_1 \cdot a, \quad b' = e \cdot e_1 \cdot b,$$

$$x' = d \cdot d_1 \cdot x, \quad y' = d \cdot d_1 \cdot y, \quad z' = d_1 \cdot d_2 \cdot e_1 \cdot e_2 \cdot z.$$

Then $a', b' \in \mathbb{Z}$, and $|x'|, |y'| \in S \subset \mathbb{N}$, and on multiplying by $d \cdot d_1 \cdot e \cdot e_1$ $(= d_1^2 \cdot d_2^2 \cdot e_1^2 \cdot e_2^2)$ equation (1) becomes

$$a' \cdot x' + b' \cdot y' = z'^2.$$

It follows that also $z' \in \mathbb{Z}$. We now drop the dashes, and thus we see that without loss of generality we may study equation (1) with the assumptions

$$(2) \qquad \begin{cases} a, b \in \mathbb{Z},\ p_i \nmid a \cdot b \text{ for } i = 1, \ldots, s, \\ (a, b) \text{ is squarefree}, \\ x \in S,\ y \in S,\ z \in \mathbb{N}, \\ x \geq y, \\ (x, y) \text{ is squarefree}. \end{cases}$$

Here we thus assume that x, y are positive, which is allowed by changing the signs of a and b, if necessary, and the assumption $x \geq y$ is allowed by interchanging a with b, if necessary.

We shall prove the following result.

THEOREM 1. *Let be given $a, b \in \mathbb{Z}$, and prime numbers $p_1, \ldots, p_s$. There exists an effectively computable constant C, depending on a, b and $p_1, \ldots, p_s$ only, such that any solution x, y, z of equation* (1) *with conditions* (2) *satisfies* $\max(x, y, z) < C$.

We shall prove this theorem with a fully explicit constant C, and we shall show how this (usually very large) upper bound can be reduced considerably. This will be of great importance if one wants to find a complete list of solutions. As an example of such an explicit result we quote the following theorem, which has been proved in de Weger [1989], Ch. 7. Note that we do not list all the solutions, but the result is stated in such a way that it is only a small task to compute all the solutions from it.

THEOREM 2. *Let $a = 1$, $b = \pm 1$, and $p_1, \ldots, p_s = 2, 3, 5, 7$. Equation* (1) *with conditions* (2) *has exactly* 388 *solutions. Of these,* 346 *satisfy*

$x \leq 250000,\ y \leq 32000,\ z \leq 500,$

$\max(\mathrm{ord}_2(x), \mathrm{ord}_2(y)) \leq 10,\ \max(\mathrm{ord}_3(x), \mathrm{ord}_3(y)) \leq 8,$

$\max(\mathrm{ord}_5(x), \mathrm{ord}_5(y)) \leq 5,\ \max(\mathrm{ord}_7(x), \mathrm{ord}_7(y)) \leq 4,$

whereas the other 42 solutions are listed in Table I.

Table 1. (Notation: $x_p = \mathrm{ord}_p(x)$, $y_p = \mathrm{ord}_p(y)$ for $p = 2, 3, 5, 7$. Entries printed in boldface are those because of which the solution is exceptional, and thus present in this Table.)

x	x_2	x_3	x_5	x_7	b	y	y_2	y_3	y_5	y_7	z
16384	**14**	0	0	0	−1	14175	0	4	2	1	47
4096	**12**	0	0	0	−1	375	0	1	3	0	61
15625	0	0	**6**	0	−1	10584	3	3	0	2	71
4096	**12**	0	0	0	1	945	0	3	1	1	71
65625	0	1	5	1	−1	**57344**	**13**	0	0	1	91
10240	**11**	0	1	0	−1	1215	0	5	1	0	95
15625	0	0	**6**	0	−1	1701	0	5	0	1	118
14336	**11**	0	0	1	−1	175	0	0	2	1	119
15625	0	0	**6**	0	1	504	3	2	0	1	127
15625	0	0	**6**	0	1	1536	9	1	0	0	131
117649	0	0	0	**6**	−1	**97200**	4	5	2	0	143
16807	0	0	0	**5**	1	13122	1	8	0	0	173
32768	**15**	0	0	0	−1	7	0	0	0	1	181
33614	1	0	0	**5**	−1	125	0	0	3	0	183
129654	1	3	0	4	−1	**78125**	0	0	**7**	0	227
59049	0	**10**	0	0	1	1960	3	0	1	2	247
48384	8	3	0	1	1	15625	0	0	**6**	0	253
59049	0	**10**	0	0	1	7000	3	0	3	1	257
140625	0	2	**6**	0	−1	**43904**	7	0	0	3	311
109375	0	0	**6**	1	−1	1134	1	4	0	**1**	329
137781	0	**9**	0	1	−1	140	2	0	1	1	371
76545	0	7	1	1	1	**71680**	**11**	0	1	1	385
196830	1	**9**	1	0	−1	**33614**	1	0	0	**5**	404
117649	0	0	0	**6**	1	**48000**	7	1	3	0	407
168070	1	0	1	**5**	1	30	1	1	1	0	410
137200	4	0	2	3	1	**59049**	0	**10**	0	0	443
201684	2	1	0	**5**	−1	1875	0	1	4	0	447
252105	0	1	1	**5**	−1	24576	**13**	1	0	0	477
245760	**14**	1	1	0	−1	735	0	1	1	2	495
262144	**18**	0	0	0	1	5145	0	1	1	3	**517**
390625	0	0	**8**	0	−1	**112896**	8	2	0	2	**527**
688905	0	**9**	1	1	−1	5	0	0	1	0	**830**
1058841	0	2	0	**6**	−1	20480	**12**	0	1	0	**1019**
1440000	8	2	4	0	1	2401	0	0	0	4	**1201**
1640625	0	1	7	1	1	336	4	1	0	1	**1281**
4214784	**12**	1	0	3	1	25	0	0	2	0	**2053**
4782969	0	14	0	0	1	4375	0	0	4	1	**2188**
5764801	0	0	0	**8**	−1	9600	7	1	2	0	**2399**
19140625	0	0	**8**	2	−1	17496	3	7	0	0	**4373**
23049600	7	1	2	4	1	1	0	0	0	0	**4801**
76545000	3	7	4	1	1	1	0	0	0	0	**8749**
199290375	0	**13**	3	0	−1	686	1	0	0	3	**14117**

REMARKS

1. We note that in order to prove Theorem 1 in its full generality, it is sufficient to consider only the cases $a=1$, $b=\pm 1$, by adding the prime divisors of a and b to the set of primes $p_1,\dots,p_s$. However, this will seriously increase the value of the upper bound C. Since we are interested in explicit bounds that should be useful for finding all the solutions, it is important that this upper bound C is as small as the method of proof permits. Moreover, the computation time used by the method for reducing the upper bound depends not only on the size of the upper bound C, but also heavily (exponentially) on the number of primes s. Thus in our proof of Theorem 1 we will not make the reduction from the general case to the cases $a=1$, $b=\pm 1$.

2. We stress that the aim of this paper is not only to prove Theorem 1, but to show as well that for any given set of parameters $a, b, p_1,\dots,p_s$ a result similar to Theorem 2 can be proved along the same lines, in a more or less algorithmic way.

3. Equation (1) with conditions (2) can be seen as a further generalization of the generalized Ramanujan-Nagell equation

$$x^2+k=p_1^{n_1}\cdot\cdots\cdot p_s^{n_s}, \tag{3}$$

namely by replacing k by $k\cdot y$ with $|y|\in S$ arbitrary, and multiplying the right hand side by another constant. Equation (3) is studied in Pethö and de Weger [1987], and the method of this paper to solve (1) is a generalization of the method employed there to solve (3).

3. REDUCTION TO PELL-LIKE EQUATIONS

In the following treatment we will allow $z<0$ and $x<y$ (the assumptions $z>0$ and $x\geq y$ are used only in the statement of Theorem 2). Thus we may assume that $a>0$.

