

On two Diophantine equations concerning Lucas sequences

By I. JOÓ and B. M. PHONG (Budapest)

1. Introduction

A linear recurrence $G = \{G_n\}_{n=1}^{\infty}$ of order $k(>1)$ is defined by rational integers $A_1, A_2, \dots, A_k$ and by recursion

$$(1) \quad G_n = A_1 G_{n-1} + A_2 G_{n-2} + \dots + A_k G_{n-k} \quad (n \geq k),$$

where the initial values $G_0, G_1, \dots, G_{k-1}$ are fixed not all zero rational integers and $A_k \neq 0$. Denote the distinct roots of the characteristic polynomial

$$(2) \quad f(x) = x^k - A_1 x^{k-1} - \dots - A_k$$

by $\alpha_1, \alpha_2, \dots, \alpha_t$, where α_i has multiplicity m_i . It is well known (see page 62 of [6]) that for $n \geq 0$

$$G_n = f_1(n)\alpha_1^n + f_2(n)\alpha_2^n + \dots + f_t(n)\alpha_t^n,$$

where $f_i(n)$ is a polynomial of degree at most $m_i - 1$, furthermore the coefficients of $f_i(n)$ are algebraic numbers from the field $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$. We shall say that the sequence G is non-degenerate if $t > 1$ and α_i/α_j is not a root of unity for $1 \leq i < j \leq t$. In case $k=2$ the sequence G is called a second order recurrence, furthermore we say that G is Lucas sequence if $k=2$, $G_0=0$ and $G_1=1$.

Let $p_1, p_2, \dots, p_r$ be rational primes and denote S the set of rational integers which have only these primes as prime factors.

In [3] K. GYÖRY, P. KISS and A. SHINZEL showed that if G is a non-degenerate Lucas sequence, then

$$(3) \quad G_x \in S$$

holds only for finitely many sequences G and for finitely many integers x . K. GYÖRY [2] improved this result giving explicit upper bound for x and for the constants of the sequences which satisfy (3).

The Diophantine equation

$$(4) \quad G_x = wy^q$$

was also studied by several authors. T. N. SHOREY and C. L. STEWART [11] proved that if $y > 1$, $q > 1$ and G is a non-degenerate recurrence of order k for which $m_1 = 1$ and $|\alpha_1| > |\alpha_j|$ ($j=2, \dots, t$), then (4) implies the inequality $q < c$, where c is an effectively computable constant in terms of w and the parameters of the sequence G . They showed that x and y are also bounded for second order recurrences. A PETHŐ [9] proved similar results for second order recurrences supposing $(A_1, A_2) = 1$ and

$w \in S$. For recent general results we refer to the papers by P. KISS [4], I. NEMES and A. PETHŐ [7], T. N. SHOREY and C. L. STEWART [12] further to the references there.

The following problem remained open: if $|\alpha_1| = |\alpha_2| = \dots = |\alpha_t|$, then the equation (4) has finite or infinite solutions? The aim of the present paper is to investigate this question.

Let G be a non-degenerate second order recurrence and t be an integer. Denote $m(t)$ the number of solutions x of the Diophantine equation $G_x = t$. K. K. KUBOTA [5] proved that $m(t) \leq 4$. F. BEUKERS [1] improved this result by showing $m(t) + m(-t) \leq 3$ with finitely many exceptions. He also proved that if G is non-degenerate Lucas sequence, then $m(t) + m(-t) \leq 2$ with at most three exceptions. J. C. PARNAMI and T. N. SHOREY [8] showed that there exists an effectively computable number $N > 0$ depending only on the sequence G such that the equation

$$(5) \quad G_x = G_y$$

has no solutions in non-negative integers x, y with $\max(x, y) > N$ and $x \neq y$. Thus $m(t) \leq 1$ for all larger t .

