JOURNAL OF NUMBER THEORY 15, 5–13 (1982)

Perfect Powers in Second Order Linear Recurrences

ATTILA PETHÖ

Mathematical Institut, Kossuth Lajos University, Debrecen, Pf. 12, 4010, Hungary

Communicated by P. Erdös

Received September 8, 1980; revised December 22, 1980

IN MEMORY OF MY MOTHER

Let A, B, G_0, G_1 be integers, and $G_n = AG_{n-1} - BG_{n-2}$ for $n \geqslant 2$. Let further S be the set of all nonzero integers composed of primes from some fixed finite set. In this paper we shall prove that natural conditions for A, B, G_0 and G_1 imply, that the diophantine equation $G_n = wx^q$ has only finitely many solutions in integers $|x| > 1$, $q \geqslant 2$, n and $w \in S$.

1. INTRODUCTION

Let A, B, G_0, G_1 be integers. We define a sequence $\{G_n\}$ by the recurrence relation

$$G_n = AG_{n-1} - BG_{n-2}, \qquad n = 2, 3, \ldots. \tag{1}$$

These sequences play an important role in various branches of number theory. Of particular interest are the Fibonacci and the Lucas sequences, which are defined with the initial terms $A = -B = G_1 = 1$, $G_0 = 0$ and $A = -B = G_1 = 1$, $G_0 = 2$. Their nth term will be denoted by F_n and L_n, respectively.

Let S be the set of all nonzero integers composed of primes from some fixed finite set. In this paper we deal with the solvability of the Diophantine equation

$$G_n = wx^q \tag{2}$$

in integers $w \in S$, $q \geqslant 2$, x, n.

Equation (2) was completely solved for F_n and L_n with $w = 1$, $q = 2$ by Wylie [12] and Cohn [2]—further with $w = q = 2$ by Cohn [3]. Bumby [1] and Cohn [4] have applied these results to solve Diophantine equations. In his book [10] Mordell gave a review of the results mentioned above.

0022-314X/82/040005-09$02.00/0

Recently Györy *et al.* [6], and Györy [5] have established the finiteness of the number of solutions of (2) for $G_0 = 0$, $G_1 = 1$ and $x = 1$, independently from A and B.

Put $C = G_1^2 - AG_0G_1 + BG_0^2$ and $D = A^2 - 4B$. We can now formulate the main result.

THEOREM. *Suppose* $A \neq 0$, $|G_0| + |G_1| \neq 0$, $(A, B) = 1$, $A^2 \neq iB$, *where* $i = 1, 2, 3$ *or* 4. *Suppose further that* D *is not a perfect square if* $BC = 0$. *Then Eq.* (2) *in integers* $w \in S$, $q \geqslant 2$, x, n *implies*

$$\begin{aligned} \max\{|w|, |x|, n, q\} &< C_1, \qquad \text{if} \quad |x| > 1, \\ \max\{|w|, n\} &< C_2, \qquad \text{if} \quad |x| = 1, \\ n &< C_3, \qquad \text{if} \quad x = 0, \end{aligned}$$

where C_1, C_2, C_3 *are effectively computable constants depending only on* A, B, G_0, G_1 *and* S.

Let α and β be the roots of the equation

$$X^2 - AX + B = 0. \tag{3}$$

Put $a = G_1 - G_0\alpha$ and $b = G_1 - G_0\beta$. Then

$$G_n = \frac{a\alpha^n - b\beta^n}{\alpha - \beta} \qquad (\alpha \neq \beta).$$

An immediate consequence of the Theorem is the following:

COROLLARY. *Let* $A \neq 0, B, G_0, G_1$ *be integers such that* $(A, B) = 1$, $A^2 \neq iB$, *where* $i = 1, 2, 3$ *or* 4, *and* $B(G_1^2 - AG_0G_1 + BG_0^2) \neq 0$. *Let further* α *and* β *be the roots of* (3) *and let* a, b *be defined as above. Then*

$$(a\alpha^n - b\beta^n)/(\alpha - \beta) = wx^q,$$

in integers $w \in S$, $q \geqslant 2$, x, n *implies*

$$\begin{aligned} \max\{|w|, |x|, n, q\} &< C_4, \qquad \textit{if} \quad |x| > 1, \\ \max\{|w|, n\} &< C_5, \qquad \textit{if} \quad |x| = 1, \\ n &< C_6, \qquad \textit{if} \quad x = 0, \end{aligned}$$

where C_4, C_5, C_6 *are effectively computable constants depending only on* A, B, G_0, G_1 *and* S.

