MATHEMATICS OF COMPUTATION
VOLUME 47, NUMBER 176
OCTOBER 1986, PAGES 729-739

Products of Prime Powers in Binary Recurrence Sequences Part II: The Elliptic Case, with an Application to a Mixed Quadratic-Exponential Equation

By B. M. M. de Weger

Abstract. In Part I the diophantine equation $G_n = wp_1^{m_1} \cdots p_t^{m_t}$ was studied, where $\{G_n\}_{n=0}^{\infty}$ is a linear binary recurrence sequence with positive discriminant. In this second part we extend this to negative discriminants. We use the p-adic and complex Gelfond-Baker theory to find explicit upper bounds for the solutions of the equation. We give algorithms to reduce those bounds, based on diophantine approximation techniques. Thus we have a method to solve the equation completely for arbitrary values of the parameters. We give an application to a quadratic-exponential equation.

6. Introduction and Preliminaries.

6A. *Introduction.* It is assumed that the reader is familiar with Part I of this paper (Pethö and de Weger [4]). We adopt notations and assumptions from Part I without further reference.

In Part I we studied Eq. (1.1):

$$G_n = wp_1^{m_1} \cdots p_t^{m_t},$$

for $\Delta > 0$. The p-adic Gelfond-Baker theory, together with a trivial observation on the exponential growth of $|G_n|$, provided us with upper bounds for the solutions. In the case $\Delta < 0$, which is our present topic, the situation is essentially more complicated. The p-adic behavior of G_n does not depend on the sign of the discriminant. But in the case $\Delta < 0$, the growth of $|G_n|$ is not as nice as in the case $\Delta > 0$. However, information on its growth can be obtained from the complex Gelfond-Baker theory. The fact that Eq. (1.1) has only finitely many solutions was shown by Mahler [3].

Section 7 is devoted to the complex arguments. In it we solve the diophantine inequality $|G_n| \leqslant v$ for a fixed v. An upper bound for n is given that has particularly good dependence on v. We present algorithms to reduce this upper bound, so that the inequality can be solved completely in any practical case. These algorithms are not new; they come essentially from Baker and Davenport [1] and Cijsouw, Korlaar, and Tijdeman (appendix to Stroeker and Tijdeman [5]).

Received December 13, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11B37, 11D61, 11J87, 11Y50.

In Subsection 8A we combine the results of Sections 3 and 7 to obtain explicit upper bounds for (1.1). In Subsection 8B an algorithm is presented to reduce these upper bounds. It is a combination of the algorithms of Sections 4 and 7. We give an example in Subsection 8C. Finally, in Section 9 we present an application to a certain type of mixed quadratic-exponential diophantine equation.

6B. *Preliminaries.* Let in the sequel $\Delta < 0$. Since α/β is not a root of unity, $B \geqslant 2$. Since (α, β) and (λ, μ) are pairs of complex conjugates, $|\alpha| = |\beta|$ and $|\lambda| = |\mu|$. Thus $L = \log\max(|eD|^{1/4}, |\alpha\lambda\sqrt{D}|)$. Lemmas 3.2, 4.2, and 4.3 hold also for $\Delta < 0$.

As in the case $\Delta > 0$, we have to exclude the case where only finitely many p_i-adic digits of θ_i are nonzero. Let $\rho = \frac{1}{2}(1 + \sqrt{-3})$.

LEMMA 6.1. *If only finitely many p_i-adic digits $u_{i,l}$ of θ_i are nonzero, then $\theta_i = 0$, and $G_n = \pm R_n$, κS_n, κT_n or κU_n, where $\kappa \in \mathbb{Q}$, and*

$$R_n = (\alpha^n - \beta^n)/(\alpha - \beta), \qquad S_n = \alpha^n + \beta^n,$$
$$T_n = (1 \pm \sqrt{-1})\alpha^n + (1 \mp \sqrt{-1})\beta^n,$$
$$U_n = (1 \pm \omega)\alpha^n + (1 \pm \bar{\omega})\beta^n, \qquad \omega = \rho \text{ or } \bar{\rho}.$$

The case $G_n = \kappa T_n$ can occur only if $d = -1$, and $G_n = \kappa U_n$ only if $d = -3$.

Proof. As in the proof of Lemma 4.4, $\theta_i = r \in \mathbb{Z}$, and $(\beta/\alpha)^r(\mu/\lambda) = \eta$ is a root of unity. Then $\eta\lambda\alpha^r = \mu\beta^r$, hence

$$G_n = \lambda\alpha^r(\alpha^{n-r} + \eta\beta^{n-r}).$$

Recall that $B = \alpha\beta \geqslant 2$. Notice that

$$G_0 B(\eta\alpha^{r-1} + \beta^{r-1}) = G_1(\eta\alpha^r + \beta^r).$$

By $(B, G_1) = 1$, it follows that $\alpha\beta \mid \eta\alpha^r + \beta^r$. By $(A, B) = 1$, we have $(\alpha, \beta) = (1)$, and from $\alpha \mid \beta^r$ it then follows that $\theta_i = r = 0$. So $G_0 = \lambda(1 + \eta) \in \mathbb{Z}$. Then $\lambda = \kappa(1 + \bar{\eta})$ for some $\kappa \in \mathbb{Q}$. Choose κ such that $G_0, G_1 \in \mathbb{Z}$ and $(G_0, G_1) = 1$. Now the result follows easily, since for η there are only the possibilities ± 1, and $\pm\sqrt{-1}$ if $d = -1$, and $\pm\rho$, $\pm\bar{\rho}$ if $d = -3$. □

