MATHEMATICS OF COMPUTATION
VOLUME 47, NUMBER 176
OCTOBER 1986, PAGES 713-727

Products of Prime Powers in Binary Recurrence Sequences Part I: The Hyperbolic Case, with an Application to the Generalized Ramanujan-Nagell Equation

By A. Pethö and B. M. M. de Weger

Abstract. We show how the Gelfond-Baker theory and diophantine approximation techniques can be applied to solve explicitly the diophantine equation $G_n = wp_1^{m_1} \cdots p_t^{m_t}$ (where $\{G_n\}_{n=0}^{\infty}$ is a binary recurrence sequence with positive discriminant), for arbitrary values of the parameters. We apply this to the equation $x^2 + k = p_1^{z_1} \cdots p_t^{z_t}$, which is a generalization of the Ramanujan-Nagell equation $x^2 + 7 = 2^z$. We present algorithms to reduce upper bounds for the solutions of these equations. The algorithms are easy to translate into computer programs. We present an example which shows that in practice the method works well.

1. Introduction. The Gelfond-Baker method is one of the most useful tools in the theory of diophantine equations. It has been used to prove effectively computable upper bounds for the solutions of many diophantine problems (cf. Baker [1], Shorey and Tijdeman [17]). However, the derived upper bounds are so large that in many cases it is hopeless to compute all solutions, even with the fastest present-day computers. It seems likely that refinements of the Gelfond-Baker method will not be able to change this situation essentially in the near future.

In those cases where this method has been applied successfully to find all solutions of a certain equation, this has been achieved by reducing the upper bounds considerably, using diophantine approximation techniques (cf. Stroeker and Tijdeman [19]), or by making use of special properties of the diophantine problem (cf. Pethö [12], [13]). These reduced bounds are in practice always small enough to admit enumeration of the remaining possibilities.

In this paper we present such a reduction algorithm for the following problem. Let A, B, G_0, G_1 be integers, and let the recurrence sequence $\{G_n\}_{n=0}^{\infty}$ be defined by

$$G_{n+1} = AG_n - BG_{n-1} \qquad (n = 1, 2, \ldots).$$

Put $\Delta = A^2 - 4B$, and assume that $\Delta > 0$, and that the sequence is not degenerate. Let w be a nonzero integer, and let $p_1, \ldots, p_t$ be distinct prime numbers. We study the diophantine equation

$$(1.1) \qquad G_n = wp_1^{m_1} \cdots p_t^{m_t}$$

Received October 25, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11B37, 11D61, 11J87, 11Y50.

in nonnegative integers n, $m_1, \ldots, m_t$. It was shown by Mahler [9] that (1.1) has only finitely many solutions, and Schinzel [16] has given an effectively computable upper bound for the solutions.

Mignotte [11] indicated how (1.1) with $t = 1$ can in some instances be solved by congruence techniques. It is, however, not clear that his method will work for any equation (1.1) with $t = 1$. Moreover, his method seems not to be generalizable for $t > 1$. Pethö [14] has given a reduction algorithm, based on the Gelfond-Baker method, to treat (1.1) in the case $w = t = 1$.

Our reduction algorithm is based on a simple case of p-adic diophantine approximation. We shall give explicit upper bounds for the solutions of (1.1) which are small enough to admit the practical application of the reduction algorithm, if the parameters of the equation are not too large.

Pethö [14] pointed out that essentially better upper bounds hold for all but possibly one solution. The reduction algorithm is of course independent of the theoretical upper bounds: it can be used to reduce any upper bound. It also works well for rather small bounds.

The generalized Ramanujan-Nagell equation

$$(1.2) \qquad x^2 + k = p_1^{z_1} \cdots p_t^{z_t}$$

(k a fixed integer, $p_1, \ldots, p_t$ fixed primes) in nonnegative integers x, $z_1, \ldots, z_t$, can be reduced to a finite number of equations of type (1.1). Equation (1.2) with $t = 1$ has a long history (cf. Hasse [5] and Beukers [2]) and interesting applications in coding theory (cf. Bremner et al. [3], MacWilliams and Sloane [8], Tzanakis and Wolfskill [21], [22]). Examples of Eq. (1.2) have been solved by the Gelfond-Baker method by D. C. Hunt and A. J. van der Poorten in an unpublished paper. They used complex, not p-adic linear forms in logarithms. As far as we know, none of the proposed methods to treat (1.2) gives rise to an algorithm which works for arbitrary values of k and p_i, whereas Tzanakis' elementary method [20] seems to be the only one that can be generalized to $t > 1$. Our method has both properties. Evertse [4] has proved that the number of solutions of (1.2) does not exceed $3 \times 7^{4t+6}$.

In Section 2 we give the necessary background on p-adic numbers and logarithms, and on linear binary recurrence sequences. In Section 3 we apply a theorem of Schinzel to find upper bounds for the solutions of (1.1). This result holds for positive Δ as well as for negative, whereas in the remaining sections we restrict ourselves to positive Δ. Section 4 includes the reduction algorithm and gives a worked-out example. In Section 5 we study (1.2). As an example we determine all integers x such that $x^2 + 7$ has no prime factors larger than 20. Finally, we note that our method can be applied to a somewhat more general type of quadratic/exponential diophantine equation.

In the second part of this paper ([23]), the second-named author intends to study Eq. (1.1) for negative discriminant.

2. Preliminaries.

2A. *p-Adic Numbers and Logarithms.* For the convenience of the reader we quote the facts that we use from the theory of p-adic numbers and functions. An extensive treatment of this theory is given in Koblitz [6].

Let p be a prime number, and Δ a nonsquare integer (positive or negative). We study the extension $\mathbf{Q}_p(\sqrt{\Delta})$ of the field of p-adic numbers $\mathbf{Q}_p$. Either $\sqrt{\Delta} \in \mathbf{Q}_p$, or $\mathbf{Q}_p(\sqrt{\Delta}) = \mathbf{Q}_p + \sqrt{\Delta}\,\mathbf{Q}_p$. In the former case, $\mathbf{Q}_p(\sqrt{\Delta}) = \mathbf{Q}_p$, and the p-adic order $\operatorname{ord}_p(\xi)$ is well defined for any $\xi \in \mathbf{Q}_p(\sqrt{\Delta})$, as usual. In the latter case, it is defined as follows. Let ξ and ξ' be the roots of $x^2 + ax + b$, a, $b \in \mathbf{Q}_p$. Then we define

$$\operatorname{ord}_p(\xi) = \operatorname{ord}_p(\xi') = \tfrac{1}{2}\operatorname{ord}_p(b).$$

Notice that this formula is not necessarily true if $\sqrt{\Delta} \in \mathbf{Q}_p$.

On $\mathbf{Q}_p(\sqrt{\Delta})$ there is a logarithmic function, denoted by $\log_p$. It is defined for all $\chi \in \mathbf{Q}_p(\sqrt{\Delta})$ with $\operatorname{ord}_p(\chi) = 0$, as follows. Let k be the smallest positive integer such that $\xi = \chi^k - 1$ has $\operatorname{ord}_p(\xi) \geqslant \frac{1}{2}$. Then

$$\log_p(\chi) = \frac{1}{k}\log_p(1 + \xi) = \frac{1}{k}(\xi - \xi^2/2 + \xi^3/3 - \xi^4/4 + \cdots).$$

Notice that this series converges, and is useful for computing $\log_p(\xi)$ to any desired degree of accuracy. Note that $\log_p(\chi) \in \mathbf{Q}_p(\sqrt{\Delta})$, $\log_p(\chi_1\chi_2) = \log_p(\chi_1) + \log_p(\chi_2)$, and $\log_p(\chi^k) = k\log_p(\chi)$ hold for all $k \in \mathbf{Z}$, χ, χ_1, $\chi_2 \in \mathbf{Q}_p(\sqrt{\Delta})$. Further, $\log_p(\chi) = 0$ if and only if χ is a root of unity.

