ACTA ARITHMETICA
133.1 (2008)

Diophantine equations with products of consecutive terms in Lucas sequences II

by

FLORIAN LUCA (Morelia) and T. N. SHOREY (Mumbai)

To Wolfgang Schmidt at his seventy-fifth birthday

1. Introduction. Let r and s be nonzero integers such that $\Delta = r^2 + 4s \neq 0$ and let α, β be the two roots of the quadratic equation $x^2-rx-s=0$. We assume further that α/β is not a root of 1. Let $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be the Lucas sequences of the first and second kind with roots α and β, given by $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ and $v_n = \alpha^n + \beta^n$ for all $n \geq 0$, respectively. These sequences can also be defined by $u_0 = 0$, $u_1 = 1$, $v_0 = 2$, $v_1 = r$ and the recurrence relations $u_{n+2} = ru_{n+1} + su_n$ and $v_{n+2} = rv_{n+1} + sv_n$ for all $n \geq 0$. When $r = s = 1$, the resulting sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ are the sequences of Fibonacci numbers $(F_n)_{n\geq 0}$ and Lucas numbers $(L_n)_{n\geq 0}$, and when $r = 3$, $s = -2$, the resulting sequence $u_n = 2^n - 1$ for $n \geq 0$ is the sequence of Mersenne numbers.

In [7], we investigated Diophantine equations of the form

$$\prod_{i=1}^{k} u_{n+i} = by^m, \tag{1}$$

in integers $k > 1$, $n \geq 0$, $|y| > 1$, $m > 1$ and b such that $P(b) \leq k$, where for an integer l we use $P(l)$ for the largest prime factor of l with the convention that $P(0) = P(\pm 1) = 1$, as well as the similar Diophantine equation where $(u_n)_{n\geq 0}$ is replaced by $(v_n)_{n\geq 0}$. The main result of [7] is that the above Diophantine equations have only finitely many effectively computable solutions. When $(u_n)_{n\geq 0}$ is the sequence of Fibonacci numbers, the above equation has no solutions when $b = 1$ and $n > 0$. A similar equation to (1) where the consecutive indices $n+i$ were replaced by arbitrary indices n_i for $i = 1, \ldots, k$, but with the additional restriction that m is a prime exceeding k was treated in [3].

2000 *Mathematics Subject Classification*: 11L07, 11N37, 11N60.

Key words and phrases: Lucas sequences, perfect powers.

In [2], Bilu, Kulkarni, and Sury investigated the Diophantine equation

$$x(x+1)\cdots(x+(k-1))+t=y^m \tag{2}$$

with a fixed *rational number* t and unknowns (x,k,y,m) with $x,k,m\in\mathbb{Z}$, $y\in\mathbb{Q}$, $|y|\neq 0,1$ and $\min\{k,m\}>1$, and showed that if t is not a perfect power of some other rational number, then (2) has only finitely many solutions, which are moreover effectively computable.

In this paper, we investigate an inhomogeneous analogue of equation (1), which is nothing else than equation (2) with the product of consecutive integers replaced by the product of consecutive members of a Lucas sequence of the first kind.

Theorem 1. *Let $(u_n)_{n\geq 0}$ be a Lucas sequence of the first kind, t be a fixed rational number, and assume that the equation*

$$u_nu_{n+1}\cdots u_{n+k-1}+t=y^m \tag{3}$$

holds with integers $n\geq 0$, $k\geq 1$, $m\geq 2$ and rational y, $|y|\neq 0,1$. Assume further that t is not a perfect power of some other rational number, that when t is written in reduced form its numerator is coprime to s, and that $\Delta>0$. Then equation (3) has only finitely many solutions (n,k,y,m). Both parameters k and m are effectively computable in terms of the sequence $(u_n)_{n\geq 0}$ and the number t. Moreover, if α and β are multiplicatively dependent, then n is also effectively computable in terms of $(u_n)_{n\geq 0}$ and t.

We do not know how to prove an analogue of Theorem 1 with $(u_n)_{n\geq 0}$ replaced by $(v_n)_{n\geq 0}$. However, in order for a result like Theorem 1 to be valid for $(v_n)_{n\geq 0}$, one also needs to eliminate the numbers $t=\pm 2$, as can be seen from the example

$$L_{2n}+2(-1)^n=L_n^2,$$

which holds for $n\geq 0$.

In particular, Theorem 1 shows that if t is a rational number which is not a perfect power of some other rational number, then the equation

$$F_nF_{n+1}\cdots F_{n+k-1}+t=y^m$$

has only finitely many effectively computable integer solutions (n,k,y,m) with $n\geq 0$, $k\geq 1$, $m\geq 2$ and $|y|>1$, and that if t is an odd integer which is not a perfect power, then the equation

$$(2^n-1)(2^{n+1}-1)\cdots(2^{n+k}-1)+t=y^m \tag{4}$$

has only finitely many effectively computable integer solutions (n,k,y,m) with $n\geq 0$, $k\geq 1$, $|y|>1$ and $m\geq 2$. Indeed, these consequences follow from the fact that for the Fibonacci sequence one has $\beta=-\alpha^{-1}$, while for $u_n=2^n-1$ for all $n\geq 0$ one has $\alpha^0=1=\beta^1$, and therefore in both cases α and β are multiplicatively dependent; hence, according to Theorem 1, all solutions are effectively computable. In (4), the assumption that t is odd is not required if m exceeds a sufficiently large effectively computable number depending only on t. This follows from the theory of linear forms in logarithms.

The above restrictions on t not being a perfect power of some rational number are essential in order to guarantee finiteness of the number of solutions, as can be seen from the examples

$$F_{2n}F_{2(n+1)}+1=F_{2n+1}^2 \tag{5}$$

and

$$F_{2n}F_{2n+1}F_{2n+2}F_{2n+3}+\frac{1}{4}=\left(\frac{2L_{4n+3}-3}{10}\right)^2, \tag{6}$$

which both hold for all $n\ge 0$.

Acknowledgements. We thank the referee for a careful reading of the manuscript and for many useful suggestions. Work on this paper started during a visit of F. L. to the Tata Institute in Mumbai with an Associateship from the TWAS in the Fall of 2005. This author thanks these institutions for their hospitality and support.

2. The proof of Theorem 1.

The line of attack here is as follows. We first show that k is bounded in an effective way. We then show that m is bounded in an effective way as well. Finally, we show that with k and m fixed, the number n can assume only finitely many values, which are furthermore effectively computable when α and β are multiplicatively dependent. We begin by noticing that $n>0$ because t is not a perfect power and there is no loss of generality in assuming that m is a prime, which we assume from now onwards. Also, we always assume that $|\alpha|\ge|\beta|$.