In the cases of Lemma 6.1, Eq. (1.1) can be treated as follows. The smallest index $n = g(mp^l)$ such that $mp^l \mid G_n$ grows exponentially with l. Also G_n grows exponentially with n (see Theorem 7.2). Hence $G_{g(mp^l)}$ grows double exponentially with l. It follows that $wp_1^{m_1} \cdots p_t^{m_t}$ cannot keep up with $G_{g(wp_1^{m_1} \cdots p_t^{m_t})}$. So, if $m_1, \ldots, m_t$ are large enough, there is a prime q such that $q \mid G_{g(wp_1^{m_1} \cdots p_t^{m_t})}$, but $q \nmid wp_1^{m_1} \cdots p_t^{m_t}$. Now the special properties of the sequences R_n, S_n, T_n, and U_n can be employed to prove that $q \mid G_n$ whenever $wp_1^{m_1} \cdots p_t^{m_t} \mid G_n$. We illustrate this with an example.

Let $A = 5$, $B = 13$, $G_0 = G_1 = 1$. Then $\Delta = -27$, $\alpha = 1 + 3\rho$, $\lambda = (1 + \rho)/3$. We solve $G_n = \pm 2^m$. The sequence $G_n = \lambda\alpha^n + \bar{\lambda}\bar{\alpha}^n$ is related to the sequence $H_n = \bar{\lambda}\alpha^n + \lambda\bar{\alpha}^n$. In fact, we have $G_n H_n R_n = R_{3n}/3$. Since R_n has nice divisibility properties, we thus have information on the prime divisors of G_n and H_n. We find:

n	0	1	2	3	4	5	6	7	8
G_n	1	1	−8	−53	−161	−116	1513	9073	25696
H_n	1	4	7	−17	−176	−659	−1007	3532	30751
R_n	0	1	5	12	−5	−181	−840	−1847	1685

Now $G_n \equiv 0 \pmod{16}$ if and only if $n \equiv 8 \pmod{12}$, $H_n \equiv 0 \pmod{16}$ if and only if $n \equiv 4 \pmod{12}$, and $R_n \equiv 0 \pmod{16}$ if and only if $n \equiv 0 \pmod{12}$. Further, $G_4 H_4 R_4 = R_{12}/3 = -2^4 \cdot 5 \cdot 7 \cdot 11 \cdot 23$, and it follows that $2^4 \cdot 7 \cdot 11 \cdot 23 | G_n H_n$ for all $n \equiv 0 \pmod 4$. In fact, $11 | G_n$ whenever $16 | G_n$. Thus $G_n = \pm 2^m$ implies $m \leqslant 3$. In the next section we show how to solve $|G_n| \leqslant 8$.

Another way to treat (1.1) in the case $\theta_i = 0$ is the following. By Lemma 4.2, $m_i \leqslant g_i + 1 + \operatorname{ord}_{p_i}(n)$. Hence,

$$|G_n| = |w| p_1^{m_1} \cdots p_t^{m_t} \leqslant v_0 n$$

for some constant v_0. Only minor changes in the arguments of Section 7 suffice to deal with this inequality, instead of $|G_n| \leqslant v$.

7. The Growth of the Recurrence Sequence.

7A. *Application of a Theorem of Waldschmidt.* In this subsection we study the diophantine inequality

$$(7.1) \qquad |G_n| \leqslant v$$

for a fixed $v \in \mathbb{R}$, $v \geqslant 1$. We apply a result of Waldschmidt [6] from the complex Gelfond-Baker theory, which gives an upper bound for n that is particularly good in v. See also Kiss [2].

Let a_0 for $\xi \in \mathbb{Q}(\sqrt{\Delta})$ be the leading coefficient of its minimal polynomial. We define the height of ξ by

$$h(\xi) = \tfrac{1}{2} \log a_0 + \log \max(1, |\xi|),$$

in accordance with Waldschmidt's height function (cf. [6, p. 259]). Let $\alpha_1, \dots, \alpha_n \in \mathbb{Q}(\sqrt{\Delta})$, $b_1, \dots, b_n \in \mathbb{Z}$. Put

$$\Lambda = b_1 \operatorname{Log} \alpha_1 + \cdots + b_n \operatorname{Log} \alpha_n,$$

where Log denotes the principal value of the complex logarithm, i.e., $-\pi < \operatorname{Im} \operatorname{Log} z \leqslant \pi$. Assume $\Lambda \neq 0$. Let $V_1, \dots, V_n$ be real numbers with $\frac{1}{2} \leqslant V_1 \leqslant \cdots \leqslant V_n$, and $V_i \geqslant \max\{h(\alpha_i), \frac{1}{2}|\operatorname{Log} \alpha_i|\}$ $(i = 1, \dots, n)$. Put $W = \max_{1 \leqslant i \leqslant n} \log|b_i|$. Define $V_i^+ = \max(1, V_i)$ for $i = n-1, n$. Put

$$C_4 = 2^{9n+53} n^{2n} V_1 \cdots V_n \log(2eV_{n-1}^+), \qquad C_5 = C_4 \log(2eV_n^+).$$