Let $\chi = 1 + \xi \in \mathbf{Q}_p(\sqrt{\Delta})$ not be a root of unity, such that

$$\operatorname{ord}_p(\xi) \geqslant \begin{cases} 3/2 & \text{if } p = 2, \\ 1 & \text{if } p = 3, \\ 1/2 & \text{if } p \geqslant 5. \end{cases} \tag{2.1}$$

Then

$$\operatorname{ord}_p\big(\log_p(\chi)\big) = \operatorname{ord}_p(\xi). \tag{2.2}$$

Suppose that $\sqrt{\Delta} \notin \mathbf{Q}_p$. Let $\alpha = a + b\sqrt{\Delta}$, a, $b \in \mathbf{Q}_p$, and let $\beta = a - b\sqrt{\Delta}$ be its conjugate. Then notice that $\log_p(\alpha)$ and $\log_p(\beta)$ are conjugates. Hence,

$$\log_p(\alpha/\beta) \in \sqrt{\Delta}\,\mathbf{Q}_p. \tag{2.3}$$

Let k be the smallest positive integer such that

$$\left(\frac{\alpha}{\beta}\right)^k = \pm\frac{1 + \xi}{1 - \xi}$$

with $\operatorname{ord}_p(\xi) \geqslant \frac{1}{2}$. Then we can compute $\log_p(\alpha/\beta)$ by the series

$$\log_p(\alpha/\beta) = \frac{2}{k}(\xi + \xi^3/3 + \xi^5/5 + \cdots). \tag{2.4}$$

2B. *Binary Recurrences.* Let A, B, G_0, G_1 be given integers. Let the sequence $\{G_n\}_{n=0}^{\infty}$ be defined by

$$G_{n+1} = AG_n - BG_{n-1} \qquad (n = 1,2,\ldots). \tag{2.5}$$

Let α, β be the roots of $x^2 - Ax + B$. We assume that $\Delta = A^2 - 4B$ is not a square, and that α/β is not a root of unity (i.e., the sequence is not degenerate). Put

$$\lambda = \frac{G_1 - G_0\beta}{\alpha - \beta}, \qquad \mu = \frac{G_0\alpha - G_1}{\alpha - \beta}. \tag{2.6}$$

Then λ and μ are conjugates. It is well known that for all $n \geqslant 0$

$$G_n = \lambda\alpha^n + \mu\beta^n. \tag{2.7}$$

Since our aim is to solve Eq. (1.1), we see from (2.5) that we may assume without loss of generality that $(G_0, G_1) = (G_1, B) = (A, B) = 1$.

LEMMA 2.1. *Let $n, m_1, \dots, m_t$ be a solution of* (1.1). *Then, with the above assumptions, we have for $i = 1, \dots, t$: either $m_i = 0$, or $n = 0$, or*

$$(2.8) \quad \operatorname{ord}_{p_i}(\alpha) = \operatorname{ord}_{p_i}(\beta) = 0, \qquad \operatorname{ord}_{p_i}(\lambda) = \operatorname{ord}_{p_i}(\mu) = -\tfrac{1}{2}\operatorname{ord}_{p_i}(\Delta) \leqslant 0.$$

Proof. Suppose $p_i \mid B$. Then $p_i \nmid A$, hence, from (2.5) and $(B, G_1) = 1$, $p_i \nmid G_n$ for all $n > 0$. Thus, $m_i = 0$ or $n = 0$. Next suppose $p_i \nmid B$. Then, by $\alpha\beta = B$,

$$\operatorname{ord}_{p_i}(\alpha) + \operatorname{ord}_{p_i}(\beta) = \operatorname{ord}_{p_i}(B) = 0.$$

Now, α and β are algebraic integers, so $\operatorname{ord}_{p_i}(\alpha)$ and $\operatorname{ord}_{p_i}(\beta)$ are nonnegative. It follows that they are zero.

Put $E = -\lambda\mu\Delta$. Note that $E \in \mathbb{Z}$, and for all $n \geqslant 0$

$$G_{n+1}^2 - AG_nG_{n+1} + BG_n^2 = EB^n.$$

Suppose that $p_i \mid E$; then we infer that $p_i \nmid G_n$ for all n, since $(G_0, G_1) = 1$. Hence $m_i = 0$. Next, suppose $p_i \nmid E$; then

$$\operatorname{ord}_{p_i}(\lambda\sqrt{\Delta}) + \operatorname{ord}_{p_i}(\mu\sqrt{\Delta}) = \operatorname{ord}_{p_i}(E) = 0.$$

Since $\lambda\sqrt{\Delta}$ and $\mu\sqrt{\Delta}$ are algebraic integers (cf. (2.6)), the result follows. □

From Lemma 2.1 it follows that we may assume without loss of generality that (2.8) holds for $i = 1, \dots, t$. Of course, we may also assume that $\operatorname{ord}_{p_i}(w) = 0$ for $i = 1, \dots, t$. The special case $t = 0$ in Eq. (1.1) is trivial if $\Delta > 0$, and demands special treatment if $\Delta < 0$.

Finally, we prove a simple auxiliary lemma.

LEMMA 2.2. *Let $a \geqslant 0$, $h \geqslant 1$, $b > (e^2/h)^h$, and let $x \in \mathbb{R}$ be the largest solution of $x = a + b(\log x)^h$. Then,*

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

Proof. By $(z_1 + z_2)^{1/h} \leqslant z_1^{1/h} + z_2^{1/h}$ we infer

$$x^{1/h} \leqslant a^{1/h} + c\log(x^{1/h}),$$

where $c = hb^{1/h} > e^2$. Put $x^{1/h} = (1 + y)c\log c$; then $y > 0$. Now,

$$\begin{aligned}(1 + y)c\log c = x^{1/h} &\leqslant a^{1/h} + c\log(1 + y) + c\log c + c\log\log c\\ &< a^{1/h} + cy + c\log c + c\log\log c,\end{aligned}$$

hence,

$$yc(\log c - 1) < a^{1/h} + c\log\log c.$$

It follows, by $c > e^2$, that

$$\begin{aligned}x^{1/h} = c\log c + yc\log c &< c\log c + \frac{\log c}{\log c - 1}\left(a^{1/h} + c\log\log c\right)\\ &< 2\left(a^{1/h} + c\log c\right). \quad \square\end{aligned}$$

3. Application of Schinzel's Theorem. In this section, Δ may be positive or negative. We quote a result of Schinzel [16] and apply it to (1.1).