If α and β are integers, this is a special case of Theorem 3 [11].

Remarks. From the hypothesis of the Theorem it follows, that α/β, where α and β are the roots of (3), is not a root of unity and that $ab \neq 0$.

In fact if $D > 0$, then α and β are real and α/β is a root of unity if and only if $\alpha = \pm\beta$. On the other hand $\alpha + \beta = -A$ and $\alpha\beta = B$. Now $\alpha \neq -\beta$ because $A \neq 0$, while $\alpha \neq \beta$ because $A^2 \neq 4B$.

If $D < 0$, then α and β are conjugate complex numbers. Let $\alpha/\beta = \varepsilon$ be a root of unity. α and β are quadratic algebraic numbers, so ε is a quadratic integer. But these are only $\varepsilon = \pm i$ and $\varepsilon = (\pm 1 \pm i\sqrt{3})/2$. From $\varepsilon = \pm i$ follows $A^2 = 2B$; from $\varepsilon = (-1 \pm i\sqrt{3})/2$ follows $A^2 = B$, finally from $\varepsilon = (1 \pm i\sqrt{3})/2$ follows $A^2 = 3B$. But these are not allowed in the Theorem.

Finally $a = 0$ means $G_1 - G_0\alpha = 0$. G_0 can not be zero, so $\alpha = G_1/G_0$. Now (3) yields $(G_1/G_0)^2 - AG_1/G_0 + B = 0$ or $C = G_1^2 - AG_1G_0 + BG_0^2 = 0$. Further α is rational, therefore D must be a perfect square.

2. Auxiliary Results

We base the proof of the Theorem on the following results, which were all proved by Baker's method.

THEOREM A. *Let $f(x, y) \in Q[x, y]$ be a binary form with $f(1, 0) \neq 0$ such that among the linear factors in the factorisation of f at least two are distinct. Let d be a positive integer. Then the equation*

$$f(x, y) = wz^q$$

in integers $w \in S, y \in S, q \geqslant 3, x, z$ with $(x, y) = d$, $|z| > 1$ implies that

$$\max\{|w|, |x|, |y|, |z|, q\} < C_7,$$

where C_7 is an effectively computable constant depending only on f, d and S.

This is due to Schinzel *et. al.* [11].

THEOREM B. *Let $f(x) \in Q[x]$ be a quadratic polynomial with distinct roots and for integral x let $P(x)$ denote the greatest positive prime factor of $f(x)$. Then there exists an effectively computable constant C_8 depending only on f such that*

$$P(x) > C_8 \log\log|x|.$$

This was proved by Keates [7]. It has many generalisations. In this connection see also [11].

THEOREM C. *Let $A \neq 0, (A, B) = 1$, $|G_1| + |G_0| \neq 0$, $A^2 \neq iB$ with $i = 1, 2, 3$ or 4, and $C \neq 0$. Then the sequence G_n defined by (1) has at most*

one zero term. Further there is an effectively computable constant C_9 *depending only on* A, B, G_0 *and* G_1 *such that* $G_n \neq 0$ *for any* $n > C_9$.

If $D < 0$, then (3) has conjugate complex roots. They have equal absolute values. A lower bound for G_n is therefore more difficult to obtain than in the case $D > 0$.

THEOREM D. *Suppose* $A \neq 0$, $D < 0$, $(A, B) = 1$, $|G_0| + |G_1| \neq 0$. *Further let* α, β *be the roots of* (3) *and let* a, b *be defined as above. Finally suppose that* α/β *is not a root of unity. Then there is an effectively computable constant* C_{10} *depending only on* A, B, G_0, G_1 *such that for any* $n > C_9$

$$\frac{|a|}{2\sqrt{|D|}}|\alpha^n| n^{-C_{10}} < |G_n| \leqslant \frac{2|a|}{\sqrt{|D|}}|\alpha^n|$$

is satisfied.

Theorems C and D were proved by Kiss [8]. He shows there explicitly, how the constants C_9 and C_{10} depend on A, B, G_0, G_1.

3. Lemmas on Second Order Linear Recurrences

In this section we shall use the notations, defined in the Introduction.