THEOREM 7.1 (WALDSCHMIDT). *With the above definitions,*

$$|\Lambda| > \exp\{-(C_4 W + C_5)\}.$$

We apply this to (7.1) as follows. Let

$$\begin{aligned}
&E = -\lambda\mu\Delta, \\
&U_2 = \tfrac{1}{2} \max(\pi, \log B), \qquad U_3 = \tfrac{1}{2} \max(\pi, \log E), \\
&U_2^+ = \min(U_2, U_3), \qquad U_3^+ = \max(U_2, U_3), \\
&C_4' = 2^{79} 3^6 U_2 U_3 \log(2eU_2^+), \qquad C_5' = C_4' \log(4eU_3^+), \\
&C_6 = \bigl(\log(\pi/2|\mu|) + C_5' + C_4' \log(4C_4'/\log B)\bigr) \times 4/\log B.
\end{aligned}$$

Theorem 7.2. *Let $v \in \mathbb{R}$, $v \geqslant 1$. Then all solutions $n \geqslant 0$ of* (7.1) *satisfy*

$$n < C_6 + \frac{4}{\log B} \log \max\left(v, 2\left|G_0 \mu \sqrt{\Delta}\right|\right).$$

Remark. Notice that C_6 does not depend on v.

Proof. By $\Delta < 0$, both (α, β) and (λ, μ) are pairs of complex conjugates. Hence $|\alpha| = |\beta| = B^{1/2} \geqslant \sqrt{2}$. We have from (7.1)

$$\left|\left(\frac{-\lambda}{\mu}\right)\left(\frac{\alpha}{\beta}\right)^n - 1\right| \leqslant \frac{v}{|\mu|} B^{-n/2}. \tag{7.2}$$

We may assume $n \geqslant 2$. Let $-\lambda/\mu = e^{2\pi i \psi}$, $\alpha/\beta = e^{2\pi i \phi}$, with $-\frac{1}{2} < \phi \leqslant \frac{1}{2}$, $-\frac{1}{2} < \psi \leqslant \frac{1}{2}$. Let $k_0, k_1 \in \mathbb{Z}$ be such that $|j\psi + n\phi + k_j| \leqslant \frac{1}{2}$. Then $|k_j| \leqslant 1 + \frac{1}{2}n \leqslant n$ $(j = 0, 1)$. Put

$$\Lambda_j = 2\pi i\left(j\psi + n\phi + k_j\right) = j \operatorname{Log}\left(\frac{-\lambda}{\mu}\right) + n \operatorname{Log}\left(\frac{\alpha}{\beta}\right) + 2k_j \operatorname{Log}(-1)$$

for $j = 0, 1$. It is an easy exercise to show that $|x| \leqslant \frac{1}{4}|e^{2\pi i x} - 1|$ holds for all $x \in \mathbb{R}$ with $|x| \leqslant \frac{1}{2}$. Now, from (7.2) we have an upper bound for $|\Lambda_1|$:

$$\begin{aligned}|\Lambda_1| &= 2\pi|\psi + n\phi + k_1| \leqslant \frac{\pi}{2}\left|e^{2\pi i(\psi + n\phi + k_1)} - 1\right| \\ &= \frac{\pi}{2}\left|\left(\frac{-\lambda}{\mu}\right)\left(\frac{\alpha}{\beta}\right)^n - 1\right| \leqslant \frac{\pi}{2|\mu|} v B^{-n/2}.\end{aligned}$$

It may happen that $\Lambda_1 = 0$. In that case, $\psi + n\phi \in \mathbb{Z}$, hence $-(\lambda/\mu)(\alpha/\beta)^n = 1$, and it follows that $G_n = \lambda\alpha^n + \mu\beta^n = 0$. Kiss [2] showed that this implies $|R_n| \leqslant 2|G_0|$, where $R_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. From this, Kiss derived an upper bound for n. We shall follow his argument, but we apply another, sharper result from the Gelfond-Baker theory than Kiss. Notice that, by $|\beta| = B^{1/2}$,

$$2|G_0| \geqslant |R_n| = \frac{B^{n/2}}{\sqrt{|\Delta|}}\left|\left(\frac{\alpha}{\beta}\right)^n - 1\right| \geqslant \frac{4B^{n/2}}{\sqrt{|\Delta|}}|\phi n + k_0| = \frac{2B^{n/2}}{\pi\sqrt{|\Delta|}}|\Lambda_0|.$$

Now $\Lambda_0 \neq 0$, since by $n \geqslant 2$ the contrary would imply $\phi \in \mathbb{Q}$, which is impossible, since α/β is not a root of unity. Thus, take $j = 1$ if $\Lambda_1 \neq 0$, and $j = 0$ otherwise. Then $\Lambda_j \neq 0$, and

$$|\Lambda_j| \leqslant \frac{\pi}{2|\mu|} \max\left(v, 2\left|G_0\mu\sqrt{\Delta}\right|\right) B^{-n/2}. \tag{7.3}$$

From Theorem 7.1 we can derive a lower bound for $|\Lambda_j|$. Notice that $\max(j, n, 2|k_j|) \leqslant 2n$, so that $W = \log(2n)$. We choose $V_1 = \frac{1}{2}$. The number α/β satisfies

$$Bx^2 - (A^2 - 2B)x + B = 0,$$

hence $h(\alpha/\beta) \leqslant \frac{1}{2}\log B$. And $-\lambda/\mu$ satisfies

$$Ex^2 - \left(2E + \Delta G_0^2\right)x + E = 0,$$

hence $h(-\lambda/\mu) \leqslant \frac{1}{2}\log E$. Thus $V_2 = U_2^+$, $V_3 = U_3^+$ satisfy the requirements for Theorem 7.1. We find

$$\begin{aligned}|\Lambda_j| &> \exp\left\{-C_4'\left(\log(2n) + \log(2eU_3^+)\right)\right\} \\ &= \exp\left\{-\left(C_4' \log n + C_5'\right)\right\}.\end{aligned} \tag{7.4}$$