Let p be prime. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$, ξ and χ nonzero elements of $\mathbb{Q}(\sqrt{\Delta})$. Put $\xi = \xi''/\xi'$, $\chi = \chi''/\chi'$, where ξ', ξ'', χ', χ'' are algebraic integers. Put

$$L = \log\max\left\{|eD|^{1/4}, \|\xi'\chi'\|, \|\xi'\chi''\|, \|\xi''\chi'\|, \|\xi''\chi''\|\right\},$$

where $\|\gamma\|$ is the maximal absolute value of the conjugates of γ. Let $\mathfrak{p}$ be a prime ideal of $\mathbf{Q}(\sqrt{\Delta})$ with norm p^ρ. Put

$$\psi = \frac{2}{\rho \log p}, \qquad \phi = \operatorname{ord}_{\mathfrak{p}}(p).$$

THEOREM 3.1 (SCHINZEL). *If ξ or χ is a $\mathfrak{p}$-adic unit and $\xi^n \neq \chi^m$, then*

$$\operatorname{ord}_{\mathfrak{p}}(\xi^n - \chi^m) < 10^6 \psi^7 \phi^{-2} L^4 p^{4\rho+4} \left(\log\max(|m|, |n|) + \phi L p^\rho + 2/L\right)^3.$$

We apply this to Eq. (1.1) as follows. Let $n_0 \geqslant 2$, and put

$$L = \log\max\left\{|eD|^{1/4}, |\alpha\lambda\sqrt{\Delta}|, |\alpha\mu\sqrt{\Delta}|, |\beta\lambda\sqrt{\Delta}|, |\beta\mu\sqrt{\Delta}|\right\}.$$

Let d be the squarefree part of Δ. For $i = 1, \dots, t$, put

$\phi_i = 2$ if $p_i \mid d$, $\phi_i = 1$ otherwise,

$\rho_i = 2$ if $p_i = 2$, $d \equiv 5 \pmod 8$ or if $p_i > 2$, $\left(\dfrac{d}{p_i}\right) = -1$,

$\rho_i = 1$ otherwise,

$$C_{1,i} = 10^6 \left(\frac{2}{\rho_i \log p_i}\right)^7 \phi_i^{-3} L^4 p_i^{4\rho_i+4} \left(1 + \frac{\phi_i L p_i^{\rho_i} + 2/L}{\log n_0}\right)^3. \tag{3.1}$$

LEMMA 3.2. *The solutions of* (1.1) *with $n \geqslant n_0$ satisfy*

$$m_i < C_{1,i} (\log n)^3 \qquad (i = 1, \dots, t).$$

Proof. Rewrite (1.1), using (2.7), as

$$\left(\frac{\alpha}{\beta}\right)^n - \left(\frac{-\mu}{\lambda}\right) = \frac{w}{\lambda} \beta^{-n} p_1^{m_1} \cdots p_t^{m_t}. \tag{3.2}$$

Then, by (2.8),

$$m_i \leqslant m_i - \operatorname{ord}_{p_i}(\lambda) = \operatorname{ord}_{p_i}\left(\frac{w}{\lambda}\beta^{-n} p_1^{m_1} \cdots p_t^{m_t}\right) = \operatorname{ord}_{p_i}\left(\left(\frac{\alpha}{\beta}\right)^n - \left(\frac{-\mu}{\lambda}\right)\right).$$

Put $\xi'' = \alpha$, $\xi' = \beta$, $\chi'' = \mu\sqrt{\Delta}$, $\chi' = -\lambda\sqrt{\Delta}$. Then, from Theorem 3.1 we find, using $\operatorname{ord}_{\mathfrak{p}_i}(x) = \phi_i \operatorname{ord}_{p_i}(x)$,

$$m_i < 10^6 \left(\frac{2}{\rho_i \log p_i}\right)^7 \phi_i^{-3} L^4 p_i^{4\rho_i+4} \left(\log n + \phi_i L p_i^{\rho_i} + 2/L\right)^3,$$

from which the result follows, since $n \geqslant n_0$. □

Remark. Instead of Schinzel's result, we could have used Theorem 1 of van der Poorten [15]. Then we would have found $m_i < C'_{1,i} \log n$. This is better in $\log n$, and $C'_{1,i}$ has better asymptotic dependence on p_i than $C_{1,i}$. But for p_i up to, say, 10^4, Schinzel's result is sharper.

4. How to Solve (1.1).

4A. *Bounds for the Solutions.* In this subsection, let $\Delta > 0$. Note that $|\alpha| \neq |\beta|$, since $\{G_n\}_{n=0}^\infty$ is not degenerate. So we may assume $|\alpha| > |\beta|$. Let $C_1 = \max(C_{1,1}, \dots, C_{1,t})$, $m = \max(m_1, \dots, m_t)$, and $P = p_1 \cdots p_t$.

The following theorem gives explicit upper bounds for the solutions of (1.1). We do not claim that this result is original or best possible. It just gives correct and rather small upper bounds.

THEOREM 4.1. *Let $\Delta > 0$ and $|\alpha| > |\beta|$, and let the assumptions of Subsection* 2B *hold. Let $n_0 > \max(2, \log|\mu/\lambda|/\log|\alpha/\beta|)$. Put*

$$\gamma = |\lambda/w| - |\mu/w|\,|\alpha/\beta|^{-n_0},$$
$$C_2 = \log P/\left(\log|\alpha| + \frac{1}{n_0}\min(0, \log\gamma)\right),$$
$$C_3 = \max\left\{8C_1(\log 27C_1C_2)^3, 841C_1\right\}.$$

Then all solutions $n, m_1, \dots, m_t$ of (1.1) *with $n \geqslant n_0$ satisfy*

$$n < \sum_{i=1}^{t} m_i \frac{\log p_i}{\log|\alpha|} - \frac{\log\gamma}{\log|\alpha|}. \tag{4.1}$$

Moreover, $n < C_2C_3$ and $m < C_3$.

Proof. Rewrite (1.1), using (2.7), as

$$\frac{\lambda}{w} + \frac{\mu}{w}\left(\frac{\alpha}{\beta}\right)^{-n} = p_1^{m_1} \cdots p_t^{m_t}\alpha^{-n}.$$

Note that $\gamma > 0$, by the choice of n_0. It follows that

$$p_1^{m_1} \cdots p_t^{m_t}|\alpha|^{-n} \geqslant \gamma,$$

and we infer (4.1) immediately. From (4.1) we obtain $n < C_2m$. By Lemma 3.2 we now have

$$m < C_1(\log n)^3 < C_1(\log C_2m)^3.$$

If $C_1C_2 > (e^2/3)^3$, we apply Lemma 2.2 with $a = 0$, $b = C_1C_2$, $h = 3$; then we find $m < 8C_1(\log 27C_1C_2)^3$. If $C_1C_2 \leqslant (e^2/3)^3$, then

$$n < C_2m < C_1C_2(\log n)^3 \leqslant (e^2/3)^3(\log n)^3,$$

from which we deduce $n < 12564$. Now, $m < C_1(\log n)^3 < 841C_1$. □

4B. *Notations and Preliminary Lemmas.* We introduce some notations. Until further notice, Δ may be positive or negative. Let for $i = 1, \dots, t$,

$$e_i = -\operatorname{ord}_{p_i}(\lambda), \qquad f_i = \operatorname{ord}_{p_i}\big(\log_{p_i}(\alpha/\beta)\big), \quad g_i = f_i - e_i,$$
$$\theta_i = -\log_{p_i}(-\lambda/\mu)/\log_{p_i}(\alpha/\beta).$$

By (2.8), the p_i-adic logarithms of α/β and λ/μ exist. Notice that $\log_{p_i}(\alpha/\beta) \neq 0$, since the sequence $\{G_n\}$ is not degenerate. By (2.3), numerator and denominator of θ_i are both in $\sqrt{\Delta}\,\mathbb{Q}_{p_i}$, so $\theta_i \in \mathbb{Q}_{p_i}$. Hence, if $\theta_i \neq 0$, we can write

$$\theta_i = \sum_{l=k_i}^{\infty} u_{i,l}p_i^l,$$

where $k_i = \operatorname{ord}_{p_i}(\theta_i)$, and $u_{i,l} \in \{0, 1, \dots, p_i - 1\}$.