STEP 1. *k is bounded.*

Assume first that t is an integer. Then so is y. Since t is not a perfect power, we conclude that $|t|>1$ and further either $-t$ is a perfect square, or the greatest common divisor of all the numbers $\mathrm{ord}_p(t)$ with $p\,|\,t$ is 1. Here, $\mathrm{ord}_p(t)$ is the exponent at which p appears in the prime factorization of t. Assume first that $-t$ is not a perfect square. Then there exists a prime p dividing t such that

$$\mathrm{ord}_p(y^m-t)\le \mathrm{ord}_p(t),$$

and the assertion follows from (3) and the fact that $\gcd(p,s)=1$. So, it remains to consider the case when $t=-a^2$ with some positive integer a which is not a perfect power of odd exponent >1 of some other positive integer. Now we argue as above to conclude that $m=2$. Therefore, we see from (3) that all the prime divisors larger than a of $u_nu_{n+1}\cdots u_{n+k-1}$ are congruent to 1 modulo 4, which implies that k is bounded since there are infinitely many primes congruent to 3 modulo 4.

Assume now that t is not an integer. Then we write $t = a/b$, where $a, b > 1$ are integers and $\gcd(a, b) = 1$. We multiply both sides of equation (3) by b and we observe that $\mathrm{ord}_p(by^m) = 0$ for every prime divisor p of b. Therefore $b = b_1^m$, where $b_1 > 1$ is an integer. Now we argue as above for the equation

$$bu_n u_{n+1} \cdots u_{n+k-1} + a = (b_1 y)^m$$

to conclude that k is bounded. ■

Step 2. *m is bounded.*

Here, we assume that k is fixed. The fact that $\Delta > 0$ implies that α and β are both real and so $|\alpha| > |\beta|$. Write $t = a/b$, where a and b are coprime integers with b positive. Then

$$w_n = bu_n u_{n+1} \cdots u_{n+k-1} + a \quad \text{for } n \geq 0 \tag{7}$$

is a linearly recurrent sequence of order either $k+1$ or $k+2$, all of whose roots are simple and are precisely $\{\alpha^{k-i}\beta^i : i = 0, 1, \ldots, k\} \cup \{1\}$. Clearly,

$$|\alpha|^k > \max\{1, |\alpha|^{k-i}|\beta|^i : i = 1, \ldots, k\}. \tag{8}$$

Furthermore,

$$w_n = \gamma_1(\alpha^k)^n + \sum_{i=1}^{k} \gamma_{i+1}(\alpha^{k-i}\beta^i)^n + \gamma_{k+2}$$

with some coefficients $\gamma_1, \ldots, \gamma_{k+2}$, where

$$\gamma_1 = \frac{b\alpha^{k(k-1)/2}}{(\alpha - \beta)^k} \neq 0. \tag{9}$$

In particular, the linearly recurrent sequence $(w_n)_{n \geq 0}$ has a *dominant root* which is precisely α^k. Now the assertion follows from a result of [8] applied to the equation $w_n = by^m = y_1^m$, where y_1 is an integer. ■

Step 3. *α and β are multiplicatively independent.*

We suppose that both $k \geq 1$ and $m \geq 2$ are fixed. All we want to prove in this case is that equation (13) below has only finitely many solutions n. We return to the sequence $(w_n)_{n \geq 0}$ given by (7) and write it as

$$w_n = b \prod_{i=0}^{k-1} \left(\frac{\alpha^i \alpha^n - \beta^i \beta^n}{\alpha - \beta} \right) + a,$$

or, equivalently,

$$w_n = \gamma_1 \alpha_1^n + \gamma_2 \alpha_2^n + \cdots + \gamma_{k+2} \alpha_{k+2}^n, \tag{10}$$

where $\gamma_i \in \mathbb{K} = \mathbb{Q}(\alpha)$, and

$$\alpha_i = \begin{cases} \alpha^{k-(i-1)}\beta^{i-1} & \text{for } i \in \{1, \dots, k+1\}, \\ 1 & \text{for } i = k+2. \end{cases} \tag{11}$$

We observe that none of α_i with $1 \le i \le k+1$ is 1 since α and β are multiplicatively independent and

$$|\alpha|^k > |\alpha_i| > |\beta|^k$$

for all $i \in \{2, \dots, k\}$. Further,

$$\gamma_1 = \frac{b\alpha^{k(k-1)/2}}{(\alpha-\beta)^k}, \qquad \gamma_{k+1} = (-1)^k \frac{b\beta^{k(k-1)/2}}{(\alpha-\beta)^k} \quad \text{and} \quad \gamma_{k+2} = a \tag{12}$$

are all nonzero. Should equation (3) have infinitely many nonnegative integer solutions n, it would follow that for infinitely many n there exists an integer $y = y(n)$ such that

$$w_n = y^m. \tag{13}$$

To see that this is impossible, we use the following extension of Fuchs [6] of a result of Corvaja and Zannier [4].

Theorem 2. *Let $(G_n)_{n\ge0}$ be a linearly recurrent sequence of integers of the form*

$$G_n = \gamma_1\alpha_1^n + \gamma_2\alpha_2^n + \cdots + \gamma_s\alpha_s^n \qquad \textit{for } n \ge 0, \tag{14}$$

where the α_i are algebraic integers for all $i = 1, \dots, s$, the ratios α_i/α_j are not roots of unity for any $i \ne j$, and the γ_i are nonzero algebraic numbers belonging to the field $\mathbb{K} = \mathbb{Q}(\alpha_1, \dots, \alpha_s)$. Assume further that $1 \ne |\alpha_1| > \max\{|\alpha_i| : i = 2, \dots, s\}$. Let $q \ge 2$ be any fixed prime number and assume that for infinitely many n there exists an integer y such that

$$G_n = y^q.$$

Then there exist an integer $t \ge 1$, algebraic numbers $\beta_1, \dots, \beta_t$ in the multiplicative subgroup of $\mathbb{K}$ generated by $\{\alpha_i : i = 1, \dots, s\}$, some other algebraic numbers $\delta_1, \dots, \delta_t$ (not necessarily in $\mathbb{K}$), and two nonzero integers c and d, such that

$$G_{c+nd} = (\delta_1\beta_1^n + \cdots + \delta_t\beta_t^n)^q \tag{15}$$

for all nonnegative integers n.