Combining (7.3) and (7.4) we find $n < a + b\log n$, where

$$a = \frac{2}{\log B}\left(\log\max\left(v, 2\left|G_0\mu\sqrt{\Delta}\right|\right) + \log\frac{\pi}{2|\mu|} + C_5'\right),$$
$$b = 2C_4'/\log B.$$

The result follows from Lemma 2.2 (Part I), since

$$b = 2C_4'/\log B = 2^{78}3^6\,\frac{\max(\pi, \log B)}{\log B}\max(\pi, \log E)\log(2eU_2^+),$$

which is certainly larger than e^2. □

We now want to reduce the bound from Theorem 7.2. We do this by studying the diophantine inequality

$$(7.5)\qquad |\psi_j + n\phi + k_j| < v_0B^{-n/2},$$

where $\psi_j = j\psi$ and $v_0 = \max(v, 2|G_0\mu\sqrt{\Delta}|)/4|\mu|$. We have to distinguish between $\psi_j = 0$ (the homogeneous case) and $\psi_j \neq 0$ (the inhomogeneous case).

7B. *The Homogeneous Case*. We first study the easier case $\psi_j = 0$. We have the following algorithm. Let N be an upper bound for the solutions of (7.5), for example the bound found in Theorem 7.2.

ALGORITHM B (reduces given upper bound for (7.5) in the case $\psi_j = 0$).

Input: ϕ, B, $|\mu|$, v_0, N.

Output: new, better bound N^* for n.

(i) (initialization) *Choose* $n_0 \geqslant 2/\log B$ *such that* $B^{n_0/2}/n_0 \geqslant 2v_0$; $N_0 := [N]$; *compute the continued fraction*

$$|\phi| = \left[0, a_1, a_2, \ldots, a_{l_0+1}, \ldots\right]$$

and the denominators $q_1, \ldots, q_{l_0+1}$ *of the convergents of* $|\phi|$, *with* l_0 *so large that* $q_{l_0} \leqslant N_0 < q_{l_0+1}$; $i := 0$;

(ii) (compute new bound) $A_i := \max(a_1, \ldots, a_{l_i+1})$; *compute the largest integer* N_{i+1} *such that*

$$B^{N_{i+1}/2}/N_{i+1} \leqslant v_0(A_i + 2);$$

and l_{i+1} *such that* $q_{l_{i+1}} \leqslant N_{i+1} < q_{l_{i+1}+1}$;

(iii) (terminate loop)

if $n_0 \leqslant N_{i+1} < N_i$ then $i := i + 1$, goto (ii);

else $N^* := \max(n_0, N_{i+1})$, stop.

LEMMA 7.3. *Algorithm* B *terminates. Inequality* (7.5) *with* $\psi_j = 0$ *has no solutions with* $N^* < n < N$.

Proof. Termination is trivial, since all N_i are integers. Notice that $B^{x/2}/x$ is an increasing function for $x \geqslant 2/\log B$. Hence, if $n \geqslant n_0$,

$$\left|\,|\phi| - |k_j|/n\right| \leqslant v_0B^{-n/2}/n < 1/2n^2.$$

It follows that $|k_j|/n$ is a convergent of $|\phi|$, say $|k_j|/n = p_m/q_m$. Then $q_m \leqslant n$, and, as is well known,

$$\left|\,|\phi| - p_m/q_m\right| > 1/(a_{m+1} + 2)q_m^2.$$

Suppose $n \leqslant N_i$ for some $i \geqslant 0$. Then $m \leqslant l_i$. Hence,

$$B^{n/2}/n \leqslant v_0 n^{-2}\left| |\phi| - |k_j|/n \right|^{-1} < v_0(a_{m+1} + 2) \leqslant v_0(A_m + 2).$$

It follows that if $N_{i+1} \geqslant n_0$, then $n \leqslant N_{i+1}$. □

We notice that the above algorithm is similar to those of Cijsouw, Korlaar, and Tijdeman (appendix to Stroeker and Tijdeman [5]), and of D. C. Hunt and A. J. van der Poorten (unpublished manuscript).

7C. *The Inhomogeneous Case*. In the more complicated case $\psi_j \neq 0$, we use a technique due to H. Davenport (see Baker and Davenport [1, pp. 133–134]). Again, let N be an upper bound for n.

ALGORITHM C (reduces upper bound for (7.5) in the case $\psi_j \neq 0$).

Input: ϕ, ψ_j, B, v_0, N.

Output: new, better upper bound N^* for all but a finite number of explicitly given n.