In below everywhere we denote Lucas sequences by $R = R(A, B)$, that is

$$R_n = AR_{n-1} - BR_{n-2} \quad (n > 1)$$

where $R_0 = 0$, $R_1 = 1$ and A, B are non-zero integers with $D = A^2 - 4B \neq 0$. It is well known that

$$(6) \quad R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α, β are distinct roots of $x^2 - Ax + B = 0$. For fixed integer $k \geq 1$ we put

$$U_0(k) := k, \quad U_n(k) := \frac{R_{kn}}{R_n} \quad (n \geq 1).$$

As is known, $U_n(k)$ -s are integers. Denote $U(k) = \{U_n(k)\}_{n=0}^\infty$. L. SOMER [13] proved that the sequence $U(k)$ is a linear integral recurrence of order k , furthermore the order k is minimal. Indeed, using (6) we get

$$U_n(k) = (\alpha^{k-1})^n + (\alpha^{k-2}\beta)^n + \dots + (\alpha\beta^{k-2})^n + (\beta^{k-1})^n = \alpha_1^n + \dots + \alpha_k^n,$$

where $\alpha_i = \alpha^{k-i} \cdot \beta^{i-1}$. If $D < 0$, then $|\alpha_1| = \dots = |\alpha_k| = |\alpha|^{k-1}$. Consequently, the investigation of the Diophantine equation

$$U_x(k) = wy^q$$

has meaning. We shall prove the following two theorems.

Theorem 1. *Let R be a non-degenerate Lucas sequence with $(A, B) = 1$ and $k \geq 1$ be a fixed integer. Then the Diophantine equation $U_x(k) = wy^q$ in integers $w \in S$, $q \geq 3$, $x, |y| > 1$ implies:*

$$\max(|w|, |y|, x, q) < C,$$

where C is an effectively computable constant depending only on A, B, k and S .

Theorem 2. *Let R be a non-degenerate Lucas sequence. Then the equation $|R_x| = |R_y|$ has no solutions in non-negative integers x, y with $x \neq y$ and $\min(x, y) > e^{398}$.*

2. Auxiliary results and lemmas

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

Theorem A. Let $F(z, t) \in Q[z, t]$ be a binary form with $F(1, 0) \neq 0$ such that among the linear factors in the linearisation of F at least two are distinct. Let d be a positive integer. Then the equation

$$F(z, t) = wy^q$$

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

$$\max(|w|, |t|, |y|, |z|, q) < C$$

where C is an effectively computable constant depending only on F , d and S .

This theorem is due to T. N. SHOREY, A. VAN DER POORTEN R. TIJDEMAN and A. SCHINZEL [10].

Theorem B. Let α be an algebraic number of height at most $H (\geq 4)$ and degree d . Let b_1 and b_2 be integers with absolute values at most $M (\geq 4)$. If

$$A = b_1 \log(-1) + b_2 \log \alpha \neq 0$$

then

$$|A| > \exp(-c \log H \log M)$$

for $c = 2^{435} \cdot (3d)^{49}$.

This was proved by C. L. STEWART [14].

Lemma 1. Let $R = R(A, B)$ be a non-degenerate Lucas sequence with condition $D = A^2 - 4B < 0$. Then $B \geq 2$ and

$$|R_n| > B^{n/4} \quad \text{for } n > e^{398}.$$

PROOF. Since $R(A, B)$ is non-degenerate Lucas sequence, we have $A^2 \neq B, 2B, 3B, 4B$. Thus if $D = A^2 - 4B < 0$, then $B \geq 2$.

Let α and β be roots of $x^2 - Ax + B = 0$. By our condition we obtain

$$(7) \quad |\alpha| = |\beta| = \sqrt[4]{B}.$$

By (6) we have

$$(8) \quad \begin{aligned} |R_n| &= \left| \frac{\alpha^n - \beta^n}{\sqrt[4]{D}} \right| = \frac{|\alpha|^n}{\sqrt[4]{|D|}} \left| 1 - \left(\frac{\beta}{\alpha} \right)^n \right| \cong \\ &\cong \frac{|\alpha|^n}{2 \sqrt[4]{|D|}} \left| t \log(-1) - n \log \frac{\beta}{\alpha} \right|, \end{aligned}$$