LEMMA 1. *Let* A, B, G_0, G_1 *be integers, and let* G_n *for* $n \geqslant 2$ *be defined by* (1). *Then for any* $n \geqslant 0$

$$G_{n+1}^2 - AG_{n+1}G_n + BG_n^2 = CB^n. \tag{4}$$

This was proved in the special case $G_0 = 0$, $G_1 = |B| = 1$ by Kiss [9].

Proof. We prove the Lemma by induction. For $n = 0$ (4) is obviously true. Further by (1)

$$\begin{aligned} G_{n+2}^2 - AG_{n+2}G_{n+1} + BG_{n+1}^2 \\ = (AG_{n+1} - BG_n)^2 - A(AG_{n+1} - BG_n)G_{n+1} + BG_{n+1}^2 \\ = B(G_{n+1}^2 - AG_{n+1}G_n + BG_n^2) = BCB^n = CB^{n+1} \end{aligned}$$

is satisfied for $n > 0$.

LEMMA 2. *Let* A, B, G_1 *be nonzero integers. If the prime number* p *divides* B, *but does not divide* AG_1, *then it does not divide* G_n *for* $n \geqslant 1$.

Proof. For $n = 1$ the Lemma is obviously true. Suppose $p \nmid G_n$ for some $n \geqslant 1$. Then by (1)

$$G_{n+1} + BG_{n-1} = AG_n.$$

This shows, that p/G_{n+1} can not be true, and so the Lemma is proved.

LEMMA 3. *Let* $A, B \neq 0, G_0, G_1$ *be integers with* $(A, B) = 1$, $C \neq 0$, $|G_0| + |G_1| \neq 0$. *Let* p *be a prime divisor of* $(G_1, B) > 1$. *Put* $G_n = p^{\alpha_n}\bar{G}_n$, $C = p^{\gamma}\bar{C}$, $B = p^{\beta}\bar{B}$, *with* $(\bar{G}_n, p) = (\bar{C}, p) = (\bar{B}, p) = 1$ *for* $n \geqslant 0$, $G_n \neq 0$. *If* $G_n = 0$ *for some* n, *then put* $\alpha_n = \alpha_{n+1}$ *and* $\bar{G}_n = 0$. *Finally take* $N_1 = (\gamma - 2\alpha_0)/\beta$. *Then*

$$\alpha_n = \alpha_N \tag{5}$$

is satisfied for any $n \geqslant N$, *with* $N = \max\{[N_1] + 3, 2\}$, *where* $[N_1]$ *denotes the greatest integer* $\leqslant N_1$.

Proof. It follows from (1), that for any $n \geqslant 2$

$$\alpha_n \geqslant \min\{\alpha_{n-1}, \beta + \alpha_{n-2}\} \tag{6}$$

and $>$ is possible only if $\alpha_{n-1} = \beta + \alpha_{n-2}$.

(i) If for some m $\alpha_m \geqslant \alpha_{m+1}$, then

$$\alpha_{m+2} \geqslant \min\{\alpha_{m+1}, \alpha_m + \beta\} = \alpha_{m+1}, \qquad \text{thus } \alpha_{m+1} = \alpha_{m+2} = \cdots.$$

If $\alpha_0 \geqslant \alpha_1$, then (5) follows immediately from (i) with $N = 2$. Furthermore $\alpha_0 < \alpha_1$ implies $G_0 \neq 0$, $\gamma \geqslant 2\alpha_0$ and $N_1 \geqslant 0$.

In the sequel we shall assume that $[N_1] \geqslant 1$. It suffices to prove that the assumption of (i) are satisfied for some $m \leqslant [N_1] + 2$. Suppose, on the contrary, that $\alpha_0 < \alpha_1 < \cdots < \alpha_{[N_1]+2}$. Then $\alpha_k = \alpha_0 + k\beta$ for $k = 0, 1, \ldots, [N_1] + 1$ can be easily proved by the application of (6). This implies $G_k \neq 0$ for $k = 0, 1, \ldots, [N_1] + 1$.