(i) (initialization) $N_0 := [N]$; *compute the continued fraction*

$$|\phi| = [0, a_1, \ldots, a_{l_0}, \ldots]$$

and the convergents p_i/q_i $(i = 1, \ldots, l_0)$, *with* l_0 *so large that* $q_{l_0} > 4N_0$ *and* $\|q_{l_0}\psi_j\| > 2N_0/q_{l_0}$ *. (*If such* l_0 *cannot be found within reasonable time, take* l_0 *so large that* $q_{l_0} > 4N_0$); $i := 0$;

(ii) (compute new bound)

if $\|q_{l_i}\psi_j\| > 2N_i/q_{l_i}$ then $N_{i+1} := [2\log(q_{l_i}^2 v_0/N_i)/\log B]$;
else *compute* $K \in \mathbb{Z}$ *with* $|K - q_{l_i}\psi_j| \leqslant \frac{1}{2}$;
compute $n_0 \in \mathbb{Z}, 0 \leqslant n_0 < q_{l_i}$, *with*
$K + n_0 p_{l_i} \equiv 0 \pmod{q_{l_i}}$,
if $n = n_0$ *is a solution of* (7.5), then
print an appropriate message;
$N_{i+1} := [2\log(4q_{l_i}v_0)/\log B]$;

(iii) (terminate loop)

if $N_{i+1} < N_i$ then $i := i + 1$;
compute the minimal $l_i < l_{i-1}$ *such that* $q_{l_i} > 4N_i$ *and* $\|q_{l_i}\psi_j\| > 2N_i/q_{l_i}$ (*If such* l_i *does not exist, choose the minimal* l_i *such that* $q_{l_i} > 4N_i$);
goto (ii);
else $N^* := N_i$, stop.

LEMMA 7.4. *Algorithm* C *terminates. Inequality* (7.5) *with* $\psi_j \neq 0$ *has for* $N^* < n < N$ *only the finitely many solutions found by the algorithm.*

Proof. It is clear that the algorithm terminates. Suppose that $n \leqslant N_i$ for some $i \geqslant 0$. Then if $\|q_{l_i}\psi_j\| > 2N_i/q_{l_i}$, we have

$$\begin{aligned}\|q_{l_i}\psi_j\| &= \|q_{l_i}(\psi_j + n\phi + k_j) - n\phi q_{l_i}\| \\ &\leqslant q_{l_i}|\psi_j + n\phi + k_j| + n/q_{l_i} \leqslant q_{l_i}v_0 B^{-n/2} + N_i/q_{l_i}.\end{aligned}$$

* $\|\cdot\|$ denotes the distance to the nearest integer.

It follows that $n \leqslant N_{i+1}$. If $\|q_{l_i}\psi_j\| \leqslant 2N_i/q_{l_i}$, then

$$|K + np_{l_i} + k_j q_{l_i}| \leqslant |K - q_{l_i}\psi_j| + q_{l_i}|\psi_j + n\phi + k_j| + n|p_{l_i} - q_{l_i}\phi|$$
$$\leqslant \tfrac{1}{2} + q_{l_i}v_0 B^{-n/2} + N_i/q_{l_i} < \tfrac{3}{4} + q_{l_i}v_0 B^{-n/2}.$$

Suppose that $q_{l_i}v_0 B^{-n/2} \leqslant \frac{1}{4}$. Then $K + np_{l_i} + k_j q_{l_i} = 0$, since it is an integer. By $(p_{l_i}, q_{l_i}) = 1$ it follows that $n \equiv n_0 \pmod{q_{l_i}}$. Since $q_{l_i} > N_i$, $n = n_0$ is the only possibility. Suppose next that $q_{l_i}v_0 B^{-n/2} > \frac{1}{4}$. Then $n \leqslant N_{i+1}$ follows immediately. □

We remark that in practice one almost always finds an l_i such that $\|q_{l_i}\psi_j\| > 2N_i/q_{l_i}$, if N_i is large enough.

8. How to Solve (1.1).

8A. *Bounds for the Solutions.* Combining the results from the p-adic and the complex Gelfond-Baker theory (Lemma 3.2 and Theorem 7.2), we now derive upper bounds for the solutions of (1.1) with $\Delta < 0$.

THEOREM 8.1. *Put* $C_1 = \max_{1 \leqslant i \leqslant t}(C_{1,i})$ *and* $P = p_1 \cdots p_t$. *Further, put*

$$C_7 = \max\left\{C_6 + \frac{4}{\log B}\log\left(2|G_0\mu\sqrt{\Delta}|\right),\right.$$
$$\left. 8\left(\left(C_6 + \frac{4\log|w|}{\log B}\right)^{1/3} + \left(\frac{4C_1\log P}{\log B}\right)^{1/3}\log\left(\frac{108C_1\log P}{\log B}\right)\right)^3\right\},$$
$$C_{8,i} = C_{1,i}(\log C_7)^3 \qquad (i = 1, \ldots, t).$$

Then all solutions of (1.1) *satisfy*

$$n < C_7, \quad m_i < C_{8,i} \qquad (i = 1, \ldots, t).$$

Proof. From Lemma 3.2 and Theorem 7.2 with $v = |w|p_1^{m_1} \cdots p_t^{m_t}$, we see that

$$n < C_6 + \frac{4}{\log B}\log\left(2|G_0\mu\sqrt{\Delta}|\right),$$

or

$$n < C_6 + \frac{4\log|w|}{\log B} + \frac{4C_1\log P}{\log B}(\log n)^3.$$

The result now follows from Lemma 2.2 if $4C_1\log P/\log B > (e^2/3)^3$. This is certainly true. □

8B. *The Algorithm.* We present an algorithm to reduce upper bounds for the solutions of Eq. (1.1). The idea is to apply alternatingly algorithms A and one of B and C. Let N be an upper bound for n, for example $N = C_7$.