The above theorem is basically Corollary 2 in [6]. In that paper, it is only stated that $\beta_1, \dots, \beta_t$ are *algebraic numbers*, but a close inspection of the proof of the main result in [6] shows that the β_j can be chosen to be of the form $\alpha_1^{\mu_{1j}} \cdots \alpha_s^{\mu_{sj}}$, where the exponents μ_{ij} are rational numbers of denominators dividing q. Now the assertion of Theorem 2 follows by considering $G_{c+n(qd)} = G_{c+(nq)d}$ for all nonnegative integers n in (15). Here, we replace β_j by β_j^q, and δ_j by $\delta_j\beta_j^c$. Hence, the β_j can indeed be chosen to be in the multiplicative subgroup of $\mathbb{K}$ generated by $\{\alpha_i : i = 1, \ldots, s\}$. Applying Theorem 2 above to the case in which equation (13) has infinitely many integer solutions (n, y_1), we find that there exist positive integers c and d such that

$$\sum_{i=1}^{k+2} \gamma_i'(\alpha_i')^n = \Big(\sum_{j=1}^{t} \delta_j \beta_j^n\Big)^m \tag{16}$$

identically for all nonnegative integers n, where $\gamma_i' = \gamma_i \alpha_i^c$ and $\alpha_i' = \alpha_i^d$ for all $i = 1, \ldots, k+2$, with some integer $t \geq 1$, algebraic numbers δ_j for $j = 1, \ldots, t$, and algebraic numbers β_j in the multiplicative subgroup of $\mathbb{K}$ generated by $\{\alpha, \beta\}$ for all $j = 1, \ldots, t$. By replacing n by $2n$ if needed, it follows that we may replace α and β by α^2 and β^2, respectively, and thus we may assume that $\alpha > \beta > 0$, and that $\beta_j > 0$ for all $j = 1, \ldots, t$. Now the positive real numbers $\alpha > \beta$ are multiplicatively independent, and therefore the functions $n \mapsto \alpha^n$ and $n \mapsto \beta^n$ are algebraically independent over $\mathbb{C}$. Thus, relation (16) implies that we may formally replace in it α^n by X and β^n by Y to obtain an equality of the form

$$\sum_{i=1}^{k+1} \gamma_i' X^{d(k-(j-1))} Y^{d(j-1)} + a = F(X, Y)^m$$

with some $F(X, Y)$ in $\overline{\mathbb{Q}}[X, Y, X^{-1}, Y^{-1}]$. Specifically, if

$$\beta_j = \alpha_1^{l_{1,j}} \cdots \alpha_{k+2}^{l_{k+2,j}} = \alpha^{\sum_{i=1}^{k+1} l_{i,j}(k-(j-1))} \beta^{\sum_{j=1}^{k+1} l_{i,j}(j-1)} = \alpha^{m_j} \beta^{n_j}$$

with some integers $l_{1,j}, \ldots, l_{k+2,j}$, then

$$F(X, Y) = \sum_{j=1}^{t} \delta_j X^{m_j} Y^{n_j}. \tag{17}$$

Thus, we have arrived at a relation of the form

$$\sum_{i=1}^{k+1} \gamma_i' X^{d(k-(j-1))} Y^{d(j-1)} + a = \Big(\sum_{j=1}^{t} \delta_j X^{m_j} Y^{n_j}\Big)^m \tag{18}$$

in $\overline{\mathbb{Q}}[X, Y, X^{-1}, Y^{-1}]$. Since the left hand side of (18) is a polynomial in X and Y, it follows that $F(X, Y)$ is a polynomial in X and Y as well.

To prove that (18) is impossible, we argue as follows. We notice that the left hand side of (18) is of the form $H_{dk}(X, Y) + a$, where $H_{dk}(X, Y)$ is a homogeneous polynomial in X and Y of degree $dk \geq 1$, and a is a nonzero constant. Evaluating (18) at $(X, Y) = (0, 0)$, we find that $F(0, 0) = \delta$ satisfies $\delta^m = a \neq 0$. Thus, $\delta \neq 0$. Let $d_1 \geq 1$ be the degree of F, and write

$$F(X, Y) = H_{d_1}(X, Y) + \cdots + H_{d_\mu}(X, Y) + \delta, \tag{19}$$

where $\mu \geq 1$, $0 < d_\mu < \cdots < d_1$, and $H_{d_i}(X,Y)$ is a nonzero homogeneous polynomial of degree d_i in X and Y for all $i = 1,\ldots,\mu$. Clearly, the representation (19) is unique. Comparing the degrees, we get $dk = d_1 m$. If $\mu \geq 2$, then

$$\begin{aligned} H_{dk}(X,Y) + a &= F(X,Y)^m \\ &= H_{d_1}(X,Y)^m + mH_{d_1}(X,Y)^{q-1}H_{d_2}(X,Y) \\ &\quad + \text{monomials of degree less than } (m-1)d_1 + d_2. \end{aligned} \tag{20}$$

This relation is impossible because the nonconstant polynomial $H_{dk}(X,Y) + a$ appearing on the left hand side of (20) does not contain monomials of positive degree $(m-1)d_1 + d_2 < d_1 m = dk$. If $\mu = 1$, we derive a contradiction similarly. Thus, equation (13) has only finitely many solutions (n,k,y,m) in this instance. ■

STEP 4. *α and β are multiplicatively dependent.*

Here, we shall distinguish two instances, according to whether α is rational or not.

CASE 1: $\alpha \in \mathbb{Q}$. Since α and β are algebraic integers, they are both integers. Moreover, since they are multiplicatively dependent, there exist an integer ϱ with $|\varrho| > 1$ and nonnegative coprime integers $e > f$ such that $\alpha = \varepsilon_1 \varrho^e$ and $\beta = \varepsilon_2 \varrho^f$, where $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$. As e and f are coprime, one of them is always odd. Thus, replacing ϱ by $-\varrho$ if necessary, we may assume that ε_1 or ε_2 is $+1$.

We split all the solutions of equation (13) into two classes, with n even or n odd. We shall show in detail that there are only finitely many solutions with n even and they are furthermore effectively computable. Up to some minor differences which we will point out, the arguments for n odd are entirely similar. For k fixed, consider the polynomial

$$P(X) = \frac{1}{(\alpha-\beta)^k} \prod_{i=0}^{k-1} (\alpha^i X^e - \beta^i X^f) + t. \tag{21}$$

Any solution of (13) will be a solution of the Diophantine equation

$$bP(\varrho^n) = by^m = y_1^m \tag{22}$$

with an integer y_1 such that $|y_1| > 1$, and a bounded prime number m.

Here is a criterion which is useful for us. Let $\mathbb{K}$ be an algebraic number field and $\mathcal{O}_\mathbb{K}$ its ring of integers. Let $P(X) \in \mathbb{K}[X]$ be nonconstant. Let $\delta_1,\ldots,\delta_\mu$ be all the distinct roots of P of respective multiplicities $\sigma_1,\ldots,\sigma_\mu$. Let $\phi \in \mathbb{K}$ be such that the greatest prime factor of $N_\mathbb{K}(\phi)$ is bounded.