where $\log$ denotes the principal value of the logarithm function and $|t| \leq 2n$, because $\left| 1 - \left(\frac{\beta}{\alpha} \right)^n \right|$ is the length of a chord of unit circle which is greater than the half of the smaller circular arc. Set

$$A = t \log(-1) - n \log \frac{\beta}{\alpha}.$$

Since β/α is not a root of unity, we have $A \neq 0$. Now apply the Theorem B to A . It is easily seen that in our case $H=2B$, $M=2n$ and $d=2$. Thus for $n \geq 2$ we get

$$(9) \quad |A| > \exp \{-2^{484} \cdot 3^{49} \log 2B \cdot \log 2n\} \\ \cong \exp \{-2^{485} \cdot 3^{49} \log B \cdot \log 2n\} = B^{-2^{485} \cdot 3^{49} \cdot \log 2n}$$

On the other hand it follows from $0 < A^2 < 4B$ that

$$|D| \leq |A^2 - 2B| + |2B| \leq 2B + 2B = 4B$$

and so

$$(10) \quad \frac{1}{2\sqrt{|D|}} > \frac{1}{4\sqrt{B}} \cong B^{-5/2},$$

Thus by (7), (8), (9) and (10) we obtain

$$|R_n| > B^{(n/2 - 2^{485} \cdot 3^{49} \log 2n - 5/2)}$$

and so $|R_n| > B^{n/4}$ if $n > e^{398}$. $\square$

Lemma 2. Let $T = \{T_m(x, y)\}_{m=0}^\infty$ be a second order recurrence sequence defined by the initial terms $T_0=1$, $T_1=x+y$ and by the recursion

$$T_m = xT_{m-1} - y^2T_{m-2}.$$

Then for any integer $m \geq 2$

$$T_m(x, y) = x^m + x^{m-1}y - (m-1)x^{m-2}y^2 - \dots$$

is a binary form such that among the linear factors in the factorisation of $T_m(x, y)$ at least two are distinct.

PROOF. Let $R=R(x, y^2)$ be Lucas sequence defined by parameters $A=x$ and $B=y^2$. It is well known that

$$(11) \quad T_m = T_1 R_m - y^2 T_0 R_{m-1}$$

for any $m \geq 1$. On the other hand we have

$$(12) \quad R_m(A, B) = \sum_{i=0}^{[(m-1)/2]} \binom{m-1-i}{i} A^{m-1-2i} \cdot (-B)^i$$

and so by (11) and (12) we get

$$(13) \quad T_m = (x+y)R_m - y^2 R_{m-1} = (xR_m - y^2 R_{m-1}) + yR_m = R_{m+1} + yR_m = \\ = \sum_{i=0}^{[m/2]} \binom{m-i}{i} x^{m-2i} (-y^2)^i + y \sum_{j=0}^{[(m-1)/2]} \binom{m-1-j}{j} x^{m-1-2j} (-y^2)^j = \\ = \sum_{i=0}^{[m/2]} (-1)^i \binom{m-i}{i} x^{m-2i} y^{2i} + \sum_{j=0}^{[(m-1)/2]} (-1)^j \binom{m-1-j}{j} x^{m-(2j+1)} y^{2j+1} = \\ = x^m + x^{m-1}y - (m-1)x^{m-2}y^2 - \dots,$$

from which it follows that $T_m(x, y)$ is a binary form. Suppose that $T_m(x, 1) = (x-\alpha)^m$.

Then by (13)

$$-m\alpha = 1 \quad \text{and} \quad \frac{m(m-1)}{2} \alpha^2 = -(m-1)$$

follow. From these $\alpha=2$ and $m=-1/2$ follow, which is a contradiction since m is an integer. $\square$

Lemma 3. Let $H=H(A, B)=\{H_n\}_{n=0}^\infty$ be a second order recurrence sequence defined by the initial terms $H_0=2$, $H_1=A$ and by the recursion

$$H_n = AH_{n-1} - BH_{n-2} \quad (n > 1).$$

If $(A, B)=1$, then $(H_n, B)=1$ for any $n>0$.