ALGORITHM D (reduces upper bounds for the solutions of (1.1)).

Input: α, β, λ, μ, w, $p_1, \ldots, p_t$, N.

Output: new, better bounds N^*, M_i for n and m_i $(i = 1, \ldots, t)$.

(i) (initialization) $N_0 := [N]$; $j := 1$;

$$\left.\begin{aligned} g_i &:= \operatorname{ord}_{p_i}(\lambda) + \operatorname{ord}_{p_i}\left(\log_{p_i}(\alpha/\beta)\right) \\ h_i &:= \operatorname{ord}_{p_i}(\lambda) + \begin{cases} 3/2 & \text{if } p_i = 2 \\ 1 & \text{if } p_i = 3 \\ 1/2 & \text{if } p_i \geqslant 5 \end{cases} \end{aligned}\right\} \quad (i = 1, \ldots, t);$$

(ii) (computation of the θ_i's, ϕ and ψ)
compute for $i = 1, \ldots, t$ *the first* r_i p_i*-adic digits 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* $u_{i,r_i} \neq 0$; *compute* $\psi = \mathrm{Log}(-\lambda/\mu)/2\pi i$, *and the continued fraction*

$$|\phi| = \left| \frac{1}{2\pi i} \mathrm{Log}(\alpha/\beta) \right| = [0, a_1, \ldots, a_{l_0}, \ldots]$$

with the convergents p_i/q_i $(i = 1, \ldots, l_0)$, *where* l_0 *is so large that* $q_{l_0 - 1} \leqslant N_0 < q_{l_0}$ *if* $\psi = 0$; $q_{l_0} > 4N_0$ *and* $\|q_{l_0}\psi\| > 2N_0/q_{l_0}$ *if* $\psi \neq 0$ *and such* l_0 *can be found in a reasonable amount of time*, $q_{l_0} > 4N_0$ *otherwise.*

(iii) (one step of Algorithm A)
$M_{i,j} := \max(h_i, g_i + \min\{s \in \mathbb{Z}\colon s \geqslant 0 \text{ and } p_i^s \geqslant N_{j-1} \text{ and } u_{i,s} \neq 0\})$ $(i = 1, \ldots, t)$;

(iv) (one step of Algorithm B or C)

<u>if</u> $\psi = 0$ <u>then</u> $A := \max(a_1, \ldots, a_{l_{j-1}})$; $v := |w| p_1^{M_{1,j}} \cdots p_t^{M_{t,j}}$;
  choose $n_0 \geqslant 2/\log B$ *such that* $B^{n_0/2}/n_0 \geqslant v/2|\mu|$;
  compute the largest integer N_j *such that* $B^{N_j/2}/N_j \leqslant (A + 2)v/4|\mu|$;
  $N_j := \max(n_0, N_j)$;
  <u>if</u> $N_j < N_{j-1}$ <u>then</u> *compute* l_j *such that*
    $q_{l_j - 1} \leqslant N_j < q_{l_j}$;
    $j := j + 1$; <u>goto</u> (iii);

<u>else</u> <u>if</u> $\|q_{l_{j-1}}\psi\| > 2N_{j-1}/q_{l_{j-1}}$
  <u>then</u> $N_j := [2\log(q_{l_{j-1}}^2 v/4|\mu|N_{j-1})/\log B]$;
  <u>else</u> *compute* $K \in \mathbb{Z}$ *with* $|K - q_{l_{j-1}}\psi| \leqslant \frac{1}{2}$;
    compute $n_0 \in \mathbb{Z}$, $0 \leqslant n_0 < q_{l_{j-1}}$,
    with $K + n_0 p_{l_{j-1}} \equiv 0 \pmod{q_{l_{j-1}}}$;
    <u>if</u> $n = n_0$ *is a solution of* (1.1)
     <u>then</u> *print an appropriate message*;
    $N_j := [2\log(q_{l_{j-1}} v/|\mu|)/\log B]$;
  <u>if</u> $N_j < N_{j-1}$ <u>then</u> *compute the minimal* $l_j < l_{j-1}$ *such that*
    $q_{l_j} > 4N_j$ *and* $\|q_{l_j}\psi\| > 2N_j/q_{l_j}$ (*if such* l_j *does not exist, choose the minimal* l_j *such that* $q_{l_j} > 4N_j$);
    $j := j + 1$; <u>goto</u> (iii);

(v) (termination) $N^* := N_{j-1}$; $M_i := M_{i,j}$ $(i = 1, \ldots, t)$; <u>stop</u>.

THEOREM 8.2. *Algorithm* D *terminates. Equation* (1.1) *has no solutions with* $N^* < n < N$ *and* $m_i > M_i$ $(i = 1, \ldots, t)$, *apart from those spotted by the algorithm.*

Proof. Clear, from the proofs of Lemmas 7.3 and 7.4. □

8C. *An Example.* Let $A = 1$, $B = 2$, $G_0 = 2$, $G_1 = 3$, then $\Delta = -7$, $\alpha = (1 + \sqrt{-7})/2$, $\lambda = (2 + \sqrt{-7})/\sqrt{-7}$. Let $w = \pm 1$, $p_1 = 3$, $p_2 = 7$. We have with $n_0 = 2$: $C_1 < 6.40 \times 10^{16}$, $C_6 < 9.14 \times 10^{29}$, $C_7 < 7.42 \times 10^{30}$, $C_8 < 2.30 \times 10^{22}$.