Equation (1) can be transformed into a number of Pell-like equations. Put

$$x=D\cdot u^2,$$

where $D, \pm u\in S$, and D is squarefree. There are only 2^s possibilities for D. Thus we treat D as a parameter, not as an unknown. Put $\Delta=a\cdot D$, then $\Delta>0$. Now, (1) is equivalent to a finite number of equations

$$z^2-\Delta\cdot u^2=b\cdot y \tag{4}$$

in $u\in S$, $y\in S$, $z\in\mathbb{Z}$, with $z>0$ and $(u,y)=1$. We treat equation (4), like one usually does with Pell equations, by factoring its both sides in the field $K=\mathbb{Q}(\sqrt{\Delta})$. Note that Δ is not necessarily squarefree. But since $(a,p_i)=1$ for all i, Δ is not a square if $D\neq 1$.

First we consider the special case $\Delta=\delta^2$ for a $\delta\in\mathbb{Z}$ (thus $D=1$ and a is a square). Then (4) is equivalent to

$$\begin{cases} z+\delta\cdot u=b_1\cdot y_1 \\ z-\delta\cdot u=b_2\cdot y_2 \end{cases},$$

where $b = b_1 \cdot b_2$, $y = y_1 \cdot y_2$, $y_1 \in S$, $\pm y_2 \in S$. Subtraction yields

$$(2 \cdot \delta) \cdot u = b_1 \cdot y_1 - b_2 \cdot y_2,$$

where now all variables u, y_1, y_2 (apart from the sign) are in S, hence in $\mathbb{Z}$. This equation is of the form

$$A \cdot X + B \cdot Y = C \cdot Z, \tag{5}$$

where $A, B, C \in \mathbb{Z}$ are constants, and $X, Y, Z \in S$ are variables. In the next section we indicate briefly how to deal with an equation of type (5). We will return to (4) with Δ not a square in Section 5.

4. THE EQUATION $A \cdot X + B \cdot Y = C \cdot Z$

Let $A, B, C \in \mathbb{Z}$ be given. We will study equation (5) in $X, Y, Z \in S$ with the additional (and obvious) assumptions that $p_i \nmid A \cdot B \cdot C$ for all i, and X, Y, Z relatively prime. Note that the case $A = B = C = 1$ has been treated in de Weger [1987], Section 5.

THEOREM 3. *Any solution of equation* (5) *with the above assumptions satisfies*

$$\operatorname{ord}_{p_i}(X \cdot Y \cdot Z) < C_1 \text{ for } i = 1, \ldots, s,$$

where C_1 is an effectively computable constant depending on A, B, C and $p_1, \ldots, p_s$ only.

PROOF. Let for a given solution i be such that $\operatorname{ord}_{p_i}(X \cdot Y \cdot Z)$ is maximal. Since (5) is essentially invariant under permutations of X, Y and Z, we may assume that $p_i \mid Z$, and of course also that even $p_i^2 \mid Z$. Put

$$X/Y = p_1^{x_1} \cdot \cdots \cdot p_s^{x_s}$$

for $x_1, \ldots, x_s \in \mathbb{Z}$ (with $x_i = 0$). Note that

$$\operatorname{ord}_{p_i}(Z) = \operatorname{ord}_{p_i}\left(\frac{A \cdot X}{B \cdot Y} + 1\right) = \operatorname{ord}_{p_i}\left(\frac{A}{B} \cdot p_1^{x_1} \cdot \cdots \cdot p_s^{x_s} + 1\right) \geq 2,$$

hence

$$\operatorname{ord}_{p_i}(Z) = \operatorname{ord}_{p_i}\left(\log_{p_i} \frac{A}{B} + x_1 \cdot \log_{p_i} p_1 + \cdots + x_s \cdot \log_{p_i} p_s\right).$$

From the p-adic theory of linear forms in logarithms (cf. Yu [1987], Yu [1988], Yu [1989], see also our Section 8) and by the choice of i it follows that

$$\operatorname{ord}_{p_i}(Z) < C_2 \cdot \log \max_j |x_j| \leq C_2 \cdot \log \operatorname{ord}_{p_i}(Z)$$

for an effectively computable number C_2, that depends only on $A, B, p_1, \ldots, p_s$. The result now follows at once. □

REMARKS

1. For the case $A=B=C=1$ and $p_1,\dots,p_s=2,3,5,7,11,13$ we found $C_1=5.6\times 10^{27}$ (cf. de Weger [1989], Section 6.2, which improves upon the bound given in de Weger [1987], Section 5.A).

2. Since the upper bound C_1 is very large, it is unavoidable to reduce it considerably, if one wants to find a complete list of solutions. A useful reduction method is that of computational inhomogeneous p-adic diophantine approximation, as described in de Weger [1989], Section 3.12. We use this method in the forthcoming sections of this paper as well. Note that its homogeneous counterpart (cf. de Weger [1987], Section 5.B or de Weger [1989], Section 3.11) has been applied to determine the solutions of (5) in the case $A=B=C=1$ and $p_1,\dots,p_s=2,3,5,7,11,13$, cf. de Weger [1987], Section 5.D.

3. In the proof of Theorem 3 we did not make any attempts to obtain the best possible constant C_1 (given some result from the p-adic theory of linear forms in logarithms). If one is interested in practical computations, it will be advisable to do such attempts, e.g. by adapting the proof of Theorem 5.1 of de Weger [1987] (or Theorem 6.1 of de Weger [1989], which uses a better bound).

5. TOWARDS GENERALIZED RECURRENCES

From now on, let Δ be a non-square. Put $K=\mathbb{Q}(\sqrt{\Delta})$, then $[K:\mathbb{Q}]=2$. Let $\sigma: K\to K$ be the automorphism of K with $\sigma(\sqrt{\Delta})=-\sqrt{\Delta}$. For any number or ideal X in K we write X' for $\sigma(X)$, for convenience. Let $\mathfrak{p}_i$ for $i=1,\dots,s$ be a prime ideal in K dividing p_i. Then we define as usual $\mathrm{ord}_{p_i}(\cdot)=\mathrm{ord}_{\mathfrak{p}_i}(\cdot)/e_{\mathfrak{p}_i}$, where $e_{\mathfrak{p}_i}$ is the ramification index of $\mathfrak{p}_i$. If p_i splits in $\mathcal{O}_K$, this defines a choice from the two possibilities for $\sqrt{\Delta}\pmod p$. Put for a solution z,u,y of (4)

$$\chi=z+u\cdot\sqrt{\Delta}.$$

Then $b\cdot y=\chi\cdot\chi'$, and by $(u,y)=1$ we have

$$\min(\mathrm{ord}_{p_i}(u),\mathrm{ord}_{p_i}(y))=0. \tag{6}$$

Equation (4) leads to the conjugated ideal equations

$$\begin{cases}(\chi)=\mathfrak{b}\cdot\prod_{i=1}^{s}\mathfrak{p}_i^{a_i}\cdot\mathfrak{p}_i'^{b_i}\\ (\chi')=\mathfrak{b}'\cdot\prod_{i=1}^{s}\mathfrak{p}_i'^{a_i}\cdot\mathfrak{p}_i^{b_i}\end{cases} \tag{7}$$

where $a_i,b_i\geq 0$, and $b_i=0$ if $\mathfrak{p}_i=\mathfrak{p}_i'$, and $(b)=\mathfrak{b}\cdot\mathfrak{b}'$. We need the following auxiliary lemma. Note that $\mathfrak{p}_i\nmid\mathfrak{b},\mathfrak{p}_i'\nmid\mathfrak{b}$.

LEMMA 4. *If $\xi\in K$ and $\mathrm{ord}_p(\xi)=\mathrm{ord}_p(\xi')$ for a prime p, then*

$$\mathrm{ord}_p(\xi)\leq\mathrm{ord}_p(\xi-\xi').$$

Moreover, if $p=2$ *and* $\Delta\equiv 1 \pmod 8$, *then*

$$\operatorname{ord}_2(\xi)\le \operatorname{ord}_2((\xi-\xi')/2),$$

and, if $p=2$ *and* $\Delta\equiv 2,3 \pmod 4$, *then*

$$\operatorname{ord}_2(\xi)\le \operatorname{ord}_2((\xi-\xi')/2\sqrt{\Delta})+\tfrac{1}{2}.$$

PROOF. This is an easy exercise, which we leave to the reader. □

We distinguish, as usual, three cases for the factorization of the prime p_i in $\mathcal{O}_K$: it may split, ramify or remain prime.