CRITERION 1. *Let $\varrho \in \mathbb{K}$ be an algebraic number which is not a root of unity and $P(X) \in \mathbb{K}[X]$. Assume that the multiplicities of the nonzero roots* *of $P(X)$ are relatively prime. Then the Diophantine equation*

$$P(\varrho^n) = \phi y^m \tag{23}$$

has only finitely many effectively computable solutions (n, y, m) with $m \geq 2$, $n > 0$ and $y \in \mathcal{O}_{\mathbb{K}}$.

We shall use the above criterion only when m is bounded.

Proof. Write

$$P(X) = a_0 \prod_{i=1}^{\mu} (X - \delta_i)^{\sigma_i},$$

where $\delta_1, \ldots, \delta_\mu$ are the distinct roots of $P(X)$. Let $\mathbb{L} = \mathbb{K}(\delta_1, \ldots, \delta_\mu)$ be the splitting field of $P(X)$. Write d for the degree of P, and D for a positive integer which is divisible by the denominators of ϱ, of the roots $\delta_1, \ldots, \delta_\mu$ and of the leading term a_0 of $P(X)$. We write $\tau = \varrho D$ and $\gamma_i = \delta_i D$ for $i = 1, \ldots, \mu$.

Multiplying now equation (23) across by D^{n+d+1}, we get an equation which can be rewritten as

$$(Da_0) \prod_{i=1}^{\mu} (\tau^n - \gamma_i D^n)^{\sigma_i} = D^{n+d+1} \phi y^m. \tag{24}$$

Since the left hand side above is an algebraic integer, so is the right hand side. We may suppose that $\gamma_1 \neq 0$ and that $\gcd(\sigma_1, m) = 1$. Now we argue as in [1] to conclude that

$$\tau^n - \gamma_1 D^n = \eta_1 \lambda_1^m, \tag{25}$$

where n is a positive integer, λ_1 is an algebraic integer in $\mathbb{L}$ and η_1 is an algebraic number in $\mathbb{L}$ having both bounded denominator and largest prime factor of $N_{\mathbb{L}}(\eta_1)$. Since $\varrho = \tau/D$ is not a root of unity and $\gamma_1 \neq 0$, the left hand side of (25) is a binary recurrent sequence of algebraic integers in $\mathbb{L}$ which is nondegenerate. It follows from known results about perfect powers in nondegenerate binary recurrent sequences (see, for example, Corollary 9.2 in [8], or the book [9]), that (25) has only finitely many such solutions n and γ_1, which are, moreover, effectively computable. This completes the proof of the criterion. ∎

Remark. The above proof of Criterion 1 proves more, namely that if $\varrho \in \mathbb{K}$ is an algebraic number which is not a root of unity such that the equation $P(\varrho^n) = \phi y^m$ has infinitely many solutions (n, y, m) with $y \in \mathbb{K}$ and m prime, then for all but finitely many such solutions, m divides all the multiplicities of all the nonzero roots of $P(X)$. We shall use this formulation in what follows.

We use Criterion 1 to infer that (22) has only finitely many solutions. Assume first that 0 is not a root of P. In this case, by the criterion, (22) has only finitely many solutions except when m is a prime number dividing the multiplicities of all the roots of P. Then there must exist a nonzero rational number c and a monic polynomial F with rational coefficients such that $P(X) = cF(X)^m$. We now show that c is not an mth power of a rational number. Indeed, if $f > 0$, then $P(0) = t = cF(0)^m$, and since $t \neq 0$ is not an mth power of a rational number, we infer that $F(0) \neq 0$, and c is not an mth power of a rational number either. If $f = 0$, then $e = 1$ and we may assume that $\alpha = \varrho$. In this case, $P(1) = t = cF(1)^m$. Since $t \neq 0$ is not an mth power of a rational number, we find again that neither is c.

We now show that (22) has no solutions when $|\varrho|^n > \max\{\delta_i : i = 1, \ldots, \mu\}$. Indeed, if it had such a solution, we would get an equation of the form

$$cF(\varrho^n)^m = y^m$$

with some rational number y. Since the roots of F are the same as the roots of P, and since n is large, we infer that $F(\varrho^n) \neq 0$. In particular, $c = (y/F(\varrho^n))^m$ is an mth power of a rational number, which we have seen to be impossible.

Thus, we are left with the case where 0 is a root of P. In this case, $f = 0$, and therefore $e = 1$, $\alpha = \varrho$ and $\beta = \pm 1$. Moreover, since $P(0) = 0$, we get

$$t = -\frac{(-1)^k \beta^{k(k-1)/2}}{(\alpha - \beta)^k}. \tag{26}$$

We now show that 0 is a simple root of P, and that P has no triple roots. Indeed, the first fact comes from the observation that the coefficient of the monomial X in $P(X)$ is precisely

$$\frac{(-1)^{k-1}\beta^{k(k-1)/2}}{(\alpha-\beta)^k} \sum_{i=0}^{k-1} \left(\frac{\alpha}{\beta}\right)^i = \frac{(-1)^{k-1}\beta^{(k-1)(k-2)/2}}{(\alpha-\beta)^{k+1}} (\alpha^k - \beta^k),$$

and this is nonzero because $\alpha/\beta = \pm\varrho$ is not a root of unity. Now observe that $P(X)$ assumes the value t at the points $(\beta/\alpha)^i$ with $i = 0, 1, \ldots, k-1$, which are all real and distinct. We apply Rolle's theorem at these points to conclude that the roots of $P'(X)$ are simple. Thus, P has no triple root. We shall use this argument several times in this paper.