PROOF. By the recursion we have

$$(H_n, B) = (H_{n-1}, B) = \dots = (H_1, B) = (A, B) = 1. \quad \square$$

3. Proofs of theorems

PROOF OF THEOREM 1.

In the following $c_1, c_2, \dots$ will denote effectively computable constants depending only on A, B, k and S .

Suppose that the integers $w \in S$, $q \geq 3$, $x, |y| > 1$ are solutions of

$$U_x(k) = \frac{R_{kx}}{R_x} = wy^q.$$

Let S_1 be the set of non-zero integers which are composed of prime divisors of B . Put $S_0 = S \cup S_1$.

First suppose that $k=2m+1$ ($m \geq 0$ is integer). If $m=1$ then, using the explicit form

$$(14) \quad H_n = \alpha^n + \beta^n$$

for the terms of the sequence H defined in Lemma 3, we get

$$(15) \quad wy^q = U_x(k) = U_x(3) = (\alpha^x + \beta^x)^2 - B^x = H_x^2 - B^x =$$

$$= \begin{cases} F_1(z, t) = z^2 - t^2 & \text{if } x \text{ even} \\ F_2(z, t) = z^2 - Bt^2 & \text{if } x \text{ odd,} \end{cases}$$

with $n = \left\lfloor \frac{x}{2} \right\rfloor$, $t = B^n$, $z = H_x$. 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 that $(z, t) = 1$ by Lemma 3.

It follows from Theorem A, that there exists an effectively computable constant c_1 depending only on F_1, F_2 and S_0 such that for any integer solution $t \in S_0$, $w \in S_0$, $|y| > 1$, $q \geq 3$, z of (15)

$$\max(|w|, |t|, |y|, |z|, q) < c_1$$

is satisfied. But F_1, F_2, S_0 therefore c_1 also depend only on A, B and S . Thus

$$|z| = |H_x| < c_1$$

from which $x < c_2$ follows. Thus in this case the Theorem is proved with $c = \max(c_1, c_2)$.

Now we suppose that $m \geq 2$. Let $z = H_{2x}$, $t = B^x$ and

$$T_v = U_x(2v+1) = \frac{R_{(2v+1)x}}{R_x} \quad (v = 0, 1, 2, \dots)$$

Using (6), (14) and the fact $B = \alpha\beta$, for $v > 1$ we have

$$T_v = H_{2x}T_{v-1} - B^{2x}T_{v-2} = zT_{v-1} - t^2T_{v-2}$$

and $T_0 = 1$, $T_1 = U_x(3) = H_{2x} + B^x = z + t$. Thus

$$T_m = U_x(2m+1) = U_x(k) = wy^q$$

from which using Lemma 2 and Theorem A we get

$$\max(|w|, |t|, |y|, |z|, q) < c_3$$

where c_3 depend only on $A, B, T_m(z, t)$ and S_0 . But $T_m(z, t)$ and S_0 depend only on k, B and S .

Because $|z| = |H_{2x}| < c_3$, hence $x < c_4$ and

$$\max(|w|, |y|, x, q) < \max(c_3, c_4).$$

Now let $k = 2m$. If $m = 1$, then according to

$$U_x(k) = U_x(2) = H_x = wy^q$$

we have

$$\max(|w|, |y|, x, q) < c_5$$

because $\{H_n\}_{n=0}^\infty$ is a second order recurrence sequence.

Let $m \geq 2$. Then

$$U_x(k) = U_x(2m) = \frac{R_{2mx}}{R_x} = H_{mx} \frac{R_{mx}}{R_x} = wy^q.$$

It is known that $(H_v, R_v) = 1$ or 2 , hence $H_{mx} = w_1 y_1^q$, where $w_1 \in S_0$, x, y_1 are integers. Hence forth

$$\max(|w_1|, |y_1|, mx, q) < c_6$$

follows and so $|wy^q| < c_7$, consequently

$$\max(|w|, |y|, x, q) < c_8. \quad \square$$

PROOF OF THEOREM 2.