Consider (4) with $n = [N_1]$. The right-hand side is divisible exactly by the $\gamma + [N_1]\beta$th power of p. At the same time the left-hand side is divisible at least by the $2\alpha_0 + (2[N_1] + 1)\beta$th power of p. Thus

$$\gamma + [N_1]\beta \geqslant 2\alpha_0 + (2[N_1] + 1)\beta.$$

But this means that

$$[N_1] \leqslant \frac{\gamma - 2\alpha_0}{\beta} - 1 < \left[\frac{\gamma - 2\alpha_0}{\beta}\right] = [N_1].$$

This is a contradiction, and the proof is completed.

In the following C_{11}, C_{12},..., will denote effectively computable constants depending only on A, B, G_0, G_1 and S.

LEMMA 4. *Under the assumptions of the Theorem*

$$|G_n| < C_{11} \tag{7}$$

implies $n < C_{12}$

Proof. First we observe, that the assumptions imply $B \neq 0$. Let α and β be the roots of

$$X^2 - AX + B = 0.$$

α/β cannot be a root of unity because of the hypothesis of the Theorem, as was pointed out in the Remarks. Put $a = G_1 - G_0\beta$ and $b = G_1 - G_0\alpha$. In the Remarks it was shown, that $ab = 0$ yields $C = 0$ and D is a perfect square. So ab cannot be zero. Further it is well known, that

$$G_n = \frac{a\alpha^n - b\beta^n}{\alpha - \beta}.$$

If $D < 0$, then by Theorem D

$$\frac{|a|}{2\sqrt{|D|}} |\alpha^n| n^{-C_{10}} < |G_n|$$

is satisfied for any $n > C_9$. Therefore by (7)

$$\frac{|a|}{2\sqrt{|D|}} |\alpha^n| n^{-C_{10}} < C_{11}.$$

The function on the left-hand side tends to infinity with n. So there exists a constant C_{13} with $n < C_{13}$. Put $C_{12} = \max\{C_9, C_{13}\}$. This is the required constant if $D < 0$.

If $D > 0$, then α and β are both real. We may assume $|\beta| < |\alpha|$ which implies $\lim_{n\to\infty} (|\beta|/|\alpha|)^n = 0$, so there exists a constant C_{14} with

$$|\alpha|^n < \frac{C_{11}|\alpha - \beta|}{C_{14}}.$$

Hence $n < C_{12} = \log(C_{11}|\alpha - \beta|/C_{14})(\log|\alpha|)^{-1}$, and this completes the proof.

4. Proof of the Theorem

Suppose that the integers $w \in S$, $q \geqslant 2, n, x$ are solutions of (2). If we replace in (4) G_n with wx^q then we obtain the Diophantine equation

$$G_{n+1}^2 - AG_{n+1}wx^q + B(wx^q)^2 = CB^n$$

in integers G_{n+1}, w, x, q. This is solvable in G_{n+1} if and only if there exists an integer z with

$$Dw^2x^{2q} = z^2 - 4CB^n. \tag{8}$$

Assume $C = 0$. Then by the hypothesis of Theorem D cannot be a perfect square. On the other hand (8) yields

$$z^2 = Dw^2x^{2q}.$$

This Diophantine equation has the only integer solution $x = z = 0$. Therefore $G_n = 0$, and by Theorem C there exists a constant C_{15} , with $n < C_{15}$.

In the sequel we shall assume $C \neq 0$. First we observe that the assumptions of the Theorem imply $B \neq 0$. By Lemmas 2 and 3 $(G_n, B^n) = (wx^q, B^n) < C_{16}$. Furthermore $(D, B) = 1$, so we have $(z, B^n) < C_{17}$.

Let S_1 be the set of the prime divisors of D and B. Put $S_0 = S \cup S_1$. (8) can be written in the form

$$vx^{2q} = f_1(z, t), \qquad \text{if} \quad n \text{ even} \tag{9}$$

$$vx^{2q} = f_2(z, t), \qquad \text{if} \quad n \text{ odd}, \tag{10}$$

with $v = Dw^2$, $h = \lfloor n/2 \rfloor$, $t = B^h$, $f_1(z, t) = z^2 - 4Ct^2$, $f_2(z, t) = z^2 - 4CBt^2$. One sees that $f_i(1, 0) = 1$ for $i = 1, 2$ and in the factorization of f_1 and f_2 the two linear factors are distinct. We note finally that $2q \geqslant 4$.