Since we already know that 0 is a simple root and $P(X)$ has no triple roots, it follows that all the nonzero roots of $P(X)$ are either simple or double. If one of them is simple, then we are in the hypothesis of Criterion 1, so (13) has only finitely many effectively computable solutions (m, n) with n even. The case of n odd can be handled similarly. Assume now that all the nonzero roots of $P(X)$ are double. Then k must be odd. But then (26) yields

$$t = \left(\frac{\beta^{(k-1)/2}}{\alpha - \beta}\right)^k.$$

Thus, t is a perfect power of a rational number when $k > 1$. We are therefore left with the case of $k = 1$, so $t = 1/(\alpha - \beta)$, and

$$u_n + t = \frac{\alpha^n + (1 - \beta^n)}{\alpha - \beta}. \tag{27}$$

If n is even, or n is odd and $\beta = 1$, we get

$$u_n + t = \frac{\alpha^n}{\alpha - \beta}.$$

Assume now that the equation

$$\frac{\alpha^n}{\alpha - \beta} = y^m \tag{28}$$

admits a solution (n, m, y) with $n \geq 2$ and y a rational number. Notice that $|\alpha|^n = |\varrho|^n > |\varrho| + 1 \geq |\alpha - \beta|$, because $|\varrho| > 1$ is an integer. Assume first that m is odd. Since α^n and $|\alpha - \beta| = \alpha \pm 1$ are coprime, it follows that $\alpha - \beta$ is an mth power of an integer since m is odd. In particular, t is an mth power of a rational number, which is impossible. Assume next that $m = 2$. Then either both α^n and $\alpha - \beta$ or both $-\alpha^n$ and $-(\alpha - \beta)$ are perfect squares. The first instance implies again that t is the square of a rational number, which is impossible, while the second implies that n is odd, $-\alpha = a_1^2$ is a perfect square, and so is $a_1^2 \pm 1 = -\alpha + \beta = a_2^2$. However, the only integer solutions (a_1, a_2) of the equation $a_1^2 \pm 1 = a_2^2$ have $|a_1| \leq 1$, so $|\varrho| = |\alpha| \leq 1$, which is impossible. This takes care of the case when n is even, or when n is odd but $\beta = 1$. Finally, when n is odd and $\beta = -1$, equation (27) becomes

$$\frac{\alpha^n + 2}{\alpha + 1} = y^m.$$

Since n is odd, $\alpha + 1 \mid (\alpha^n + 1)$, and therefore $\alpha + 1$ and $\alpha^n + 2$ are coprime. Since their ratio is an mth power of a rational number, we deduce that $\alpha + 1$ is an mth power of an integer, so, in particular, t is an mth power of a rational number, which is a contradiction.

The case $\alpha \in \mathbb{Q}$ is therefore settled. ■

Case 2: $\alpha \notin \mathbb{Q}$. Let $\mathbb{K} = \mathbb{Q}(\alpha)$. Then $[\mathbb{K} : \mathbb{Q}] = 2$. Since α and β are multiplicatively dependent, there exist integers $i > 0$ and j such that $\alpha^i = \beta^j$. Conjugating this relation by the only nontrivial Galois automorphism of $\mathbb{K}$, we also get $\beta^i = \alpha^j$. Thus,

$$\beta^{i^2} = (\beta^i)^i = (\alpha^j)^i = \alpha^{ij} = (\alpha^i)^j = (\beta^j)^j = \beta^{j^2},$$

and therefore

$$\beta^{i^2 - j^2} = 1.$$

Since β is not a root of unity (otherwise, so is α, and therefore also α/β, which is impossible), we must have $i^2 = j^2$, so $i = j$ or $i = -j$. The case

$i = j$ leads to $(\alpha/\beta)^i = 1$, which is impossible. The case $i = -j$ gives $(\alpha\beta)^i = 1$, implying $\beta = \zeta\alpha^{-1}$, where $\zeta \in \{\pm 1\}$.

In particular, $s = -\zeta = \pm 1$. Since $\Delta = r^2 + 4s = r^2 \pm 4$ and $r\Delta \neq 0$, we get $\Delta > 0$, and therefore $\mathbb{K}$ is a real quadratic field.

We shall write $R(X)$ for the element of $\mathbb{K}[X, X^{-1}]$ given by

$$R(X) = \frac{1}{(\alpha - \beta)^k} \prod_{i=0}^{k-1} \left(\alpha^i X - \frac{\zeta^n \beta^i}{X} \right) + t = c\,\frac{P_1(X)}{X^k}, \tag{29}$$

where

$$c = \frac{\alpha^{k(k-1)/2}}{(\alpha - \beta)^k}, \tag{30}$$

and $P_1(X)$ is the monic polynomial in $\mathbb{K}[X]$ given by

$$P_1(X) = \prod_{i=0}^{k-1} (X^2 - \zeta^n \varrho^i) + t_1 X^k, \tag{31}$$

with

$$\varrho = \frac{\beta}{\alpha} = \frac{\zeta}{\alpha^2} \quad \text{and} \quad t_1 = \frac{t}{c} = t\,\frac{(\alpha - \beta)^k}{\alpha^{k(k-1)/2}}. \tag{32}$$

Any solution (n, y) of equation (13) leads to a solution of the equation

$$y^m = R(x) = c\,\frac{P_1(x)}{x^k}$$

with $x = \alpha^n$, and therefore of the equation

$$P_1(\alpha^n) = \frac{\alpha^{nk}}{c}\, y^m \tag{33}$$

with some rational number y with $|y| \neq 0, 1$, which has a bounded denominator. Since α is a unit in $\mathbb{K}$ (but not a root of unity), it follows that we may apply Criterion 1 to conclude that equation (33) has only finitely many effectively computable solutions (n, y), provided that the polynomial $P_1(X)$ satisfies, of course, the conditions from that criterion.

From now on, we focus on proving that $P_1(X)$ satisfies the conditions from Criterion 1. We assume that this is not the case. Clearly, 0 is not a root of $P_1(X)$, because the constant term of $P_1(X)$ is $(-1)^k \varrho^{k(k-1)/2} \neq 0$. By the Remark following the proof of Criterion 1, it follows that we may assume that (33) has infinitely many solutions (n, y, m), where m is a prime dividing all the multiplicities of all the nonzero roots of $P_1(X)$.

To ensure first that $P_1(X)$ has a sufficiently large degree, we shall start by treating separately the cases in which $k \in \{1, 2\}$.

Subcase 2.1: $k = 1$. In this case, we have $P_1(X) = X^2 + t_1 X - \zeta^n$, whose discriminant is $\Delta_1 = t_1^2 + 4\zeta^n = 0$ implying $t_1^2 = -4\zeta^n$, n is odd,

$\zeta = -1$, $t_1 = \pm 2$, and $t = ct_1 = \pm 2/(\alpha - \beta) = \pm 2/\sqrt{r^2+4}$, which is impossible since $t \in \mathbb{Q}$. ∎

Subcase 2.2: $k = 2$. In this case,

$$P_1(X) = (X^2 - \zeta^n)(X^2 - \zeta^n \varrho) + t_1 X^2 = X^4 - (\zeta^n + \zeta^n \varrho - t_1)X^2 + \varrho. \tag{34}$$

The degree of $P_1(X)$ is four and 0 is not a root of $P_1(X)$. Since all the roots of $P_1(X)$ are multiple, we get $m = 2$. Equation (3) now implies that $\alpha > 0$ since if $\alpha < 0$, then

$$u_n u_{n+1} + t < 0$$

for all sufficiently large n, so this expression cannot be a perfect square. Further, $P_1(X)$ has a double root if and only if

$$(\zeta^n + \zeta^n \varrho - t_1)^2 = 4\varrho = 4\zeta/\alpha^2,$$

implying $\zeta = 1$ and $t = 1/(r - 2\varepsilon)$, where $\varepsilon \in \{\pm 1\}$.