$\to p_i$ remains prime in K. Then $p_i \nmid \Delta$, and if $p_i=2$ then $\Delta\equiv 5 \pmod 8$. We have $(p_i)=\mathfrak{p}_i=\mathfrak{p}_i'$, and from $\operatorname{ord}_{p_i}(\chi)=\operatorname{ord}_{p_i}(\chi')$ and Lemma 4 we obtain

$$\operatorname{ord}_{p_i}(y)=2\cdot\operatorname{ord}_{p_i}(\chi)\le 2\cdot\operatorname{ord}_{p_i}(\chi-\chi')=2\cdot\operatorname{ord}_{p_i}(2\cdot u\cdot\sqrt{\Delta}).$$

It follows, using (6), that

$$\text{if } p_i\ne 2 \text{ then } \operatorname{ord}_{p_i}(y)=2\cdot a_i=0,$$

$$\text{if } p_i=2 \text{ then } \operatorname{ord}_2(y)=2\cdot a_i=0,2, \text{ and if } a_i=1 \text{ then } \operatorname{ord}_2(u)=0.$$

$\to p_i$ ramifies in K. Then $p_i \mid \Delta$ if $p_i\ne 2$, and $\Delta\equiv 2,3 \pmod 4$ if $p_i=2$. We have $(p_i)=\mathfrak{p}_i^2$, $\mathfrak{p}_i=\mathfrak{p}_i'$, and $\operatorname{ord}_{p_i}(\chi)=\operatorname{ord}_{p_i}(\chi')=\frac{1}{2}\cdot a_i$. From Lemma 4 we find

$$\operatorname{ord}_{p_i}(y)=2\cdot\operatorname{ord}_{p_i}(\chi)\le 1+2\cdot\operatorname{ord}_{p_i}((\chi-\chi')/2\cdot\sqrt{\Delta})=1+2\cdot\operatorname{ord}_{p_i}(u).$$

By (6) we obtain

$$\operatorname{ord}_{p_i}(y)=a_i=0,1, \text{ and if } a_i=1 \text{ then } \operatorname{ord}_{p_i}(u)=0.$$

$\to p_i$ splits in K. Then $p_i \nmid \Delta$, and if $p_i=2$ then $\Delta\equiv 1 \pmod 8$. We have $(p_i)=\mathfrak{p}_i\cdot\mathfrak{p}_i'$, $\mathfrak{p}_i\ne\mathfrak{p}_i'$. Further, $\operatorname{ord}_{p_i}(\mathfrak{p}_i)=1$, $\operatorname{ord}_{p_i}(\mathfrak{p}_i')=0$. Hence $\operatorname{ord}_{p_i}(\chi)=a_i$, $\operatorname{ord}_{p_i}(\chi')=b_i$. If $a_i=b_i$ then from

$$\operatorname{ord}_{p_i}(y)=2\cdot\operatorname{ord}_{p_i}(\chi)\le 2\cdot\operatorname{ord}_{p_i}(\chi-\chi')/2)=2\cdot\operatorname{ord}_{p_i}(u)$$

we obtain by (6) that

$$\operatorname{ord}_{p_i}(y)=a_i=b_i=0.$$

If $a_i\ne b_i$ then $\operatorname{ord}_{p_i}(y)=a_i+b_i>0$, hence $\operatorname{ord}_{p_i}(u)=0$, by (6). We infer in this case

$$\begin{aligned}\operatorname{ord}_{p_i}(y)=a_i+b_i&\ge 1+2\cdot\min(a_i,b_i)=1+2\cdot\operatorname{ord}_{p_i}(\chi-\chi')\\&=1+2\cdot\operatorname{ord}_{p_i}(2).\end{aligned}$$

It follows that

$$\operatorname{ord}_{p_i}(y)=\max(a_i,b_i),\ \min(a_i,b_i)=0 \text{ if } p_i\ne 2,$$

$$\operatorname{ord}_{p_i}(y)=\max(a_i,b_i)+1,\ \min(a_i,b_i)=1 \text{ if } p_i=2.$$

Put $b_0=\min(a_i,b_i)$ if $p_i=2$ occurs, and $b_0=0$ otherwise. (Note that $\min(a_i,b_i)=1$ may occur only if $\mathfrak{p}_i\neq\mathfrak{p}_i'$, hence only if $p_i=2$ splits).

Let us assume that the splitting primes of $p_1,\dots,p_s$ are $p_1,\dots,p_t$ for some $0\leq t\leq s$. Put

$$I=\{i\mid 1\leq i\leq t, a_i>b_i\},$$

$$I'=\{i\mid 1\leq i\leq t, a_i<b_i\}.$$

For $i=1,\dots,t$, let h_i be the smallest positive integer such that $\mathfrak{p}_i^{h_i}$ is a principal ideal, say

$$\mathfrak{p}_i^{h_i}=(\pi_i).$$

If h denotes the class number of K, then $h_i\mid h$. Now, $\pi_i\in K$ is determined up to multiplication by a unit. Thus we may choose π_i such that

$$|\pi_i|>|\pi_i'| \text{ if } i\in I,\ |\pi_i|<|\pi_i'| \text{ if } i\in I'.$$

For $i=1,\dots,t$, put

$$|a_i-b_i|=c_i\cdot h_i+d_i,$$

with $c_i,d_i\in\mathbb{Z}$, and $0\leq d_i\leq h_i-1$. Consider the ideal

$$\mathfrak{a}=\mathfrak{b}\cdot(2)^{b_0}\cdot\prod_{i\in I}\mathfrak{p}_i^{d_i}\cdot\prod_{i\in I'}\mathfrak{p}_i'^{d_i}\cdot\prod_{i=t+1}^{s}\mathfrak{p}_i^{a_i}.$$

From the above considerations it follows that for given b, K and $p_1,\dots,p_s$ there are only finitely many possibilities for $\mathfrak{a}$. By (7) it follows that

$$(\chi)=\mathfrak{a}\cdot\prod_{i\in I}(\pi_i)^{c_i}\cdot\prod_{i\in I'}(\pi_i')^{c_i} \tag{8}$$

(namely, $|a_i-b_i|=\max(a_i,b_i)$ if $p_i\neq 2$, since then $\min(a_i,b_i)=0$; and $|a_i-b_i|=\max(a_i,b_i)-1$ if $p_i=2$ and $b_0=1$). Hence $\mathfrak{a}$ is a principal ideal, say

$$\mathfrak{a}=(\alpha)$$

for an $\alpha\in\mathcal{O}_K$. Up to multiplication by a unit, there are only finitely many possibilities for α. Let ε be the fundamental unit of K with $\varepsilon>1$.

Now, (8) leads to the system of equations

$$\begin{cases}\chi=z+u\sqrt{\Delta}=\pm\alpha\cdot\varepsilon^n\cdot\prod_{i\in I}\pi_i^{c_i}\cdot\prod_{i\in I'}\pi_i'^{c_i}\\ \chi'=z-u\sqrt{\Delta}=\pm\alpha'\cdot\varepsilon'^n\cdot\prod_{i\in I}\pi_i'^{c_i}\cdot\prod_{i\in I'}\pi_i^{c_i}\end{cases}, \tag{9}$$

where $n\in\mathbb{Z}$. Put for $n\in\mathbb{Z}$, $m_1,\dots,m_t\in\mathbb{N}\cup\{0\}$, and for each possible α

$$G_\alpha(n,m_1,\dots,m_t)=\frac{\alpha}{2\sqrt{\Delta}}\cdot\varepsilon^n\cdot\prod_{i\in I}\pi_i^{m_i}\cdot\prod_{i\in I'}\pi_i'^{m_i}-\frac{\alpha'}{2\sqrt{\Delta}}\cdot\varepsilon'^n\cdot\prod_{i\in I}\pi_i'^{m_i}\cdot\prod_{i\in I'}\pi_i^{m_i},$$

$$H_\alpha(n,m_1,\dots,m_t)=\frac{\alpha}{2}\cdot\varepsilon^n\cdot\prod_{i\in I}\pi_i^{m_i}\cdot\prod_{i\in I'}\pi_i'^{m_i}+\frac{\alpha'}{2}\cdot\varepsilon'^n\cdot\prod_{i\in I}\pi_i'^{m_i}\cdot\prod_{i\in I'}\pi_i^{m_i}.$$

Then (9) is equivalent to

$$(10) \qquad \begin{cases} \pm u = G_\alpha(n, c_1, \ldots, c_t) \\ \pm z = H_\alpha(n, c_1, \ldots, c_t) \end{cases}.$$

The functions G_α and H_α are generalized recurrences in the sense that if all variables but one are fixed, then they yield integral binary recurrence sequences when the one not-fixed variable runs from 0 to ∞.