Further, $g_1 = 1$, $g_2 = 0$, $h_1 = 1$, $h_2 = 0$. Let $N_0 = 7.42 \times 10^{30}$. We have

$$\begin{aligned}
\phi &= \operatorname{Log}(\alpha/\beta)/2\pi i = \left(\pi - \arctan(\sqrt{7}/3)\right)/2\pi \\
&= [0, 2, \quad 1, 1, 2, 16, \quad 6, \ 1, \quad 2, 2, 13, \\
&\qquad 1, \quad 1, 3, 1, \ 1, \quad 2, \ 1, \quad 2, 1, \ 1, \\
&\qquad 1, \quad 1, 1, 9, \ 2, \quad 1, \ 2, \quad 1, 7, \ 1, \\
&\qquad 6, 269, 4, 3, \ 1, \quad 1, 50, \quad 2, 1, \ 6, \\
&\qquad 1, \quad 1, 2, 1, \ 1, \quad 7, \ 1, 61, 1, 12, \\
&\qquad 3, \quad 7, 4, 7, \ 3, 121, \quad 1, 21, 2, \quad 1, 7, \ldots], \\
\psi &= \operatorname{Log}(-\lambda/\mu)/2\pi i = \left(\pi - \arctan(4\sqrt{7}/3)\right)/2\pi \\
&= 0.29396\,28336\,99645\,40267\,89566\,60520\,01908\,06203\ldots, \\
\theta_1 &= 0.20010\,12210\,00011\,02102\,00211\,00222\,02220\,12021 \\
&\qquad 10020\,20202\,21102\,00121\,01000\,01002\,11100\,20122 \\
&\qquad 11111\,22202\,21021\,02212\,2200\ldots, \\
\theta_2 &= 0.32542\,12042\,43561\,34020\,61561\,13452\,10116\,33152 \\
&\qquad 25336\,45044\,11254\,55033\ldots.
\end{aligned}$$

Now, $M_{1,1} = 67$, $M_{2,1} = 37$; we choose $l_0 = 61$, since

$$q_{61} = 142\,51183\,31142\,44361\,19375\,51238\,81743 > 4N_0,$$

and $\|q_{61}\psi\| = 0.24487\ldots > 2N_0/q_{61} = 0.104\ldots$. So we find $N_1 = 637$. Next, $M_{1,2} = 7$, $M_{2,2} = 4$; we choose $l_1 = 9$, since $q_9 = 10102 > 4 \times 637$, and $\|q_9\psi\| = 0.38745\ldots > 2 \times 637/10102$. So we find $N_2 = 74$. Next, $M_{1,3} = 6$, $M_{2,3} = 3$; we choose $l_2 = 6$, since $q_6 = 1291 > 4 \times 74$, and $\|q_6\psi\| = 0.49398\ldots > 2 \times 74/1291$. So we find $N_3 = 60$. In the next step we find no improvement. Hence $n \leqslant 60$, $m_1 \leqslant 6$, $m_2 \leqslant 3$. It is a matter of straightforward computation to check that there are the following 6 solutions of $G_n = \pm 3^{m_1}7^{m_2}$: $G_1 = 3$, $G_2 = -1$, $G_3 = -7$, $G_5 = 9$, $G_7 = 1$, $G_{17} = 441$.

9. A Mixed Quadratic-Exponential Equation. In this section, we give an application of the preceding algorithm to the following diophantine equation. Let

$$\Phi(X, Y) = aX^2 + bXY + cY^2$$

be a quadratic form with integral coefficients, such that $D = b^2 - 4ac < 0$. Let q, v, w be nonzero integers, and $p_1, \ldots, p_t$ prime numbers. Consider the equation

$$\text{(9.1)} \qquad \begin{cases} \Phi(X, Y) = vq^n, \\ Y = wp_1^{m_1} \cdots p_t^{m_t} \end{cases}$$

in integers X, $n \geqslant 0$, $m_i \geqslant 0$ $(i = 1, \ldots, t)$.

Let β, $\bar{\beta}$ be the roots of $\Phi(x, 1)$. Let h be the class number of $\mathbf{Q}(\sqrt{D})$. There exists a $\pi \in \mathbf{Q}(\sqrt{D})$ such that we have the principal ideal equation $(\pi)(\bar{\pi}) = (q^h)$. Put $n = n_1 + hn_2$, with $0 \leqslant n_1 < h$. Then $\Phi(X, Y) = vq^n$ is equivalent to finitely many ideal equations

$$(aX - a\beta Y)(aX - a\bar{\beta}Y) = (\sigma)(\bar{\sigma})(\pi)^{n_2}(\bar{\pi})^{n_2},$$

with $(\sigma)(\bar{\sigma}) = (avq^{n_1})$. Hence we have the equations (in algebraic numbers)

$$\begin{cases} aX - a\beta Y = \gamma\pi^{n_2}, \\ aX - a\bar{\beta}Y = \bar{\gamma}\bar{\pi}^{n_2}, \end{cases} \qquad \begin{cases} aX - a\beta Y = \gamma\bar{\pi}^{n_2}, \\ aX - a\bar{\beta}Y = \bar{\gamma}\pi^{n_2}, \end{cases}$$

where γ is composed of units, common divisors of $aX - a\beta Y$, $aX - a\bar{\beta}Y$, and σ. Notice that there are only finitely many choices for γ possible. Thus, (9.1) is equivalent to a finite number of equations

$$a(\bar{\beta} - \beta)wp_1^{m_1} \cdots p_t^{m_t} = \gamma\pi^{n_2} - \bar{\gamma}\bar{\pi}^{n_2},$$

or, if we put $\lambda = \gamma/a(\bar{\beta} - \beta)$ and $G_{n_2} = \lambda\pi^{n_2} + \bar{\lambda}\bar{\pi}^{n_2}$,

(9.2) $$G_{n_2} = wp_1^{m_1} \cdots p_t^{m_t}.$$

Here $\{G_{n_2}\}_{n_2=0}^{\infty}$ is a recurrence sequence with negative discriminant. So (9.2) is of type (1.1), and it can thus be solved by the method presented in Sections 7 and 8.