Returning to our original problem, we get

$$\begin{aligned} u_n u_{n+1} + t &= \frac{(\alpha^n - 1/\alpha^n)(\alpha^{n+1} - 1/\alpha^{n+1})}{r^2 - 4} + \frac{1}{r - 2\varepsilon} \\ &= \frac{1}{r^2-4}\left(\alpha^{2n+1} + \frac{1}{\alpha^{2n+1}} - \left(\alpha + \frac{1}{\alpha}\right) + r + 2\varepsilon\right) \\ &= \frac{1}{r^2-4}\left(\alpha^{2n+1} + \frac{1}{\alpha^{2n+1}} + 2\varepsilon\right) \\ &= \frac{1}{r^2-4}\left((\sqrt{\alpha})^{2n+1} + \left(\frac{\varepsilon}{\sqrt{\alpha}}\right)^{2n+1}\right)^2. \end{aligned} \tag{35}$$

Let $\alpha_1 = \sqrt{\alpha}$. If the equation (13) has at least one solution (n, y) with an integer $n \ge 0$ and a rational number y, then

$$(\sqrt{\alpha})^{2n+1} + \left(\frac{\varepsilon}{\sqrt{\alpha}}\right)^{2n+1} = \pm y\sqrt{r^2-4} \in \mathbb{K}, \tag{36}$$

and since $\alpha_1^2 = \alpha \in \mathbb{K}$, we deduce that $\alpha_1^{2n+1} \in \mathbb{K}$, so $\alpha_1 \in \mathbb{K}$. Let β_1 be the conjugate of $\alpha_1 \in \mathbb{K}$. If $\beta_1 = \varepsilon/\alpha_1$, it follows that

$$(\sqrt{\alpha})^{2n+1} + \left(\frac{\varepsilon}{\sqrt{\alpha}}\right)^{2n+1} = \alpha_1^{2n+1} + \beta_1^{2n+1} \in \mathbb{Z}, \tag{37}$$

because this is the $(2n+1)$th member of the Lucas sequence of the second kind $(v_m)_{m \ge 0}$ with roots α_1 and β_1. Now (36) and (37) together imply that $\sqrt{r^2-4} \in \mathbb{Q}$, which is impossible. Thus, $\beta_1 = -\varepsilon/\alpha_1$, and therefore

$$\begin{aligned} u_n u_{n+1} + t &= \frac{1}{r^2-4}\,(\alpha_1^{2n+1} - \beta_1^{2n+1})^2 \\ &= \frac{(\alpha_1 - \beta_1)^2}{r^2-4}\left(\frac{\alpha_1^{2n+1} - \beta_1^{2n+1}}{\alpha_1 - \beta_1}\right)^2. \end{aligned} \tag{38}$$

We now observe that the number $(\alpha_1^{2n+1} - \beta_1^{2n+1})/(\alpha_1 - \beta_1)$ appearing on the right hand side of (38) is an integer (it is the $(2n+1)$th member of the Lucas sequence of the first kind with roots α_1 and β_1), and therefore $(\alpha_1 - \beta_1)^2/(r^2-4)$ must be a square of a rational number. However,

$$\frac{(\alpha_1 - \beta_1)^2}{r^2-4} = \frac{\alpha + \beta - 2\alpha_1\beta_1}{r^2-4} = \frac{r+2\varepsilon}{r^2-4} = \frac{1}{r-2\varepsilon} = t,$$

so t is a perfect square of a rational number, which is impossible.

Remark. Incidentally, we have proved a somewhat stronger statement: if $(u_n)_{n\geq 0}$ is a Lucas sequence of the first kind with $s = \pm 1$, then there exists a rational number t such that the equation $u_n u_{n+1} + t = y^2$ has infinitely many solutions (n, y) with a nonnegative integer $n \geq 0$ and a rational number y if and only if $\alpha = \alpha_1^2$ is a perfect square in $\mathbb{Q}(\alpha_1)$, and in this case, with $-\varepsilon = \alpha_1\beta_1$, the number t must be equal to $1/(r-2\varepsilon)$ and must be a perfect square. In particular, t is unique. Such a result also appears in [5]. As an example of this phenomenon, when $(u_n)_{n\geq 0} = (F_{2n})_{n\geq 0}$ is the Lucas sequence of the first kind of all even indexed Fibonacci numbers, the resulting value of t is precisely $t = 1$, which explains formula (5).

From now on, we assume that $k \geq 3$. To understand the multiplicities of the roots of $P_1(X)$, we use the obvious fact that δ is a root of multiplicity σ of $P_1(X)$ if and only if δ is a root of multiplicity σ of

$$R_1(X) = \frac{P_1(X)}{X^k}. \tag{39}$$

Also notice that the functions $R_1(X)$ and

$$R_2(X) = \prod_{i=0}^{k-1}\left(X - \frac{\zeta^n \varrho^i}{X}\right) = R_1(X) - t_1$$

differ by the additive constant t_1. In particular, $R_1'(X)$ and $R_2'(X)$ are equal, so they have the same roots with the same multiplicities. Based on these observations, we shall show that we may apply Criterion 1 when $m \geq 3$.

When $\zeta = 1$, $R_1(X)$ assumes the value t_1 at exactly $2k$ distinct real points $\{\pm\alpha^{-i} : i = 0, \ldots, k-1\}$. By Rolle's theorem, $R_1'(X)$ has $2k-1$ roots in the interval $[-1, 1]$ and they are all distinct. In particular, $P_1(X)$ cannot have a triple root, because $R_1'(X)$ would then have a double root, and this is impossible. Thus, we may apply Criterion 1 when $m \geq 3$.