6. TOWARDS LINEAR FORMS IN LOGARITHMS

Let us write $u_i = \mathrm{ord}_{p_i}(u)$ for $i = 1, \ldots, s$. Put for each α

$$I'' = \{i \mid 1 \le i \le s,\ \mathrm{ord}_{p_i}(G_\alpha(n, m_1, \ldots, m_t)) > 0 \text{ occurs for at least one } (n, m_1, \ldots, m_t)\}.$$

Note that since $(u, y) = 1$ the sets I, I', I'' are disjunct. We proceed with the first equation of system (10). Written out in full detail it reads

$$(11) \qquad \frac{\alpha}{2\sqrt{\Delta}} \cdot \varepsilon^n \cdot \prod_{i \in I} \pi_i^{c_i} \cdot \prod_{i \in I'} \pi_i'^{c_i} - \frac{\alpha'}{2\sqrt{\Delta}} \cdot \varepsilon'^n \cdot \prod_{i \in I} \pi_i'^{c_i} \cdot \prod_{i \in I'} \pi_i^{c_i} = \pm \prod_{i \in I''} p_i^{u_i}.$$

This equation (11) bears some resemblance to equation (5), that we were led to in the case of Δ being a square. Both (5) and (11) are derived by factorizing equation (4) in $\mathbb{Q}(\sqrt{\Delta})$, and both are purely exponential equations, with the variables in the exponents only. A minor difference is that the parameters of (11) are quadratic numbers, whereas the parameters of (5) are rational integers. The essential difference however is that in (11) there occur the units ε^n and ε'^n, that may be a priori arbitrarily large or small. Therefore (11) is essentially more difficult to treat than (5) was.

Now, I, I', I'' depend on α, which depends on the particular solution of equation (4) that we presupposed. However, we know that α belongs to a finite set, which can be computed explicitly. So if we can solve (11) completely for each α of this set, then we can find all the solutions of (10), hence of (1).

The set of the α's may be reduced, without loss of generality, as follows. If $\Delta \equiv 1 \pmod 8$ then $b_0 = 0, 1$ may both occur, with $\alpha = \alpha_0$, $2 \cdot \alpha_0$ respectively. We only have to consider $2 \cdot \alpha_0$, because if $u = u_0$, $z = z_0$ is a solution of (10) for $\alpha = \alpha_0$, then $u = 2 \cdot u_0$, $z = 2 \cdot z_0$ is a solution of (10) for $\alpha = 2 \cdot \alpha_0$. Hence it is not necessary to consider $\alpha = \alpha_0$ if also $\alpha = 2 \cdot \alpha_0$ is already being considered. By the same argument, if $\Delta \equiv 5 \pmod 8$ then with $\alpha = \alpha_0$ such that $\mathrm{ord}_2(\alpha_0) = 0$ also $\alpha = 2 \cdot \alpha_0$ may occur, so that we only have to consider the latter. Note that it may now occur that $(u, y) = 2$. The condition $(u, y) = 1$ is used only to ensure that I'' and $I \cup I'$ are disjunct. This remains true in the above cases with $(u, y) = 2$. Further, if $(\alpha_0) \neq (\alpha_0')$ for some α_0, then we only have to consider one α of the pair α_0, α_0'. Namely, if the I, I' belonging to α_0 are I_0, I_0', then the I, I' belonging to α_0' are I_0', I_0, and then

$$G_{\alpha_0'}(n, m_1, \ldots, m_t) = \frac{\alpha_0'}{2\sqrt{\Delta}} \cdot \varepsilon^n \cdot \prod_{I_0'} \pi_i^{c_i} \cdot \prod_{I_0} \pi_i'^{c_i} - \frac{\alpha_0}{2\sqrt{\Delta}} \cdot \varepsilon'^n \cdot \prod_{I_0'} \pi_i'^{c_i} \cdot \prod_{I_0} \pi_i^{c_i}$$

$$= \pm\left(\frac{\alpha_0'}{2\sqrt{\Delta}} \cdot \varepsilon'^{-n} \cdot \prod_{I_0} \pi_i'^{c_i} \cdot \prod_{I_0'} \pi_i^{c_i} - \frac{\alpha_0}{2\sqrt{\Delta}} \cdot \varepsilon^{-n} \cdot \prod_{I_0} \pi_i^{c_i} \cdot \prod_{I_0'} \pi_i'^{c_i}\right)$$

$$= \mp G_{\alpha_0}(-n, m_1, \ldots, m_t),$$

(by using $\varepsilon \cdot \varepsilon' = \pm 1$), and analogously

$$H_{\alpha_0'}(n, m_1, \ldots, m_t) = \pm H_{\alpha_0}(-n, m_1, \ldots, m_t).$$

From equation (11) we now derive p_i-adic linear forms in logarithms, in three different ways, according to $i \in I$, I' or I''. Put

$$\gamma_i = \tfrac{3}{2} \text{ if } p_i = 2,\ \gamma_i = 1 \text{ if } p_i = 3,\ \gamma_i = \tfrac{1}{2} \text{ if } p_i \geq 5.$$

Then $\gamma_i > 1/(p_i - 1)$, hence if $\operatorname{ord}_{p_i}(\xi) \geq \gamma_i$ for a $\xi \in K$ then

(12) $$\operatorname{ord}_{p_i}(\log_{p_i}(1 \pm \xi)) = \operatorname{ord}_{p_i}(\xi).$$

We now have the following result.

LEMMA 5. *Let* n, $c_i (i \in I \cup I')$, $u_i (i \in I'')$ *satisfy* (11).

(i). *For* $i \in I''$ *put*

$$\lambda_i = \operatorname{ord}_{p_i}(2\sqrt{\Delta}/\alpha'),$$

$$\Lambda_i = \log_{p_i}\left(\frac{\alpha}{\alpha'}\right) + n \cdot \log_{p_i}\left(\frac{\varepsilon}{\varepsilon'}\right) + \sum_{j \in I} c_j \cdot \log_{p_i}\left(\frac{\pi_j}{\pi_j'}\right) - \sum_{j \in I'} c_j \cdot \log_{p_i}\left(\frac{\pi_j}{\pi_j'}\right).$$

If $u_i + \lambda_i \geq \gamma_i$ *then*

$$u_i + \lambda_i = \operatorname{ord}_{p_i}(\Lambda_i).$$

(ii). *For* $i \in I$ *put*

$$\kappa_i = \operatorname{ord}_{p_i}\left(\frac{\alpha}{\alpha'}\right),$$

$$K_i = \log_{p_i}\left(\frac{\alpha'}{2\sqrt{\Delta}}\right) + n \cdot \log_{p_i}(\varepsilon') - \sum_{j \in I''} u_j \cdot \log_{p_i}(p_j)$$

$$+ \sum_{j \in I} c_j \cdot \log_{p_i}(\pi_j') + \sum_{j \in I'} c_j \cdot \log_{p_i}(\pi_j).$$

If $h_i \cdot c_i + \kappa_i \geq \gamma_i$ *then*

$$h_i \cdot c_i + \kappa_i = \operatorname{ord}_{p_i}(K_i).$$

(ii'). *For* $i \in I'$ *put*

$$\kappa_i' = \operatorname{ord}_{p_i}\left(\frac{\alpha'}{\alpha}\right),$$

$$K_i' = \log_{p_i}\left(\frac{\alpha}{2\sqrt{\Delta}}\right) + n \cdot \log_{p_i}(\varepsilon) - \sum_{j \in I''} u_j \cdot \log_{p_i}(p_j)$$
$$+ \sum_{j \in I} c_j \cdot \log_{p_i}(\pi_j) + \sum_{j \in I'} c_j \cdot \log_{p_i}(\pi_j').$$

If $h_i \cdot c_i + \kappa_i' \geq \gamma_i$ *then*

$$h_i \cdot c_i + \kappa_i' = \mathrm{ord}_{p_i}(K_i').$$

REMARK. Note that all the above p_i-adic logarithms are well-defined, since their arguments have p_i-adic order zero. This follows from the fact that I, I' and I'' are disjunct, and if $\Delta \equiv 1 \pmod 8$ from the choice $\alpha = 2 \cdot \alpha_0$.