The following, almost trivial lemma is at the heart of our reduction algorithm. It localizes the elements of $\{G_n\}$ with many factors p_i in terms of the p_i-adic expansion of θ_i.

LEMMA 4.2. *Let* $n \in \mathbb{Z}$, $n \geqslant 0$. *If*

$$\operatorname{ord}_{p_i}(G_n) + e_i \geqslant \begin{cases} 3/2 & \text{if } p_i = 2, \\ 1 & \text{if } p_i = 3, \\ 1/2 & \text{if } p_i \geqslant 5, \end{cases}$$

then $\operatorname{ord}_{p_i}(G_n) = g_i + \operatorname{ord}_{p_i}(n - \theta_i)$.

Proof. By (2.8) we have

$$\operatorname{ord}_{p_i}(G_n) + e_i = \operatorname{ord}_{p_i}\left(\left(\frac{\alpha}{\beta}\right)^n - \left(\frac{-\mu}{\lambda}\right)\right) = \operatorname{ord}_{p_i}\left(\left(\frac{-\lambda}{\mu}\right)\left(\frac{\alpha}{\beta}\right)^n - 1\right).$$

With $\xi = (-\lambda/\mu)(\alpha/\beta)^n - 1$, condition (2.1) holds. Hence, from (2.2),

$$\begin{aligned} \operatorname{ord}_{p_i}(G_n) + e_i &= \operatorname{ord}_{p_i}\left(n \log_{p_i}\left(\frac{\alpha}{\beta}\right) + \log_{p_i}\left(\frac{-\lambda}{\mu}\right)\right) \\ &= \operatorname{ord}_{p_i}(n - \theta_i) + f_i. \quad \square \end{aligned}$$

Before we give the algorithm, we have to exclude some trivial cases.

LEMMA 4.3. *If* $\operatorname{ord}_{p_i}(\theta_i) < 0$, *then for the solutions of* (1.1),

$$m_i \leqslant \max\left(1, \operatorname{ord}_{p_i}\left(\log_{p_i}(-\lambda/\mu)\right)\right) - e_i.$$

Proof. If $m_i \geqslant 3/2 - e_i$, we apply Lemma 4.2, and obtain

$$m_i = f_i - e_i + \operatorname{ord}_{p_i}(n - \theta_i).$$

Since $n \in \mathbb{Z}$ and $\operatorname{ord}_{p_i}(\theta_i) < 0$, we have $\operatorname{ord}_{p_i}(n - \theta_i) = \operatorname{ord}_{p_i}(\theta_i)$. Hence

$$m_i = f_i + \operatorname{ord}_{p_i}(\theta_i) - e_i = \operatorname{ord}_{p_i}\left(\log_{p_i}(-\lambda/\mu)\right) - e_i. \quad \square$$

Thus we may assume that $\operatorname{ord}_{p_i}(\theta_i) \geqslant 0$ for $i = 1, \ldots, t$. The reduction algorithm is based on the assumption that infinitely many p_i-adic digits $u_{i,l}$ of θ_i are nonzero. We now show that if this is not the case, then Eq. (1.1) can be solved in an elementary way. From now on, $\Delta > 0$.

LEMMA 4.4. *There are only finitely many p_i-adic digits $u_{i,l}$ of θ_i nonzero if and only if there exists a nonnegative integer r such that $G_n = \pm R_{n-r}$ or $G_n = \pm \kappa S_{n-r}$, where $\kappa = 1$ or $\frac{1}{2}$ and*

$$R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad S_n = \alpha^n + \beta^n.$$

Proof. By $\operatorname{ord}_{p_i}(\theta_i) \geqslant 0$ we have $\theta_i = r$ for some rational integer $r \geqslant 0$. From the definition of θ_i,

$$\log_{p_i}\left(\frac{\alpha}{\beta}\right)^r\left(\frac{-\lambda}{\mu}\right) = 0,$$

hence $(\alpha/\beta)^r(-\lambda/\mu)$ is a root of unity. Since $\Delta > 0$, it is ± 1. Hence, $\lambda\alpha^r = \pm\mu\beta^r$, and we infer

$$G_n = \lambda\alpha^r(\alpha^{n-r} \pm \beta^{n-r}). \tag{4.2}$$

Suppose that $\alpha\beta = \pm 1$. Then

$$\begin{aligned} G_0 &= \lambda\alpha^r(\alpha^{-r} \pm \beta^{-r}) = \pm\lambda\alpha^r(\alpha^r \pm \beta^r), \\ G_1 &= \lambda\alpha^r(\alpha^{1-r} \pm \beta^{1-r}) = \pm\lambda\alpha^r(\alpha^{r-1} \pm \beta^{r-1}). \end{aligned}$$

Notice that

$$\left(\alpha^{r-1} + \beta^{r-1}, \alpha^r + \beta^r\right) = (2, \alpha + \beta) = 1 \text{ or } 2,$$

and

$$\left(\alpha^{r-1} - \beta^{r-1}, \alpha^r - \beta^r\right) = \alpha - \beta.$$

By $(G_0, G_1) = 1$ it follows that $\pm\lambda\alpha^r = 1$, $\frac{1}{2}$ or $1/(\alpha - \beta)$, respectively, and the assertion follows.

Suppose next that $|\alpha\beta| > 1$. Notice that

$$G_0 B\left(\alpha^{r-1} \pm \beta^{r-1}\right) = G_1\left(\alpha^r \pm \beta^r\right),$$

where all factors are integers. Since $(B, G_1) = 1$, we have $\alpha\beta \mid \alpha^r \pm \beta^r$. Suppose $r > 0$. Then it follows that $(\alpha, \beta) \neq 1$, which contradicts $(A, B) = 1$. Hence $r = 0$, and the assertion follows from (4.2) and $(G_0, G_1) = 1$. □

Thus, in the situation of Lemma 4.4 we have to solve (1.1) for R_n and S_n. These recurrences enjoy the following divisibility properties,

$$\begin{aligned} &R_n \mid R_m \quad \text{if and only if } n \mid m, \\ &S_n \mid S_{kn} \quad \text{for odd } k, \\ &\operatorname{ord}_2(S_n) \leqslant \operatorname{ord}_2(S_3) \quad \text{for all } n \geqslant 1. \end{aligned}$$

Ideas similar to those of Størmer [18], Mahler [10], and Lehmer [7] can be employed to solve (1.1) using these properties. We do not work this out, but we confine ourselves to an illustrative example at the end of this section. It is also possible to derive elementary upper bounds in this case. Note that $\theta_i = r$ holds for all i with the same r. Thus, by Lemma 4.2,

$$m_i \leqslant \max\left(g_i + \operatorname{ord}_{p_i}(n - r), 1 - e_i\right) \leqslant g_i + 1 + \operatorname{ord}_{p_i}(n - r).$$

Then we have, by (4.1),

$$n \log|\alpha| < \sum_{i=1}^{t} (g_i + 1)\log p_i - \log\gamma + \log|n - r|,$$

from which a good upper bound for n can be derived.