Before giving an example, we remark that Eq. (9.1) with $D > 0$ is not solvable with our method. This is due to the fact that in $\mathbf{Q}(\sqrt{D})$ with $D > 0$ there are infinitely many units, hence infinitely many possibilities for γ. Another generalization of Eq. (9.1) is to replace q^n by $q_1^{n_1} \cdots q_s^{n_s}$. This problem is also not solvable by our method, since it does not lead to a binary recurrence sequence if $s \geqslant 2$. It seems that these problems can be solved by using multi-dimensional approximation techniques. This is the subject of further investigations by the author.

We finally present an example.

THEOREM 9.1. *The equation*

$$X^2 - 3^{m_1}7^{m_2}X + 2(3^{m_1}7^{m_2})^2 = 11 \cdot 2^n$$

in integers X, $n \geqslant 0$, $m_1 \geqslant 0$, $m_2 \geqslant 0$ has only the following solutions:

n	m_1	m_2	X		n	m_1	m_2	X	
1	1	0	−1,	4	5	2	0	−10,	19
1	0	0	−4,	5	6	0	0	−26,	27
2	0	0	−6,	7	7	0	0	−37,	38
3	0	1	2,	5	7	3	0	2,	25
3	1	0	−7,	10	11	1	1	−137,	158
4	0	1	−6,	13	17	2	2	−829,	1270

Sketch of Proof. Put $\beta = (1 + \sqrt{-7})/2$. Then

$$X^2 - XY + 2Y^2 = (X - \beta Y)(X - \bar{\beta}Y).$$

Notice that $\mathbf{Q}(\sqrt{-7})$ has class number 1, and that

$$2 = (1 + \sqrt{-7})/2 \times (1 - \sqrt{-7})/2, \qquad 11 = (2 + \sqrt{-7})(2 - \sqrt{-7}).$$

Suppose $\gamma \mid X - \beta Y$ and $\gamma \mid X - \bar{\beta}Y$. Then $\gamma \mid (\bar{\beta} - \beta)Y = -\sqrt{-7}\,3^{m_1}7^{m_2}$. On the other hand, $\gamma \mid 11 \cdot 2^n$. It follows that $\gamma = \pm 1$; hence $X - \beta Y$ and $X - \bar{\beta}Y$ are coprime. Thus we have two possibilities:

$$X - \beta Y = \pm(2 \pm \sqrt{-7})\left(\frac{1 \pm \sqrt{-7}}{2}\right)^n,$$

$$X - \beta Y = \pm(2 \mp \sqrt{-7})\left(\frac{1 \pm \sqrt{-7}}{2}\right)^n,$$

in each equation the 2nd and 3rd $\pm$ being independent. Hence, we have to solve

$$G_n^{(j)} = \lambda^{(j)}\beta^n + \bar{\lambda}^{(j)}\bar{\beta}^n = 3^{m_1}7^{m_2} \qquad (j = 1,2), \tag{9.3}$$

with $G_{n+1}^{(j)} = G_n^{(j)} - 2G_{n-1}^{(j)}$ $(j = 1,2)$ and $\lambda^{(1)} = \bar{\lambda}^{(2)} = (2 + \sqrt{-7})/\sqrt{-7}$, so that $G_0^{(1)} = G_0^{(2)} = 1$, $G_1^{(1)} = 3$, $G_1^{(2)} = -1$. Notice that $\theta_i^{(1)} = -\theta_i^{(2)}$ $(i = 1,2)$, and $\psi^{(1)} = -\psi^{(2)}$. For $j = 1$ we solved (9.3) in the example of Subsection 8C. We leave it to the reader to solve (9.3) for $j = 2$; this can be done with the numerical data given in Subsection 8C. □

Acknowledgments. The author wishes to thank F. Beukers, A. Pethö and R. Tijdeman for their comments. He was supported by the Netherlands Foundation for Mathematics (SMC) with financial aid from the Netherlands Organization for the Advancement of Pure Research (ZWO).

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

1. A. BAKER & H. DAVENPORT, "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$," *Quart. J. Math. Oxford Ser.* (2), v. 20, 1969, pp. 129–137.

2. P. KISS, "Zero terms in second order linear recurrences," *Math. Sem. Notes Kobe Univ.*, v. 7, 1979, pp. 145–152.

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

4. A. PETHÖ & B. M. M. DE WEGER, "Products of prime powers in binary recurrence sequences. I," *Math. Comp.*, v. 47, 1986, pp. 713–727.

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

6. M. WALDSCHMIDT, "A lower bound for linear forms in logarithms," *Acta Arith.*, v. 37, 1980, pp. 257–283.