PROOF. For (i), divide (11) by its second term. For (ii), divide (11) by its second term, and add 1. For (ii'), divide (11) by its first term, and add -1. Then in all three cases take the p_i-adic order, and apply (12). □

The linear forms in logarithms Λ_i, K_i, K_i', as they appear in Lemma 5, can be simplified a bit, by incorporating parts of the first terms into the other ones, as follows. First we treat Λ_i. Put

$$h^* = lcm(2, h_1, \ldots, h_s).$$

Note that, by the definitions of α and $\mathfrak{a}$,

$$\mathfrak{a}^{h^*} = \mathfrak{b}^{h^*} \cdot \prod_{i \in I} (\pi_i)^{n_i} \cdot \prod_{i \in I'} (\pi_i')^{n_i} \cdot \prod_{i=t+1}^{s} (p_i)^{n_i} \cdot (2)^{h^* \cdot b_0},$$

where the exponents n_i for $1 \leq i \leq s$ are fixed integers. It follows that $\mathfrak{b}^{h^*}$ is principal, say

$$\mathfrak{b}^{h^*} = (\beta)$$

for an integral $\beta \in K$. Now we obtain

$$\alpha^{h^*} = \pm \beta \cdot \varepsilon^{n_0} \cdot \prod_{i \in I} \pi_i^{n_i} \cdot \prod_{i \in I'} \pi_i'^{n_i} \cdot \prod_{i=t+1}^{s} p_i^{n_i} \cdot 2^{h^* \cdot b_0}, \tag{13}$$

where $n_0 \in \mathbb{Z}$ is fixed. Thus

$$\left(\frac{\alpha}{\alpha'}\right)^{h^*} = \pm \left(\frac{\beta}{\beta'}\right) \cdot \left(\frac{\varepsilon}{\varepsilon'}\right)^{n_0} \cdot \prod_{i \in I} \left(\frac{\pi}{\pi'}\right)^{n_i} \cdot \prod_{i \in I'} \left(\frac{\pi'}{\pi}\right)^{n_i}.$$

Put

$$\Lambda_i^* = h^* \cdot \Lambda_i, \; n^* = h^* \cdot n + n_0, \; c_j^* = h^* \cdot c_j + n_j.$$

Then it follows that

$$\Lambda_i^* = \log_{p_i}\left(\frac{\beta}{\beta'}\right) + n^* \cdot \log_{p_i}\left(\frac{\varepsilon}{\varepsilon'}\right) + \sum_{j \in I} c_j^* \cdot \log_{p_i}\left(\frac{\pi_j}{\pi_j'}\right) - \sum_{j \in I'} c_j^* \cdot \log_{p_i}\left(\frac{\pi_j}{\pi_j'}\right).$$

Note that if $b = 1$ then $\beta = \beta' = 1$, and thus Λ_i^* is a homogeneous linear form.

Next we treat K_i and K_i'. Note that the prime odd divisors of Δ are just the ramifying odd primes. By (13),

$$\left(\frac{\alpha}{2\sqrt{\Delta}}\right)^{h^*} = \pm\beta \cdot \varepsilon^{n_0} \cdot \prod_{i\in I} \pi_i^{n_i} \cdot \prod_{i\in I'} \pi_i'^{n_i} \cdot \prod_{i=t+1}^{s} p_i^{n_i - v_i} \cdot 2^{h^*\cdot(b_0 - v_0)},$$

where $v_i = \frac{1}{2}\cdot h^* \cdot \mathrm{ord}_{p_i}(4\Delta) \in \mathbb{Z}$ for $i = t+1, \ldots, s$, and $v_0 = 1$ if 2 splits, $v_0 = 0$ otherwise. If $p_i = 2$ splits we have assumed that $b_0 = 1$. Hence the last factor vanishes. So put

$$K_i^* = h^* \cdot K_i,\ K_i'^* = h^* \cdot K_i',\ u_j^* = h^* \cdot u_j - (n_j - v_j),$$

$$I''^* = I'' \cup \{i \mid t+1 \le i \le s, v_i \neq 0\}.$$

Then it follows that

$$K_i^* = \log_{p_i}(\beta') + n^* \cdot \log_{p_i}(\varepsilon') - \sum_{j\in I''^*} u_j^* \cdot \log_{p_i}(p_j)$$
$$+ \sum_{j\in I} c_j^* \cdot \log_{p_i}(\pi_j') + \sum_{j\in I'} c_j^* \cdot \log_{p_i}(\pi_j),$$

$$K_i'^* = \log_{p_i}(\beta) + n^* \cdot \log_{p_i}(\varepsilon) - \sum_{j\in I''^*} u_j^* \cdot \log_{p_i}(p_j)$$
$$+ \sum_{j\in I} c_j^* \cdot \log_{p_i}(\pi_j) + \sum_{j\in I'} c_j^* \cdot \log_{p_i}(\pi_j').$$

Again the linear forms K_i^* and $K_i'^*$ are homogeneous if $b = 1$. Now all this leads to the following reformulation of Lemma 5.

LEMMA 6. *Let n, c_i for $i \in I \cup I'$, u_i for $i \in I''$ be a solution of* (11), *let λ_i, κ_i, κ_i' be as in Lemma* 5, *and let h^*, Λ_i^*, K_i^*, $K_i'^*$, n_i^*, c_i^*, u_i^*, I''^* be as above.*

(i). *Let $i \in I''$. If $u_i + \lambda_i \ge \gamma_i$ then*

$$u_i + \lambda_i + \mathrm{ord}_{p_i}(h^*) = \mathrm{ord}_{p_i}(\Lambda_i^*).$$

(ii). *Let $i \in I$. If $h_i \cdot c_i + \kappa_i \ge \gamma_i$ then*

$$h_i \cdot c_i + \kappa_i + \mathrm{ord}_{p_i}(h^*) = \mathrm{ord}_{p_i}(K_i^*).$$

(ii'). *Let $i \in I'$. If $h_i \cdot c_i + \kappa_i' \ge \gamma_i$ then*

$$h_i \cdot c_i + \kappa_i' + \mathrm{ord}_{p_i}(h^*) = \mathrm{ord}_{p_i}(K_i'^*).$$

REMARK. We will study the linear forms in logarithms Λ_i^*, K_i^*, $K_i'^*$ for arbitrary integral values of the variables n^*, c_i^*, u_i^*. Notice that of the parameter α only the factor β survived in these linear forms. This means that we have to consider the linear forms for the different Δ and β only, instead of for each α.

7. UPPER BOUNDS FOR THE SOLUTIONS: OUTLINE

Let us first give a global explanation of our application of the theory of p-adic linear forms in logarithms, that gives explicit upper bounds for the

variables occurring in the linear forms Λ_i^*, K_i^*, $K_i'^*$. Then we give our reasons for our choice of applying the theory this way, and not other possible ways. In the next section we give full details of the derivation of the upper bounds. In the sequel, by the 'constants' $C_1, \ldots, C_{12}$ we mean numbers that depend only on the parameters of (11), not on the unknowns n, c_i, u_i.

Put

$$M = \max_{i \in I \cup I'} (c_i), \quad U = \max_{i \in I''} (u_i), \quad B = \max(M, U, |n|),$$

$$M^* = \max_{i \in I \cup I'} (c_i^*), \quad U^* = \max_{i \in I''} (u_i^*), \quad B^* = \max(M^*, U^*, |n^*|),$$

$$N = \max(|n_0|, \ldots, |n_t|, |n_{t+1} - v_{t+1}|, \ldots, |n_s - v_s|).$$

Then it follows that

$$X^* \leq h^* \cdot X + N, \quad X \leq \frac{X^* + N}{h^*} \tag{14}$$

for $X = M, U, B$. We apply a theorem of Yu (cf. Yu [1987], see also Section 8) to the p-adic linear forms in logarithms. For Λ_i^* we find, in view of Lemma 6(i),

$$U < C_1 + C_2 \cdot \log(B^*), \tag{15}$$

and for K_i^*, $K_i'^*$ we find, in view of Lemma 6(ii), (ii'),

$$M < C_3 + C_4 \cdot \log(B^*). \tag{16}$$

Here, C_1, C_2, C_3, C_4 are constants that can be written down explicitly. In order to find an upper bound for B we try to find C_{10}, C_{11} such that

$$B < C_{10} + C_{11} \cdot \log(B^*). \tag{17}$$

In view of (14) we may insert and delete asterisks any time we like, as long as we don't specify the constants. In order to prove (17) it remains, in view of (15) and (16), to bound $|n|$ by a constant times $\log B$. We will introduce certain constants C_5, C_6, C_7, and distinguish three cases:

$$\begin{cases} \text{(a)} & -(C_6 + C_7 \cdot M) \leq n \leq C_5, \\ \text{(b)} & n > C_5, \\ \text{(c)} & n < -(C_6 + C_7 \cdot M). \end{cases} \tag{18}$$

In case (a) it is, by (16), obvious that (17) holds. In cases (b) and (c) one of the two terms of G_α dominates. We shall show that there exist constants C_8, C_9 such that

$$|n| < C_8 + C_9 \cdot U. \tag{19}$$

Then (17) follows from (15).