So we assume in the sequel that infinitely many p_i-adic digits of θ_i are nonzero.

4C. *The Reduction Algorithm*. Let all the above assumptions hold. Let N be a positive real number such that we are only interested in the solutions n, $m_1, \dots, m_t$ of (1.1) with $n < N$. For example, take $N = C_2C_3$, as in Theorem 4.1.

```
ALGORITHM A (reduces given upper bounds for the solutions of (1.1)).
  Input: $\alpha$, $\beta$, $\lambda$, $\mu$, $w$, $p_1, \dots, p_t$, $N$
  Output: new, better upper bounds $M_i$ and $N^*$ for $m_i$ $(i = 1, \dots, t)$ and $n$.

(i)   (initialization) Choose an $n_0 \geqslant 0$ such that $n_0 > \log|\mu/\lambda|/\log|\alpha/\beta|$;
      $\gamma := |\lambda/w| - |\mu/w|\,|\alpha/\beta|^{-n_0}$;
      $g_i := \operatorname{ord}_{p_i}(\lambda) + \operatorname{ord}_{p_i}\left(\log_{p_i}(\alpha/\beta)\right)$
      $h_i := \operatorname{ord}_{p_i}(\lambda) + \begin{cases} 3/2 & \text{if } p_i = 2 \\ 1 & \text{if } p_i = 3 \\ 1/2 & \text{if } p_i \geqslant 5 \end{cases}$      $(i = 1, \dots, t)$;
      $g := \gamma/\prod_{i=1}^{t} p_i^{g_i}$; $N_0 := N$;
```

```
(ii)   (computation of the $\theta_i$'s) Compute for $i = 1,\dots,t$, using (2.4), the first $r_i$
       $p_i$-adic digits $u_{i,l}$ of
           $\theta_i = -\log_{p_i}(-\lambda/\mu)/\log_{p_i}(\alpha/\beta) = \sum_{l=0}^{\infty} u_{i,l}p_i^l$,
       where $r_i$ is so large that $p_i^{r_i} \geqslant N_0$ and $u_{i,r_i} \neq 0$;
(iii)  (further initialization, start outer loop) $s_{i,0} := r_i + 1$ $(i = 1,\dots,t)$; $j := 1$;
(iv)   (start inner loop) $i := 1$; $K_j :=$ .false.;
(v)    (computation of the new bounds for $m_i$)
       $s_{i,j} := \min\{s \in \mathbb{Z}\colon s \geqslant 0$ and $p_i^s \geqslant N_{j-1}$ and $u_{i,s} \neq 0\}$;
       if $s_{i,j} < s_{i,j-1}$ then $K_j :=$ .true.;
(vi)   (terminate inner loop) if $i < t$ then $i := i + 1$, goto (v);
(vii)  (computation of the new bound for $n$)
       $N_j := \min\{N_{j-1}, (\sum_{i=1}^{t} s_{i,j}\log p_i - \log g)/\log|\alpha|\}$;
(viii) (terminate outer loop)
       if $N_j \geqslant n_0$ and $K_j$ then $j := j + 1$, goto (iv);
                                else $N^* := \max(N_j, n_0)$;
                                     $M_i := \max(h_i, g_i + s_{i,j})$ $(i = 1,\dots,t)$;
                                     stop.
```

THEOREM 4.5. *With the above assumptions, Algorithm* A *terminates. Equation* (1.1) *has no solutions with $N^* \leqslant n < N$, $m_i > M_i$ $(i = 1,\dots,t)$.*

Proof. Since the p_i-adic expansion of θ_i is assumed to be infinite, there exist r_i with the required properties. It is clear that $s_{i,1} \leqslant r_i < s_{i,0}$, and that $N_j \leqslant N_{j-1}$. So $s_{i,j} \leqslant s_{i,j-1}$ holds for all $j \geqslant 1$. Since $s_{i,j} \geqslant 0$, there is a j such that $N_j \leqslant n_0$ or $s_{i,j} = s_{i,j-1}$ for all $i = 1,\dots,t$. In the latter case, K_j remains .false.; in both cases the algorithm terminates.

We prove by induction on j that $m_i \leqslant g_i + s_{i,j}$ $(i = 1,\dots,t)$ and $n < N_j$ holds for all j. For $j = 0$, it is clear that $n < N_0$. Suppose $n < N_{j-1}$ for some $j \geqslant 1$. Suppose there exists an i such that $m_i > g_i + s_{i,j}$. From Lemma 4.2 we have

$$\operatorname{ord}_{p_i}(n - \theta_i) = m_i - g_i \geqslant s_{i,j} + 1,$$

hence, by $u_{i,s_{i,j}} \neq 0$,

$$n \geqslant u_{i,0} + u_{i,1}p + \cdots + u_{i,s_{i,j}}p^{s_{i,j}} \geqslant p^{s_{i,j}} \geqslant N_{j-1},$$

which contradicts our assumption. Thus, $m_i \leqslant g_i + s_{i,j}$ $(i = 1,\dots,t)$. Then from (4.1), it follows that

$$n < \left(\sum_{i=1}^{t} (g_i + s_{i,j})\log p_i - \log\gamma\right)/\log|\alpha|,$$

hence, $n < N_j$. □

Remark 1. In general, one expects that $p_i^{s_{i,j}}$ will not be much larger than N_j, i.e., not too many consecutive p_i-adic digits of θ_i will be zero. Then N_j is about as large as $\log N_{j-1}$. In practice, the algorithm will often terminate in three or four steps, near to the largest solution. The computation time is polynomial in t, the bottleneck of the algorithm is the computation of the p_i-adic logarithms.

Remark 2. Pethö [14] gives for $t = 1$ a different reduction algorithm. For a prime p_i he computes the function $g(u)$, defined for $u \in \mathbb{N}$ as the smallest index $n \geqslant 0$ such that $G_n \neq 0$ and $p_i^u | G_n$. Notice that if the p_i-adic limit $\lim_{u \to \infty} g(u)$ exists, then by Lemma 4.2 it is equal to θ_i.

Remark 3. If $B = \pm 1$, we can extend the sequence $\{G_n\}_{n=0}^{\infty}$ to negative indices n as follows. For $n < 0$, we define

$$G_n = \lambda\alpha^n + \mu\beta^n = B^n\left(\mu\alpha^{|n|} + \lambda\beta^{|n|}\right) \in \mathbb{Z}.$$

We can solve Eq. (1.1) with $n \in \mathbb{Z}$ not necessarily nonnegative, by applying Algorithm A twice: once for $\{G_n\}_{n=0}^{\infty}$, and once for the sequence $\{G_n'\}_{n=0}^{\infty}$, defined by $G_n' = G_{-n}$. Notice that

$$\theta_i' = -\frac{\log_{p_i}(-\mu/\lambda)}{\log_{p_i}(\alpha/\beta)} = +\frac{\log_{p_i}(-\lambda/\mu)}{\log_{p_i}(\alpha/\beta)} = -\theta_i \qquad (i = 1, \ldots, t).$$

Now, instead of applying the algorithm twice, we can modify it, so that it works for all $n \in \mathbb{Z}$.