Denote $r = r(m)$ the smallest natural number for which $m | R_r$.

First we prove that $r(R_n) = n$ if $n > e^{398}$. Let $r(R_n) = m$, where $n > e^{398}$. Then $m | n$ i.e. $n = tm$, hence $R_n | R_m$ and $R_m | R_n$ i.e. $|R_n| = |R_m|$.

If $D > 0$, then from the result of M. WARD [15] it follows that $r(R_n) = n$ for $n > 12$. Thus if $|R_x| = |R_y|$, where $\min(x, y) > 12$, then $x = r(|R_x|) = r(|R_y|) = y$.

If $D < 0$, then $|D| \geq 4$, because for $D = -1, -2, -3$ we get contradiction. Applying Lemma 1 and the fact $B = |\alpha|^2$ we get

$$|\alpha|^{n/2} < |R_n| \leq |R_m| < \frac{2|\alpha|^m}{\sqrt{|D|}} \leq |\alpha|^m,$$

i.e. $\frac{n}{2} < m$, hence $n = m$.

If $(R_x) = (R_y)$ where $\min(x, y) > e^{398}$ then using our considerations above it follows

$$x = r(R_x) = r(R_y) = y. \quad \square$$

References

- [1] F. BEUKERS, The multiplicity of binary recurrences, *Comp. Math.* **40** (1980), 251—267.
- [2] K. GYÖRY, On some arithmetical properties of Lucas and Lehmer numbers, *Acta Arith.* **40** (1982), 369—373.
- [3] K. GYÖRY, P. KISS and A. SCHINZEL, On Lucas and Lehmer sequences and their applications to Diophantine equations, *Colloq. Math.* **45** (1981), 75—80.
- [4] P. KISS, Differences of the terms of linear recurrences, *Studia Sci. Math. Hung.*, (to appear).
- [5] K. K. KUBOTA, On a conjecture of Motgan Ward I, II., *Acta Arith.* **33** (1977), 11—48.
- [6] D. J. LEWIS, Diophantine equation: p -adic methods, Studies in number theory 6, ed. W. J. Leveque, Englewood Cliffs, New Jersey, 1969.
- [7] I. NEMES and A. PETHŐ, Polynomial values in linear recurrences, *Publ. Math. (Debrecen)* **31** (1984), 229—233.
- [8] J. C. PARNAMI and T. N. SHOREY, Subsequences of binary recursive sequences, *Acta Arith.* **40** (1982), 193—196.
- [9] A. PETHŐ, Perfect powers in second order linear recurrences, *J. of Number Theory* **15** (1982), 5—13.
- [10] T. N. SHOREY, A. VAN DER POORTEN, R. TIJDEMAN and A. SCHINZEL, Applications of the Gelfond Baker method to Diophantine equations, Transcendence Theory: Advances and Applications, *Academic Press, New York*, 1977.
- [11] 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, *Math. Second.* **52** (1983), 24—36.
- [12] T. N. SHOREY and C. L. STEWART, Pure powers in recurrence sequences and some related Diophantine equations, (to appear).
- [13] L. SOMER, The generation of higher — order linear recurrences from second — order linear recurrences, *Fibonacci Quart.* **22** (1984), 98—100.
- [14] C. L. STEWART, Primitive divisors of Lucas and Lehmer numbers, Transcendence Theory: Advances and Applications, *Academic Press, New York*, 1977.
- [15] M. WARD, The intrinsic divisors of Lehmer numbers, *Ann. of Math. (2)*, **62** (1955), 230—236.

I. JOÓ AND B. M. PHONG
MATHEMATICAL INSTITUT
EÖTVÖS LORÁND UNIVERSITY
H—1445 BUDAPEST 8, PF. 323,
HUNGARY

(Received Jun: 8, 1986)