From (17) we derive immediately an explicit upper bound C_{12} for B, hence

for all the variables involved. Since the constants $C_1, \ldots, C_4$ will be very large, also C_{12} will be very large. To find all solutions we proceed by reducing this upper bound, by applying the computational p-adic diophantine approximation technique described in de Weger [1989], Section 3.12 (Section 3.11 for homogeneous linear forms), to the p-adic linear forms Λ_i^*, K_i^*, $K_i'^*$. Crucial in that line of argument is that the constants $C_5, \ldots, C_9$ are very small compared to $C_1, \ldots, C_4$. This method leads to reduced bounds for the p-adic orders of the linear forms. Then we can replace (15) and (16) by much sharper inequalities, and repeat the above argument, to find a much sharper inequality for (17). In general we expect that it is in this way possible to reduce in one step the upper bound C_{12} for B to a reduced bound of size $\log C_{12}$.

Before going into detail we explain briefly that it is possible to treat (11) partly by the theory of real (instead of p-adic) linear forms in logarithms, and subsequently by a real computational diophantine approximation technique (cf. de Weger [1989], Section 3.8, or Section 3.7 for homogeneous forms), and why we prefer not to do so.

First, note that K_i and K_i' have generically more terms than Λ_i, and are therefore more complicated to handle. Since K_i, K_i' occur only in case (a), this is the most difficult case. Equation (11) consist of three terms, each of which is purely exponential, i.e. the bases are fixed and the exponents are variable. If one of these three terms is essentially smaller than the other two (more specifically, smaller than the other terms raised to the power δ, for a fixed $\delta \in (0, 1)$), then we can apply the real method. There are two ways of doing this. Write (11) as

$$\chi - \chi' = 2 \cdot u \cdot \sqrt{D}.$$

First, suppose that $|\chi - \chi'| < |\chi'|^{\delta}$. Then $|n|$ cannot be very large, and we are essentially (i.e. apart from a finite domain) in case (a). Unfortunately, the range for $|n|$ that can be covered this way becomes smaller as $M \to \infty$. Second, suppose that $|\chi| > |\chi'|^{1/\delta}$, or $|\chi| < |\chi'|^{\delta}$. Then we are essentially in case (b) or (c). But this area can be dealt with easier p-adically, since here we use the linear forms Λ_i, whereas the real linear forms in logarithms used in this case will generically have more terms. The areas sketched above, in which we can apply the real theory, will not cover the whole domain corresponding to case (a), no matter what choice we make for δ. Hence we cannot avoid working with the p-adic linear forms K_i, K_i'. But then it is more convenient to completely avoid the use of real linear forms.

8. UPPER BOUNDS FOR THE SOLUTIONS: DETAILS

We now proceed with filling in the details of the procedure outlined in the previous section. We start with quoting Yu's bound for p-adic linear forms in logarithms (Yu [1987], Theorem 1).

THEOREM 7 (Yu). *Let $\alpha_1, \ldots, \alpha_n$ $(n \geq 2)$ be nonzero algebraic numbers. Put $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $d = [L : \mathbb{Q}]$. Let $b_1, \ldots, b_n$ be rational integers. Let $\mathfrak{p}$ be a*

prime ideal of L, lying above the rational prime p. Let $e_\mathfrak{p}$ be the ramification index, and $f_\mathfrak{p}$ the residue class degree of $\mathfrak{p}$. Write $L_\mathfrak{p}$ for the completion of L with respect to $\mathrm{ord}_\mathfrak{p}$ *(then for all $\beta \in L_\mathfrak{p}$ we have $\mathrm{ord}_\mathfrak{p}(\beta) = e_\mathfrak{p} \cdot \mathrm{ord}_p(\beta)$). Let q be a rational prime such that*

$$q \nmid p \cdot (p^{f_\mathfrak{p}} - 1).$$

Let $h(\cdot)$ be the logarithmic height function on L, and let

$$V_j \geq \max(h(\alpha_j), f_\mathfrak{p} \cdot (\log p)/d) \text{ for } j = 1, \ldots, n,$$

$$\text{such that } V_1 \leq \cdots \leq V_{n-1},\ V_{n-1}^+ = \max(1, V_{n-1}),$$

$$B_0 \geq \min_{1 \leq j \leq n,\, b_j \neq 0} |b_j|,\ B_n \geq |b_n|,\ B' \geq \max_{1 \leq j \leq n-1} |b_j|,$$

$$B \geq \max(|b_1|, \ldots, |b_n|, 2),$$

$$W \geq \max\left(\log\left(1 + \frac{3}{4 \cdot n} \cdot B\right),\ \log B_0, f_\mathfrak{p} \cdot (\log p)/d\right).$$

Suppose that $\mathrm{ord}_\mathfrak{p}(\alpha_j) = 0$ *for* $j = 1, \ldots, n$, *that*

$$[L(\alpha_1^{1/q}, \ldots, \alpha_n^{1/q}) : L] = q^n,$$

that $\mathrm{ord}_p(b_n) \leq \mathrm{ord}_p(b_j)$ *for* $j = 1, \ldots, n$, *and* $\alpha_1^{b_1} \cdot \cdots \cdot \alpha_n^{b_n} \neq 1$. *Then*

$$\mathrm{ord}_\mathfrak{p}(\alpha_1^{b_1} \cdot \cdots \cdot \alpha_n^{b_n} - 1) < 2780000 \cdot 10.15^n \cdot n^{n+5/2} \cdot q^{2 \cdot n} \cdot (q-1) \cdot \log^2(n \cdot q) \cdot$$

$$(p^{f_\mathfrak{p}} - 1) \cdot \left(2 + \frac{1}{p-1}\right)^n \cdot (f_\mathfrak{p} \cdot (\log p)/d)^{-(n+2)} \cdot V_1 \cdot \cdots \cdot V_n \cdot$$

$$\left(\frac{W}{6 \cdot n} \log(4 \cdot d)\right) \cdot (\log(4 \cdot d \cdot V_{n-1}^+) + f_\mathfrak{p} \cdot (\log p)/8 \cdot n).$$

Yu [1987] gives a somewhat more detailed statement giving a slightly better constant. We apply this theorem as follows. We have $L = K = \mathbb{Q}(\sqrt{D})$, so $d = 2$. For the α_i we have β/β', ε/ε', π_j/π_j', or β, β', ε, ε', p_j, π_j, π_j'. We have to compute the heights of these numbers. We have at once

$$h(p_j) = \log(p_j) \text{ if } p_j \geq 3,\ h(2) = 1,$$

$$h(\varepsilon) = h(\varepsilon') = \tfrac{1}{2} \cdot \log(\varepsilon),$$

$$h(\pi_j) = h(\pi_j') = \tfrac{1}{2} \cdot \log(\max(1, |\pi_j|) \cdot \max(1, |\pi_j'|)),$$

$$h(\beta) = h(\beta') = \tfrac{1}{2} \cdot \log(\max(1, |\beta|) \cdot \max(1, |\beta'|)).$$

Further, let $\gamma = \beta$ or $\gamma = \varepsilon$ or $\gamma = \pi_j$. Then the leading coefficient of γ/γ' is $a_0 = |\gamma \cdot \gamma'|$, and we infer

$$h\left(\frac{\gamma}{\gamma'}\right) = \tfrac{1}{2}\log\left(|\gamma \cdot \gamma'| \cdot \max\left(1, \left|\frac{\gamma}{\gamma'}\right|\right) \cdot \max\left(1, \left|\frac{\gamma'}{\gamma}\right|\right)\right) = \log(\max(|\gamma|, |\gamma'|)).$$