Lemmas 3.2 and 4.2 remain correct if we replace n by $|n|$. In Theorem 4.1, the lower bound for n_0 must be replaced by

$$n_0 > \max\left(2, \left|\log|\mu/\lambda|\right|/\log|\alpha/\beta|, \left|\log|\lambda/\mu|\right|/\log|\alpha/\beta|\right),$$

and γ has to be replaced by

$$\gamma = \min\left(|\lambda/w| - |\mu/w|\,|\alpha/\beta|^{-n_0}, |\mu/w| - |\lambda/w|\,|\alpha/\beta|^{-n_0}\right).$$

Similar modifications should be made in step (i) of Algorithm A. Further, in step (ii), r_i should be chosen so large that

$$\underline{\text{if}}\ p_i \neq 2\ \underline{\text{then}}\ p_i^{r_i} \geqslant N_0 \text{ and } u_{i,r_i} \neq 0,\ u_{i,r_i} \neq p - 1;$$
$$\underline{\text{else}}\ p_i^{r_i - 1} \geqslant N_0 \text{ and } u_{i,r_i} \neq u_{i,r_i - 1};$$

and similar modifications have to be made in step (v). With these changes, Theorem 4.5 remains true with n replaced by $|n|$.

4D. *Examples*. We give two examples, one of the reduction algorithm, and one example where the reduction algorithm fails, because $\theta_i = 0$.

First Example. Let $A = 6$, $B = 1$, $G_0 = 1$, $G_1 = 4$, $w = 1$, $p_1 = 2$, $p_2 = 11$. Then $\alpha = 3 + 2\sqrt{2}$, $\beta = 3 - 2\sqrt{2}$, $\lambda = (1 + 2\sqrt{2})/4\sqrt{2}$, $\mu = (-1 + 2\sqrt{2})/4\sqrt{2}$, and $\Delta = 32$. With $n_0 = e^{60} = 1.142\ldots \times 10^{26}$ we find from (3.1) that $C_1 < 2.49 \times 10^{20}$. With the modifications of Subsection 4C we have in Theorem 4.1 $\gamma > 0.323$, $C_2 < 1.76$, $C_3 < 2.62 \times 10^{26}$, $C_2C_3 < 4.62 \times 10^{26}$. Hence, all solutions of $G_n = 2^{m_1}11^{m_2}$ satisfy $|n| < 4.62 \times 10^{26}$, m_1, $m_2 < 2.62 \times 10^{26}$. We perform the reduction algorithm step by step:

(i) $n_0 = 2$, $\gamma > 0.303$, $g_1 = 0$, $g_2 = 1$, $g > 0.0275$, $h_1 = -1$, $h_2 = \frac{1}{2}$, $N_0 = 4.62 \times 10^{26}$.

(ii) $\theta_1 = 0.10111\ 10111\ 01000\ 11100\ 10100\ 01001\ 10001\ 10010$
$00001\ 11101\ 01000\ 10000\ 01001\ 10011\ 10101\ 01101$
$11100\ 01011\ 00001\ 11010\ 00011\ 01001\ 01010\ 00101$
$10001\ 01011\ 00000\ 11001\ 01011\ 11101\ 10100\ 01011$
$001 \ldots.$ *

$\theta_2 = 0.\mathrm{A}9359\ 05530\ 7330\mathrm{A}\ 1\mathrm{A}223\ 96230\ 3\mathrm{A}006\ \mathrm{A}3366\ 83368$
$8270 \ldots.$ **

so $r_1 = 90$ (since $u_{1,89} = 1$, $u_{1,90} = 0$, $2^{89} > N_0$), $r_2 = 29$ (since $u_{2,29} = 6$, $11^{29} > N_0$).

(iii) $s_{1,0} = 91$, $s_{2,0} = 30$;

(v-vii) $s_{1,1} = 90$, $s_{2,1} = 29$, $K_1 =$ .true., $N_1 < 76.9$;

(v-vii) $s_{1,2} = 10$, $s_{2,2} = 2$, $K_2 =$ .true., $N_2 < 8.7$;

(v-vii) $s_{1,3} = 6$, $s_{2,3} = 1$, $K_3 =$ .true., $N_3 < 5.8$;

(v-vii) $s_{1,4} = 6$, $s_{2,4} = 1$, $K_4 =$ .false., $N_4 < 5.8$.

Hence, $|n| \leqslant 5$, $m_1 \leqslant 6$, $m_2 \leqslant 2$. We have

n	-5	-4	-3	-2	-1	0	1	2	3	4	5
G_n	2174	373	64	11	2	1	4	23	134	781	4552

So there are 5 solutions: with $n = -3, -2, -1, 0$, and 1.

Second Example. Let $A = 16$, $B = 1$, $G_0 = 1$, $G_1 = 8$, $w = 1$, $p_1 = 2$, $p_2 = 11$. Then $\alpha = 8 + 3\sqrt{7}$, $\beta = 8 - 3\sqrt{7}$, $\lambda = \mu = \frac{1}{2}$, so $\lambda/\mu = 1$ is a root of unity, hence $\theta_1 = \theta_2 = 0$. Notice that $\{G_n\}$ is of type $\{S_n\}$. We have

n	-3	-2	-1	0	1	2	3
G_n	2024	127	8	1	8	127	2024
$G_n \pmod{16}$	8	-1	8	1	8	-1	8
$G_n \pmod{11}$	0	6	8	1	8	6	0
$G_n \pmod{11^2}$	88	6	8	1	8	6	88

It follows that $\mathrm{ord}_2(G_n)$ is 0 or 3, according as n is even or odd, and $\mathrm{ord}_{11}(G_n) > 0$ if and only if $n \equiv 3 \pmod 6$. Now, $G_3 \mid G_{3k}$ for all odd k. Notice that $11^2 \nmid G_3$, and G_3 is not 11 times a power of 2. Hence, G_3 has an odd prime divisor different from 11, namely 23. It follows that $23 \mid G_n$ whenever $11 \mid G_n$. Thus $m_2 = 0$, and there remain only three solutions: for $n = -1, 0$, and 1.

We note that it is not difficult to prove that a similar argument applies whenever $\lambda/\mu = \pm 1$.