It follows from Theorem A, that there exists an effectively computable constant C_{18} depending only on f_1, f_2, d and S_0 such that for any integer solution $t \in S_0$, $v \in S_0$, $|x| > 1$, $q \geqslant 2$, z with $(z, t) = d < C_{17}$ of (9) and (10)

$$\max\{|t|, |v|, |x|, |z|, q\} < C_{18}$$

is satisfied. But f_1, f_2, S_0 and d, therefore C_{18} also, depend only on A, B, G_0, G_1 and S. Moreover we have

$$|w| = \sqrt{v/D} < C_{18}^{1/2}/\sqrt{|D|}$$

and

$$|G_n| = |w||x|^q < C_{18}^{q+1/2}/\sqrt{|D|}.$$

This yields in combination with Lemma 4 $n < C_{19}$. C_{18} and C_{19} depend on d. Now we can choose C_1 to be the maximum of C_{18} and C_{19} as d runs over its finitely many possible values.

In the sequel we shall prove the Theorem for $|x| \leqslant 1$. First we shall study the case $x = 0$. Then $G_n = 0$ and by Theorem C there is a constant C_3 with $n < C_3$.

It remains to study the case $|x| = 1$. Now from (8) we obtain

$$4CB^n = z^2 - D_1 w^2, \tag{11}$$

with $D_1 = D$ or $D_1 = -D$ according as $x = 1$ or $x = -1$. The function on the right-hand side of (11) satisfies obviously the hypothesis of Theorem A. So if $|B| \neq 1$ and $n > 2$, we have for any integer solution $w \in S$, $n > 2$, z of (11)

$$\max\{|w|, |z|, n\} < C_{20}.$$

If we choose C_{20} large enough, the last inequality remains true for $0 \leqslant n \leqslant 2$ also.

For $|B| = 1$ we put $C_1 = C$ or $C_1 = -C$ according as $B = 1$ or $B = -1$. With this notation if follows from (11) that

$$z^2 - 4C_1 = D_1 w^2. \tag{12}$$

The quadratic polynomial $z^2 - 4C_1$ has two distinct zeros. Hence we obtain from Theorem B

$$|G_n| = |w| < C_{21}.$$

This implies again by Lemma 4, that $n < C_{22}$. Putting C_2 to be the maximum of C_{21} and C_{22} we complete the proof of the Theorem.

Note added in proof. A result similar to our Theorem has been proved by T. N. Shorey and C. L. Stewart, On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, to appear. They proved that (2) has finitely many, effectively computable solutions for any fixed integer d under the hypothesis of our Theorem except $(A, B) = 1$.

REFERENCES

1. R. T. BUMBY, The Diophantine equation $3x^4 - 2y^2 = 1$, *Math. Scand.* **21** (1967), 144-148.
2. J. H. E. COHN, On square Fibonacci numbers, *J. London Math. Soc*, **39** (1964), 537–540.
3. J. H. E. COHN, Lucas and Fibonacci numbers and some Diophantine equations, *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.
4. J. H. E. COHN, Eight Diophantine equations, *Proc. London Math. Soc.* **16** (1966), 153–166. Addendum, *ibid*, **17** (1967), 381.

5. K. GYÖRY, On some arithmetical properties of Lucas and Lehmer numbers, *Acta Arith.*, in press.
6. K. GYÖRY, P. KISS AND A. SCHINZEL, A note on Lucas and Lehmer sequences and their application to Diophantine equations, *Coll. Math.*, in press.
7. M. KEATES, On the greates prime factor of a polynomial, *Proc. Edinburgh Math. Soc.* **16** (1969), 301–303.
8. P. KISS, Zero terms in second order linear recurrences, *Math. Sem. Notes Kobe Univ.* 7 (1979), 145–152.
9. P. KISS, Diophantine representation of generalized Fibonacci numbers, *Elem. Math.* **34** (1979), 129–132.
10. L. J. MORDELL, "Diophantine Equations," Academic Press, New York, 1969.
11. T. N. SHOREY, A. VAN DER POORTEN, R. TIJDEMAN AND A. SCHINZEL, Applications of the Gel'fond–Baker Method to Diophantine equations, *in* "Transcendence Theory: Advances and Applications," Academic Press, New York, 1977.
12. O. WYLIE, Solution of the problem. In the Fibonacci series $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ the first, second and twelfth terms are squares. Are there any others? *Amer. Math. Monthly* **71** (1964), 220–222.