Hence

$$h\left(\frac{\beta}{\beta'}\right)=\log(\max(|\beta|,|\beta'|)),\ h\left(\frac{\varepsilon}{\varepsilon'}\right)=\log(\varepsilon),$$

$$h\left(\frac{\pi_j}{\pi_j'}\right)=\log(\max(|\pi_j|,|\pi_j'|)).$$

The order of the α_i is important in two respects: it is required that the V_i for $i=1,\ldots,n-1$ are in increasing order, and that $\mathrm{ord}_p(b_n)$ is minimal among the $\mathrm{ord}_p(b_i)$. Since the b_i are the unknowns, we should assume that $V_n\le V_1\le\cdots\le V_{n-1}$. In the final bound however, only the product $V_1\cdot\cdots\cdot V_n$ and V^+_{n-1} appear. So the ordering of the V_i only matters for defining V^+_{n-1}. It follows that we can take

$$V_i=\max(h(\alpha_i), f_\mathfrak{p}\cdot(\log p)/d),$$

with the α_i in any order, if we define

$$V^+_{n-1}=\max(1, V_1,\ldots, V_n).$$

Further, we take (on noting that $b_1=1$)

$$B=B_0=B_n=B'=\max(1,|b_2|,\ldots,|b_n|,2,\tfrac{4}{3}\cdot n\cdot(p^{f_\mathfrak{p}/d}-1)).$$

Then $\log(1+3/4n\cdot \mathrm{B})\ge f_\mathfrak{p}\cdot(\log p)/d$. By $B\ge 2$ it follows that $1+3/4\mathrm{n}\cdot\mathrm{B}<B$. Hence we can take

$$W=\log B.$$

There are two more conditions to be checked. The first one is that $\alpha_1^{b_1}\cdot\cdots\cdot\alpha_n^{b_n}\ne 1$. This is immediate, if we assume the obvious condition that not all b_i are zero. The second one is $[K(\alpha_1^{1/q},\ldots,\alpha_n^{1/q}):K]=q^n$, which is less obvious. Application of Yu's newest results avoids such a condition (cf. Yu [1989]). Therefore we do not prove this condition here. For the case $\beta=1$ we proved it in de Weger [1989], Lemma 7.7. This proof can be adapted easily for our general case.

REMARKS

1. If $\mathrm{ord}_p(\alpha_1^{b_1}\cdot\cdots\cdot\alpha_n^{b_n}-1)>1/(p-1)$ then

$$\mathrm{ord}_p(\alpha_1^{b_1}\cdot\cdots\cdot\alpha_n^{b_n}-1)=\mathrm{ord}_p(b_1\cdot\log_p(\alpha_1)+\cdots+b_n\cdot\log_p(\alpha_n)).$$

We prefer to work with the logarithmic version, since that is the one we use in the computational method of reducing the upper bounds.

2. In order to apply Yu's theorem we can take for q the smallest odd prime that does not divide $h\cdot p\cdot(p^{f_\mathfrak{p}}-1)$.

We now proceed to compute the constants C_1 to C_{12}. To find C_1 and C_2 we apply Theorem 7 to Λ_i^*, for all $i\in I''$. Then we find for each such i constants $C_{1,i}$, $C_{2,i}$ such that, under the conditions

$$u_i+\lambda_i\ge\gamma_i,\ B^*\ge\max(2,\tfrac{4}{3}\cdot t_i\cdot(p_i^{f_{\mathfrak{p}_i}/2}-1)),$$

(where t_i denotes the number of terms in Λ_i^*), we obtain

$$\mathrm{ord}_{\mathfrak{p}_i}(\Lambda_i^*) < C_{1,i} + C_{2,i} \cdot \log B^*.$$

By Lemma 6(i) and the relation $\mathrm{ord}_{\mathfrak{p}}(\cdot) = e_{\mathfrak{p}} \cdot \mathrm{ord}_p(\cdot)$, and assuming that

$$(20) \qquad U \geq \max_{i \in I''} (\gamma_i - \lambda_i), \; B^* \geq \max_{i \in I''} (2, \tfrac{4}{3} \cdot t_i \cdot (p_i^{f_{\mathfrak{p}_i}/2} - 1)),$$

we see that it suffices to take

$$C_1 = \max_{i \in I''} (-(\lambda_i + \mathrm{ord}_{p_i}(h^*)) + C_{1,i}/e_{\mathfrak{p}_i}), \; C_2 = \max_{i \in I''} (C_{2,i}/e_{\mathfrak{p}_i}).$$

Then (15) holds.

Next we apply Theorem 7 to K_i^* and $K_i'^*$, for all $i \in I$ and I' respectively, to obtain C_3 and C_4. By $X^{(\prime)}$ we denote X if $i \in I$, and X' if $i \in I'$. There exist by Yu's theorem constants $C_{3,i}$ and $C_{4,i}$ such that under the conditions

$$h_i \cdot c_i + \kappa_i^{(\prime)} \geq \gamma_i, \; B^* \geq \max(2, \tfrac{4}{3} \cdot t_i \cdot (p_i^{f_{\mathfrak{p}_i}/2} - 1))$$

(where again t_i denotes the number of terms of $K_i^{(\prime)*}$), it follows that

$$\mathrm{ord}_{\mathfrak{p}_i}(K_i^{(\prime)*}) < C_{3,i} + C_{4,i} \cdot \log B^*.$$

Again, by Lemma 6(ii), (ii′) it follows that, under the conditions

$$(21) \qquad M \geq \max_{i \in I \cup I'} \left(\frac{\gamma_i - \kappa_i^{(\prime)}}{h_i} \right), \; B^* \geq \max_{i \in I \cup I'} (2, \tfrac{4}{3} \cdot t_i \cdot (p_i^{f_{\mathfrak{p}_i}/2} - 1))$$

it suffices to take

$$C_3 = \max_{i \in I \cup I'} \left(\frac{\kappa_i^{(\prime)} + \mathrm{ord}_{p_i}(h^*)}{h_i} + \frac{C_{3,i}}{h_i \cdot e_{\mathfrak{p}_i}} \right), \; C_4 = \max_{i \in I \cup I'} \left(\frac{C_{4,i}}{h_i \cdot e_{\mathfrak{p}_i}} \right).$$

Then (16) holds.

We take C_5 to C_7 as follows:

$$C_5 = \log\left(2 \cdot \left|\frac{\alpha'}{\alpha}\right|\right) \Big/ 2 \cdot \log \varepsilon, \; C_6 = \log\left(2 \cdot \left|\frac{\alpha}{\alpha'}\right|\right) \Big/ 2 \cdot \log \varepsilon,$$

$$C_7 = \left(\sum_{i \in I} \log \left|\frac{\pi_i}{\pi_i'}\right| + \sum_{i \in I'} \log \left|\frac{\pi_i'}{\pi_i}\right| \right) \Big/ 2 \cdot \log \varepsilon.$$

Note that C_5 or C_6 may be negative, but that always $-C_6 < C_5$. Further, C_7 is always strictly positive, unless $I = I' = \emptyset$. Next we show how to take C_8 and C_9. Suppose first that

$$n > \max(C_5, 0).$$

Then, from $\varepsilon \cdot \varepsilon' = \pm 1$ and the choice of π_i we find by (9) that

$$\left|\frac{\chi}{\chi'}\right| = \left|\frac{\alpha}{\alpha'}\right| \cdot \left|\frac{\varepsilon}{\varepsilon'}\right|^n \cdot \prod_{i \in I} \left|\frac{\pi_i}{\pi_i'}\right|^{c_i} \cdot \prod_{i \in I'} \left|\frac{\pi_i'}{\pi_i}\right|^{c_i} \geq \left|\frac{\alpha}{\alpha'}\right| \cdot \varepsilon^{2 \cdot n} > 2,$$

which expresses that the first term of G_α dominates. Put

$$P = \prod_{i \in I''} p_i .$$

Then we infer

$$P^U \geq \prod_{i \in I''} p_i^{u_i} = |\chi - \chi'|/2 \cdot \sqrt{D} > |\chi|/4 \cdot \sqrt{D}$$

$$= \frac{|\alpha|}{4\sqrt{D}} \cdot \varepsilon^n \cdot \prod_{i \in I} |\pi_i|^{c_i} \cdot \prod_{i \in I'} |\pi_i'|^{c_i} > \frac{|\alpha|}{4\sqrt{D}} \cdot \varepsilon^n ,$$

hence

$$n < \left(\log\left(\frac{4\sqrt{D}}{|\alpha|} \right) + U \cdot \log(P) \right) \Big/ \log \varepsilon .$$