5. The Generalized Ramanujan-Nagell Equation. The most interesting application of the reduction algorithm of the preceding section seems to be the solution of the generalized Ramanujan-Nagell equation (1.2). Let k be a nonzero integer, and $p_1, \ldots, p_t$ distinct prime numbers. Then we ask for all nonnegative integers x, $z_1, \ldots, z_t$ with

$$x^2 + k = p_1^{z_1} \cdots p_t^{z_t}.$$

* We write the p-adic number $\sum_{l=0}^{\infty} u_l p^l$ as $0.u_0 u_1 u_2 \ldots.$

** A denotes 10.

First we note that $z_i = 0$ whenever $-k$ is a quadratic nonresidue $(\bmod\, p_i)$. Thus we assume that this is not the case for all i. Let $p_i \mid k$ for $i = 1, \dots, s$ and $p_i \nmid k$ for $i = s+1, \dots, t$. Let $\operatorname{ord}_{p_i}(k)$ be odd for $i = 1, \dots, r$ and even for $i = r+1, \dots, s$. Dividing by large enough powers of p_i $(i = 1, \dots, s)$, (1.2) reduces to a finite number of equations

$$D_0 x_1^2 + k_1 = p_{r+1}^{z'_{r+1}} \cdots p_t^{z'_t} \tag{5.1}$$

with $p_i \nmid k_1$ $(i = 1, \dots, t)$ and D_0 composed of $p_1, \dots, p_r$ only, and squarefree. We distinguish between the 2^{t-r} combinations of z'_i odd or even $(i = r+1, \dots, t)$. Suppose that z'_i is odd for $i = r+1, \dots, u$ and even for $i = u+1, \dots, t$. Put

$$y = p_{r+1}^{(z'_{r+1}-1)/2} \cdots p_u^{(z'_u-1)/2} p_{u+1}^{z'_{u+1}/2} \cdots p_t^{z'_t/2}; \tag{5.2}$$

then, from (5.1),

$$D_0 x_1^2 - p_{r+1} \cdots p_u y^2 = -k_1. \tag{5.3}$$

Put $D = D_0 p_{r+1} \cdots p_u$. Then (5.2) and (5.3) lead to

$$\begin{cases} v^2 - Dw^2 = k_2, \\ v = p_{r+1}^{m_{r+1}} \cdots p_t^{m_t}, \end{cases} \tag{5.4}$$

with $v = p_{r+1} \cdots p_u y$, $w = x_1$, $k_2 = k_1 p_{r+1} \cdots p_u$, and also to

$$\begin{cases} v^2 - Dw^2 = k_2, \\ w = p_{r+1}^{m_{r+1}} \cdots p_t^{m_t}, \end{cases} \tag{5.5}$$

with $v = D_0 x_1$, $w = y$, $k_2 = -k_1 D_0$. We proceed with either (5.4) or (5.5), whichever is the most convenient (e.g., the one with the smaller $|k_2|$).

If $D = 1$, then (5.4) and (5.5) are trivial. So assume $D > 1$. Let $\varepsilon \in \mathbb{Z} + \sqrt{D}\,\mathbb{Z}$ be the smallest unit with $\varepsilon > 1$ and $N(\varepsilon) = \pm 1$. It is well known that the solutions v, w of $v^2 - Dw^2 = k_2$ decompose into a finite number of classes of associated solutions. Let there be T classes, and choose in the τth class $(\tau = 1, \dots, T)$ the solution $v_{\tau,0}$, $w_{\tau,0}$ such that $\gamma_\tau = v_{\tau,0} + w_{\tau,0}\sqrt{D} > 1$ is minimal. Then all solutions of $v^2 - Dw^2 = k_2$ are given by $v = \pm v_{\tau,n}$, $w = \pm w_{\tau,n}$, with

$$\begin{cases} v_{\tau,n} = \left(\gamma_\tau \varepsilon^n + \gamma'_\tau \varepsilon^{-n}\right)/2, \\ w_{\tau,n} = \left(\gamma_\tau \varepsilon^n - \gamma'_\tau \varepsilon^{-n}\right)/2\sqrt{D} \end{cases} \tag{5.6}$$

for $n \in \mathbb{Z}$, where $\gamma'_\tau = v_{\tau,0} - w_{\tau,0}\sqrt{D}$. That is, $\{v_{\tau,n}\}_{n=-\infty}^{\infty}$ and $\{w_{\tau,n}\}_{n=-\infty}^{\infty}$ are linear binary recurrence sequences. Now, (5.4) and (5.5) reduce to T equations of type (1.1). If $k_2 = 1$, then $\gamma_\tau = \varepsilon$, $\gamma'_\tau = \varepsilon^{-1}$. If $k_2 \mid 2D$, $k_2 \neq 1$, then it is easy to prove that $\gamma_\tau^2 = |k_2|\varepsilon$, $\gamma_\tau'^2 = |k_2|\varepsilon^{-1}$, so that

$$\begin{aligned} v_{\tau,n} &= |k_2|^{1/2}\left(\left(\gamma_\tau |k_2|^{-1/2}\right)^{2n+1} + \left(\gamma'_\tau |k_2|^{-1/2}\right)^{2n+1}\right)/2, \\ w_{\tau,n} &= |k_2|^{1/2}\left(\left(\gamma_\tau |k_2|^{-1/2}\right)^{2n+1} - \left(\gamma'_\tau |k_2|^{-1/2}\right)^{2n+1}\right)/2\sqrt{D}. \end{aligned}$$

In both cases, (5.4) and (5.5) can be solved by elementary means (see the remarks following Lemma 4.4, and Mahler [10]). If $k_2 \nmid 2D$, then we apply the reduction algorithm to one of the equations $v_{\tau,n} = p_{r+1}^{m_{r+1}} \cdots p_t^{m_t}$, $w_{\tau,n} = p_{r+1}^{m_{r+1}} \cdots p_t^{m_t}$. Notice that n is allowed to be negative, so we can apply the modified algorithm (see Subsection 4C, Remark 3).

Thus we have a procedure for solving (1.2). It is well known how the unit ε and the minimal solutions $v_{\tau,0}$, $w_{\tau,0}$ $(\tau = 1, \ldots, T)$ can be computed by the continued fraction algorithm.

We conclude this section with an example.

THEOREM 5.1. *The only nonnegative integers x such that $x^2 + 7$ has no prime divisors larger than* 20 *are the* 16 *in the following table*:

x	$x^2 + 7$	x	$x^2 + 7$	x	$x^2 + 7$	x	$x^2 + 7$
0	7	5	$32 = 2^5$	13	$176 = 2^4 \times 11$	53	$2816 = 2^8 \times 11$
1	$8 = 2^3$	7	$56 = 2^3 \times 7$	21	$448 = 2^6 \times 7$	75	$5632 = 2^9 \times 11$
2	11	9	$88 = 2^3 \times 11$	31	$968 = 2^3 \times 11^2$	181	$32768 = 2^{15}$
3	$16 = 2^4$	11	$128 = 2^7$	35	$1232 = 2^4 \times 7 \times 11$	273	$74536 = 2^3 \times 7 \times 11^3$

Sketch of Proof. Since -7 is a quadratic nonresidue modulo 3, 5, 13, 17, and 19, we have only the primes 2, 7, and 11 left. Only one factor 7 can occur, thus we have to solve the two equations

$$x^2 + 7 = 2^{z_1} 11^{z_2}, \tag{5.7}$$

$$x^2 + 7 = 7 \times 2^{z_1} 11^{z_2}. \tag{5.8}$$

Equation (5.8) can be solved in an elementary way. We distinguish four cases, each leading to an equation of the type

$$y^2 - Dz^2 = c$$

with $c \mid 2D$, and either y or z composed of factors 2 and 11 only. We have

(i) z_1 even, z_2 even, $y = 2^{z_1/2} 11^{z_2/2}$, $z = x/7$, $c = 1$, $D = 7$;

(ii) z_1 odd, z_2 even, $y = 2^{(z_1+1)/2} 11^{z_2/2}$, $z = x/7$, $c = 2$, $D = 14$;

(iii) z_1 even, z_2 odd, $y = x$, $z = 2^{z_1/2} 11^{(z_2-1)/2}$, $c = -7$, $D = 77$;

(iv) z_1 odd, z_2 odd, $y = x$, $z = 2^{(z_1-1)/2} 11^{(z_2-1)/2}$, $c = -7$, $D = 154$.