When $\zeta = -1$, the situation is more complicated because $R_2(X)$ has complex nonreal roots, so we cannot apply Rolle's theorem right away. Let us consider just the case where n is even because the case of n odd is entirely similar. For n even,

$$R_2(X) = \prod_{j=0}^{k-1}\Big(X - \frac{(-1)^j}{\alpha^{2j}X}\Big). \tag{40}$$

By an argument as before, $R_1(X)$ assumes the value t_1 at $2\lfloor(k-1)/2\rfloor + 2$ real points, namely $\{\pm\alpha^{-j} : 0 \le j \le k-1 \text{ and } j \equiv 0 \pmod 2\}$; therefore, by Rolle's theorem, $R_1'(X)$ has at least $2\lfloor(k-1)/2\rfloor + 1$ real roots which are all distinct. Let $i = \sqrt{-1}$ and

$$R_3(X) = i^{-k}R_2(iX) = \prod_{j=0}^{k-1}\Big(X - \frac{(-1)^{j+1}}{\alpha^{2j}X}\Big). \tag{41}$$

It is clear that $i\delta$ is a root of $R_2(X)$ if and only if δ is a root of $R_3(X)$. Further, we see from Rolle's theorem again that $R_3'(X)$ has at least $2\lfloor k/2\rfloor - 1$ distinct real roots; thus, $R_2'(X) = R_1'(X)$ also has at least $2\lfloor k/2\rfloor - 1$ distinct complex roots, all of them on the imaginary axis. Thus, we have identified $2\lfloor k/2\rfloor + 2\lfloor(k-1)/2\rfloor = 2k-2$ roots of $R_1'(X)$ which are all distinct (notice that the intersection of the real axis with the imaginary axis is the origin, which is not one of these roots), and so we conclude that either all the roots of $P_1(X)$ are of multiplicity at most two, or there exists only one root of multiplicity three, and all the others have multiplicities at most 2. But the degree of $P_1(X)$ is $2k > 4$ and even, so if there exists a triple root, there must exist another root of $P_1(X)$ which is simple, and therefore we can apply Criterion 1 for all $m > 2$.

Thus, it remains to investigate the case where $m = 2$ and all the roots of $P_1(X)$ are double. In this case, there exists a monic polynomial $P_2(X) \in \mathbb{K}[X]$ such that

$$P_1(X) = P_2(X)^2. \tag{42}$$

We now show that k is even. Indeed, suppose that k is odd. Notice that all the monomials appearing in $P_1(X)$, except X^k, are of even degrees. Let j be the smallest possible odd degree of a monomial that appears in $P_2(X)$. Thus,

$$P_2(X) = X^{j+1}P_3(X) + a_jX^j + \sum_{0\le i<j/2} a_iX^{2i}. \tag{43}$$

Such a j exists, for if not, then $P_1(X) = P_2(X)^2$ will not contain any monomial of odd degree. One proves immediately that $j = k$, and since the degree of $P_2(X)$ is precisely k and $P_2(X)$ is monic, we get $P_2(X) = X^k + P_4(X^2)$ with some $P_4(X) \in \mathbb{K}[X]$ of degree $< k/2$. Thus,

$$P_1(X) = (X^k + P_4(X^2))^2 = X^{2k} + P_4(X^2)^2 + 2X^kP_4(X^2). \tag{44}$$

Equating the monomials of odd degrees on both sides of (44), we get $t_1 = 2P_4(X^2)$, and so $P_4(X^2) = d$ is constant. In particular, $P_1(X) = (X^k+d)^2 =$

$X^{2k}+2dX^k+d^2$ does not contain the monomial X^{2k-2}, because $k>2$. However, the coefficient of X^{2k-2} in $P_1(X)$ is obviously

$$-\zeta^n\sum_{i=0}^{k-1}\varrho^i=-\zeta^n\,\frac{1-\varrho^k}{1-\varrho}\neq 0,$$

because ϱ is not a root of unity. This contradiction shows that k must be even. Thus, $k\geq 4$.

SUBCASE 2.3: $k=4$. In this case,

$$P_1(X)=(X^2-\zeta^n)(X^2-\zeta^n\varrho)(X^2-\zeta^n\varrho^2)(X^2-\zeta^n\varrho^3)+t_1X^4. \tag{45}$$

Since $P_1(X)=P_2(X)^2$ and $P_1(-X)=P_1(X)$, and 0 is not a root of $P_1(X)$, it follows easily that $P_2(X)$ contains only monomials of even degrees. Thus, there exist a and b in $\mathbb{K}$ such that $P_2(X)=X^4+aX^2+b$, and substituting X^2 by Z in (42), we get

$$(Z-\zeta^n)(Z-\zeta^n\varrho)(Z-\zeta^n\varrho^2)(Z-\zeta^n\varrho^3)+t_1Z^2=(Z^2+aZ+b)^2. \tag{46}$$

Equating the coefficients in (46), we get

$$2a=-\zeta^n(1+\varrho+\varrho^2+\varrho^3),\qquad a^2+2b=\varrho+\varrho^2+2\varrho^3+\varrho^4+\varrho^5+t_1, \tag{47}$$

$$2ab=-\zeta^n\varrho^3(1+\varrho+\varrho^2+\varrho^3),\qquad b^2=\varrho^6. \tag{48}$$

From the first equations in (47) and in (48), we get $b=\varrho^3$, and inserting this into the second equation of (47) we find

$$\begin{aligned} t_1&=a^2+2b-(\varrho+\varrho^2+2\varrho^3+\varrho^4+\varrho^5)\\ &=\frac{1}{4}\,(1+\varrho+\varrho^2+\varrho^3)^2+2\varrho^3-(\varrho+\varrho^2+2\varrho^3+\varrho^4+\varrho^5)\\ &=\frac{1-2\varrho-\varrho^2+4\varrho^3-\varrho^4-2\varrho^5+\varrho^6}{4}.\end{aligned}$$

Thus, with formulas (32), we get

$$t=\frac{\alpha^6-2\alpha^5\beta-\alpha^4\beta^2+4\alpha^3\beta^3-\alpha^2\beta^4-2\alpha\beta^5+\beta^6}{4(\alpha-\beta)^4}. \tag{49}$$

If we write $\alpha\beta=-s=\pm1$, and use $(v_n)_{n\geq 0}$ for the Lucas sequence of the second kind with roots α and β, the above formula (49) can be rewritten as

$$t=\frac{v_6+2sv_4-v_2-4s}{4(r^2+4s)^2}. \tag{50}$$

Since $v_0=2$ and $v_1=r$, one can use the recurrence relation $v_{n+2}=rv_{n+1}+sv_n$, which holds for all $n\geq 0$, to check that $v_2=r^2+2s$, $v_4=r^4+4r^2s+2$, $v_6=r^6+6r^4s+9r^2+2s$, and plugging all these into (50), we get, after some simplifications,

$$t=\frac{r^6+8r^4s+16r^2}{4(r^2+4s)^2}=\frac{r^2(r^4+8r^2s+16s^2)}{4(r^2+4s)^2}=\frac{r^2}{4}=\left(\frac{r}{2}\right)^2. \tag{51}$$

Of course, (51) is impossible, because t is not allowed to be a perfect power of some other rational number.