Next suppose that

$$n < \min(-(C_6 + C_7 \cdot M), 0).$$

Then we find that the second term of G_α dominates, namely

$$\left| \frac{\chi'}{\chi} \right| = \left| \frac{\alpha'}{\alpha} \right| \cdot \left| \frac{\varepsilon'}{\varepsilon} \right|^n \cdot \prod_{i \in I} \left| \frac{\pi_i'}{\pi_i} \right|^{c_i} \cdot \prod_{i \in I'} \left| \frac{\pi_i}{\pi_i'} \right|^{c_i}$$

$$\geq \left| \frac{\alpha'}{\alpha} \right| \cdot \varepsilon^{-2 \cdot n} \cdot \left(\prod_{i \in I} \left| \frac{\pi_i'}{\pi_i} \right| \cdot \prod_{i \in I'} \left| \frac{\pi_i}{\pi_i'} \right| \right)^M = \left| \frac{\alpha'}{\alpha} \right| \cdot \varepsilon^{-2 \cdot (n + C_7 \cdot M)}$$

$$> \left| \frac{\alpha'}{\alpha} \right| \cdot \varepsilon^{2 \cdot C_6} = 2.$$

Put

$$\Gamma = \prod_{i \in I} \min(1, |\pi_i'|) \cdot \prod_{i \in I'} \min(1, |\pi_i|).$$

Then we infer

$$P^U \geq |\chi - \chi'|/2 \cdot \sqrt{D} > |\chi'|/4 \cdot \sqrt{D} = \frac{|\alpha'|}{4\sqrt{D}} \cdot \varepsilon^{|n|} \cdot \prod_{i \in I} |\pi_i'|^{c_i} \cdot \prod_{i \in I'} |\pi_i|^{c_i}$$

$$\geq \frac{|\alpha'|}{4\sqrt{D}} \cdot \varepsilon^{|n|} \cdot \prod_{i \in I} \min(1, |\pi_i'|)^{c_i} \cdot \prod_{i \in I'} \min(1, |\pi_i|)^{c_i}$$

$$\geq \frac{|\alpha'|}{4\sqrt{D}} \cdot \varepsilon^{|n|} \cdot \Gamma^M > \frac{|\alpha'|}{4\sqrt{D}} \cdot \varepsilon^{|n|} \cdot \Gamma^{-(|n| - C_6)/C_7}.$$

Hence

$$|n| < \left(\log\left(\frac{4\sqrt{D}}{|\alpha'|} \cdot \Gamma^{-C_6/C_7} \right) + U \cdot \log(P) \right) \Big/ \log(\varepsilon \cdot \Gamma^{1/C_7}).$$

The remaining possibilities in cases (b) and (c) are $C_5 < n \leq 0$ and $0 \leq$

$\leq n < -(C_6 + C_7 \cdot M) < -C_6$. So we may take, noting that $\Gamma \leq 1$,

$$C_8 = \max\left(\log\left(\frac{4\sqrt{D}}{|\alpha|}\right)\Big/\log \varepsilon, \log\left(\frac{4\sqrt{D}}{|\alpha'|}\cdot \Gamma^{-C_6/C_7}\right)\Big/\log(\varepsilon \cdot \Gamma^{1/C_7}), -C_5, -C_6\right),$$

$$C_9 = (\log P)/\log(\varepsilon \cdot \Gamma^{1/C_7}).$$

Then (19) holds in the cases (b) and (c). Now take

$$C_{10} = \max(C_1, C_3, |C_5|, |C_6| + C_3 \cdot C_7, C_8 + C_1 \cdot C_9),$$

$$C_{11} = \max(C_2, C_4, C_4 \cdot C_7, C_2 \cdot C_9).$$

Then it follows that (17) is true, if conditions (20) and (21) hold. Hence, by de Weger [1989], Lemma 2.1, we infer the following result.

LEMMA 8. *In the above notation,*

$$B^* < C_{12}^*, B < C_{12}$$

hold unconditionally, where $C_{12} = (C_{12}^* + N)/h^*$, *and*

$$C_{12}^* = \max\Bigg(2 \cdot (N + h^* \cdot C_{10} + h^* \cdot C_{11} \cdot \log(h^* \cdot C_{11})), \max_{i \in I''}(h^* \cdot (\gamma_i - \lambda_i) + N),$$
$$\max_{i \in I \cup I'}\left(h^* \cdot \frac{\gamma_i - \kappa_i^{(\prime)}}{h_i} + N\right), 2, \max_{i \in I \cup I' \cup I''}(\tfrac{4}{3} \cdot t_i \cdot (p_i^{f_{\mathfrak{p}_i}/2} - 1))\Bigg).$$

PROOF. Clear. □

REMARKS

1. Theorem 1 is an immediate corollary of Theorem 3 and Lemma 8.

2. In practice, almost always the first term in the max-definition of C_{12}^* dominates. Moreover, the term N will in practice disappear in the rounding off. Similarly, in the definitions of C_{10} and C_{11}, the dominating factors are in practice C_1 to C_4.

9. THE REDUCTION TECHNIQUE

We now want to reduce the upper bound C_{12} for B (or C_{12}^* for B^*, which is equivalent), to a much smaller upper bound. That can be done using the p-adic computational diophantine approximation technique described in de Weger [1989], Section 3.12 (or Section 3.11 for homogeneous linear forms).

One has to perform this procedure for $\Lambda = \Lambda_i^*$, K_i^*, $K_i'^*$, for the relevant i. The computational bottlenecks are the computation of the p-adic logarithms to the desired precision, and the application of the L^3-Algorithm. We refer to de Weger [1989], Chapter 3 for further details. Once we have found reduced bounds for $\mathrm{ord}_p(\Lambda)$ for the above mentioned Λ, we combine these bounds with Lemma 6 and with estimates (14), (18) and (19) to find reduced bounds for B and B^*. Generically these bounds are of the size of $\log C_{12}$. We do not work this out any further, but refer instead to Chapter 7 of de Weger [1989], where an example (with $b = 1$) is treated to the bottom.

When reduced upper bounds for B, B^* are found in this way, we may try the above procedure again, with C_{12}, C_{12}^* replaced by their reduced analogons. We may repeat the argument as long as improvement is still being made. But at a certain stage, usually near to the actual largest solution, the procedure will not yield any further improvement. Then we have to find all solutions by some other method. One technique that may be useful is the algorithm of Fincke and Pohst (cf. Fincke and Pohst [1985] or de Weger [1989], Section 3.6). Another way is to search directly for solutions of the original diophantine equation below the reduced bounds. For our equation (1) this may well be done by employing congruence arguments for finding all solutions of the second equation of system (10) below the obtained bounds.

REFERENCES

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

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

Pinch, R.G.E. – Elliptic curves with good reduction away from 2. Math. Proc. Cambridge Phil. Soc. **96**, 25–38 (1984).

Setzer, B. – Elliptic curves of prime conductor. J. London Math. Soc. **10**, 367–378 (1975).

Weger, B.M.M. de – Solving exponential diophantine equations using lattice basis reduction algorithms. J. Number Th. **26**, 325–367 (1987). Erratum: J. Number Th. **31**, 88–89 (1989).

Weger, B.M.M. de – Algorithms for diophantine equations, CWI-Tract No. 65, Centre for Mathematics and Computer Science, Amsterdam (1989).

Yu, K.R. – Linear forms in the p-adic logarithms. Report MPI/87-20, Max Planck Institut für Mathematik, Bonn, to appear in Acta Arith (1987).

Yu, K.R. – Linear forms in logarithms in the p-adic case. New advances in transcendence theory (Proc. Symp. Durham July 1986), A. Baker (ed.), Cambridge University Press, Cambridge, pp. 411–434 (1988).

Yu, K.R. – Linear forms in p-adic logarithms, to appear (1989).