In the second example of Subsection 4D we have worked out case (i). We leave the other cases to the reader.

Equation (5.7) can be solved by the reduction algorithm. Again, we have four cases, each leading to an equation of the type

$$y^2 - Dz^2 = c$$

with either y or z composed of factors 2 and 11 only. We have

(i) z_1 even, z_2 even, $y = x$, $z = 2^{z_1/2} 11^{z_2/2}$, $c = -7$, $D = 1$;

(ii) z_1 odd, z_2 even, $y = x$, $z = 2^{(z_1-1)/2} 11^{z_2/2}$, $c = -7$, $D = 2$;

(iii) z_1 even, z_2 odd, $y = x$, $z = 2^{z_1/2} 11^{(z_2-1)/2}$, $c = -7$, $D = 11$;

(iv) z_1 odd, z_2 odd, $y = x$, $z = 2^{(z_1-1)/2} 11^{(z_2-1)/2}$, $c = -7$, $D = 22$.

Case (i) is trivial. The other three cases each lead to one equation of type (1.1). In the first example of Subsection 4D we have worked out case (ii). With the following data the reader should be able to perform Algorithm A by hand for the cases (iii) and (iv), thus completing the proof. It will be safe to take $N < 10^{30}$.

Case (iii) $\alpha = 10 + 3\sqrt{11}$, $\lambda = (2 + \sqrt{11})/2\sqrt{11}$,

θ_1 = 0.10011 01000 00110 10100 00110 10110 01001 11110
11011 10010 00001 10110 10111 10100 00110 01101
01010 10010 11101 11001 10000 10010 01010 11011
00010 00111 01110 00101 01101 01111 10101 11110
10....

θ_2 = 0.23075 76425 39004 26090 A92A1 03757 07314 58414
7A238....

Case (iv) $\alpha = 197 + 42\sqrt{22}$, $\lambda = (9 + 2\sqrt{22})/2\sqrt{22}$,

θ_1 = 0.11101 01101 01110 01010 10111 10001 00100 00011
10000 00110 10101 01100 01101 01111 01101 10101
01011 10100 01100 11101 10011 00011 00010 11110
10101 01100 10011 11111 01001 01110 00000 01110
011....

θ_2 = 0.6A001 68184 22921 902A0 724A4 16769 45650 16482
5A6AA....

Remark. Let $\Phi(X,Y) = aX^2 + bXY + cY^2$ be a quadratic form with integral coefficients, and $\Delta = b^2 - 4ac$ positive or negative. Let k be a nonzero integer, and $p_1, \dots, p_t$ distinct prime numbers. Then we notice that

$$4a\Phi(X,Y) = (2aX + bY)^2 - \Delta Y^2,$$

so that the diophantine equation

$$\Phi(X,k) = p_1^{z_1} \cdots p_t^{z_t}$$

in integers $X \neq 0$, $z_1, \dots, z_t \geqslant 0$, can be solved by our method. Also the equation

$$\Phi(X, p_1^{z_1} \cdots p_t^{z_t}) = k$$

can be solved in this way.

Acknowledgments. We thank F. Beukers and R. Tijdeman for their comments. The first-named author was supported by a fellowship of the Alexander von Humboldt Stiftung. The second-named author was supported by the Netherlands Foundation for Mathematics (SMC) with finanical aid from the Netherlands Organization for the Advancement of Pure Research (ZWO).

KLTE Matematikai Intézet
H-4010 Debrecen Pf 12, Hungary

Mathematisch Instituut R. U. Leiden
Postbus 9512
2300 RA Leiden, The Netherlands

1. A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, New York, 1975.

2. F. Beukers, "On the generalized Ramanujan-Nagell equation," I: *Acta Arith.*, v. 38, 1981, pp. 389–410; II: *Acta Arith.*, v. 39, 1981, pp. 113–123.

3. A. Bremner, R. Calderbank, P. Hanlon, P. Morton & J. Wolfskill, "Two-weight ternary codes and the equation $y^2 = 4 \times 3^\alpha + 13$," *J. Number Theory*, v. 16, 1983, pp. 212–234.

4. J.-H. Evertse, "On equations in S-units and the Thue-Mahler equation," *Invent. Math.*, v. 75, 1984, pp. 561–584.

5. H. Hasse, "Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung," *Nagoya Math. J.*, v. 27, 1966, pp. 77–102.

6. N. Koblitz, *p-Adic Numbers, p-Adic Analysis and Zeta-Functions*, Springer-Verlag, New York, 1977.

7. D. H. Lehmer, "On a problem of Størmer," *Illinois J. Math.*, v. 8, 1964, pp. 57–79.

8. F. J. MacWilliams & N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

9. K. Mahler, "Eine arithmetische Eigenschaft der rekurrierenden Reihen," *Mathematika B (Leiden)*, v. 3, 1934, pp. 153–156.

10. K. Mahler, "Über den grössten Primteiler spezieller Polynome zweiten Grades," *Arch. Math. Naturvid. B*, v. 41, 1935, pp. 3–26.

11. M. Mignotte, "On the automatic resolution of certain diophantine equations," in *EUROSAM* 84, *Proceedings*, Lecture Notes in Comput. Sci., v. 174, Springer-Verlag, 1984, pp. 378–385.

12. A. Pethö, "Perfect powers in second order recurrences," in *Topics in Classical Number Theory*, Colloq. Math. Soc. Jànos Bolyai, vol. 34, Budapest, 1981, pp. 1217–1227.

13. A. Pethö, "Full cubes in the Fibonacci sequence," *Publ. Math. Debrecen*, v. 30, 1983, pp. 117–127.

14. A. Pethö, "On the solution of the diophantine equation $G_n = p^z$," *Proceedings EUROCAL* 85, Linz, Austria, Vol. 2, Lecture Notes in Comput. Sci., vol. 204, Springer-Verlag, 1985, pp. 503–512.

15. A. J. van der Poorten, "Linear forms in logarithms in the p-adic case," in *Transcendence Theory: Advances and Applications* (A. Baker & D. W. Masser, eds.), Academic Press, London, 1977, pp. 29–57.

16. A. Schinzel, "On two theorems of Gelfond and some of their applications," *Acta Arith.*, v. 13, 1967, pp. 177–236.

17. T. N. Shorey & R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1986.

18. C. Størmer, "Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications," *Skrifter Videnskabs-selskabet I, Math.-Naturv. Kl.*, 1897, pp. 1–48.

19. R. J. Stroeker & R. Tijdeman, "Diophantine equations," in *Computational Methods in Number Theory* (H. W. Lenstra, Jr. & R. Tijdeman, eds.), MC Tract 155, Amsterdam, 1982, pp. 321–369.

20. N. Tzanakis, "On the diophantine equation $y^2 - D = 2^k$," *J. Number Theory*, v. 17, 1983, pp. 144–164.

21. N. Tzanakis & J. Wolfskill, "On the diophantine equation $y^2 = 4q^n + 4q + 1$," *J. Number Theory*. (To appear.)

22. N. Tzanakis & J. Wolfskill, "The diophantine equation $x^2 = 4q^{a/2} + 4q + 1$ with an application in coding theory." (To appear.)

23. B. M. M. de Weger, "Products of prime powers in binary recurrence sequences II," *Math. Comp.*, v. 47, 1986, pp. 729–739.