Remark. Incidentally, we proved that if $(u_n)_{n\geq 0}$ is a Lucas sequence of the first kind with $s=\pm 1$ such that there exists a rational number t with $u_nu_{n+1}u_{n+2}u_{n+3}+t$ being a perfect square for infinitely many $n\geq 0$, then $t=(r/2)^2$. In particular, t is uniquely determined, and is a perfect square. When $(u_n)_{n\geq 0}=(F_n)_{n\geq 0}$ is the Fibonacci sequence, we have $r=1$, so $t=1/4$, which explains the example in (6). ■

From now on, we assume that $k\geq 6$. We notice that either $4\,|\,k$, or $\zeta=1$. Indeed, the fact that $\zeta=1$ when $k\equiv 2 \pmod 4$ follows by identifying the constant term of $P_1(X)$ from (42), which on the one hand must be a perfect square (the perfect square of the constant term of $P_2(X)$), while on the other hand it must be, by (31) and (32),

$$(-\zeta^n)^k\,\varrho^{k(k-1)/2}=\zeta^{k(k-1)/2}\,\frac{1}{\alpha^{k(k-1)}},$$

and $\alpha^{k(k-1)}$ is already a perfect square in $\mathbb{K}$, while when $\zeta=-1$, we have $\zeta^{k(k-1)/2}=-1$, because $k\equiv 2 \pmod 4$, and -1 cannot be a square in $\mathbb{K}$, because the quadratic field $\mathbb{K}$ is real. Hence, $4\,|\,k$ when $\zeta=-1$. We also write $t_1=t_2^2$ for some algebraic number t_2. Note that $t_2\in\mathbb{K}$ when $\zeta=1$ (or when $\zeta=-1$ and n is even) because in this case by evaluating (42) at $X=1$ we find that $t_1=P_1(1)=P_2(1)^2$ is a square of an element of $\mathbb{K}$.

We shall first treat the case where $4\,|\,k$. In particular, $k\geq 8$. As pointed out before, $P_1(X)$ has only monomials of even degrees, hence so does $P_2(X)$. In particular, if we write $P_5(X)$ for the polynomial in $\mathbb{K}[X]$ such that $P_2(X)=P_5(X^2)$ and $Z=X^2$, formula (42) becomes

$$\prod_{i=0}^{k-1}(Z-\varepsilon\varrho^i)+t_2^2Z^{k/2}=P_5(Z)^2,$$

where $\varepsilon=\zeta^n\in\{\pm1\}$, which can be rewritten as

$$\prod_{i=0}^{k-1}(Z-\varepsilon\varrho^i)=(P_5(Z)-t_2Z^{k/4})(P_5(Z)+t_2Z^{k/4}). \tag{52}$$

From (52), together with the fact that $P_5(Z)$ is monic of degree $k/2$, it follows that there exists a partition of $\{0,\dots,k-1\}$ into two subsets I and J of the same cardinality $k/2$ such that

$$P_5(Z)-t_2Z^{k/4}=\prod_{i\in I}(Z-\varepsilon\varrho^i),\qquad P_5(Z)+t_2Z^{k/4}=\prod_{j\in J}(Z-\varepsilon\varrho^j). \tag{53}$$

Thus,

$$2t_2Z^{k/4} = \prod_{j\in J}(Z-\varepsilon\varrho^j) - \prod_{i\in I}(Z-\varepsilon\varrho^i). \tag{54}$$

By equating the coefficients of $Z^{k/2-1}$ on both sides of (54), we get

$$\sum_{i\in I}\varrho^i = \sum_{j\in J}\varrho^j \tag{55}$$

since $k > 5$. If we write $\alpha_2 = \alpha^2$, equations (32) and (55) lead to a relation

$$\alpha_2^{k-1} = \sum_{i=0}^{k-2}\varepsilon_i\alpha_2^i \quad \text{with some } \varepsilon_i \in \{\pm 1\} \text{ for } i = 0,\dots,k-2. \tag{56}$$

This implies that $\alpha_2 < 2$. However, $\alpha_2 = \alpha^2$, and α is a quadratic unit, so $|\alpha| \ge (1+\sqrt{5})/2$, which is a contradiction.

Finally, the case of $k \equiv 2 \pmod 4$ can be dealt with in a similar way. Namely, in this case we have $\zeta = 1$. Further, $\alpha > 0$ by (3). Indeed, if $\alpha < 0$, then $u_n u_{n+1} < 0$ for all large n. In particular, for $k \equiv 2 \pmod 4$, the inequality

$$\prod_{i=0}^{k-1} u_{n+i} + t = t + \prod_{i=0}^{k/2-1} u_{n+2i}u_{n+2i+1} < 0$$

holds for all large values of n, so (3) cannot hold with some rational number y and $m = 2$. Thus, $\alpha > 0$ and we may write

$$\prod_{i=0}^{k-1}(X^2-\varrho^i) + t_2^2X^k = P_2(X)^2,$$

and therefore

$$\prod_{i=0}^{k-1}(X-\varrho^i)(X+\varrho^i) = (P_2(X)-t_2X^{k/2})(P_2(X)+t_2X^{k/2}). \tag{57}$$

Hence, again we may partition the set $\{\pm\varrho^i : i = 0,\dots,k-1\}$ into two subsets, say $\mathcal{A}$ and $\mathcal{B}$, each of cardinality k, such that

$$\begin{aligned} P_2(X) - t_2X^{k/2} &= \prod_{\varrho\in\mathcal{A}}(X-\varrho), \\ P_2(X) + t_2X^{k/2} &= \prod_{\varrho'\in\mathcal{B}}(X-\varrho'). \end{aligned} \tag{58}$$

Thus, we get the relation

$$2t_2X^{k/2} = \prod_{\varrho'\in\mathcal{B}}(X-\varrho') - \prod_{\varrho\in\mathcal{A}}(X-\varrho). \tag{59}$$

Since $k > 3$ in this case, we may equate the coefficients of X^{k-1} to get

$$\sum_{\varrho' \in \mathcal{B}} \varrho' = \sum_{\varrho \in \mathcal{A}} \varrho. \tag{60}$$

The above relation (60) may be trivial or not. That is, if there exists $\varrho \in \mathcal{A}$ such that $-\varrho \notin \mathcal{A}$, then, as in the previous case, equation (60) leads to the conclusion that there exist $\mu \geq 1$, indices $0 \leq i_1 < \cdots < i_\mu$ in $\{0, \ldots, k-1\}$, and signs $\varepsilon_\nu \in \{\pm 1\}$ for $\nu = 0, \ldots, \mu$ such that

$$\sum_{\nu=0}^{\mu} \varepsilon_\nu \alpha^\nu = 0. \tag{61}$$

The conclusion is again that $\alpha < 2$. However, since $\zeta = 1$, it follows that α is a quadratic unit of norm 1, and the smallest such is again at least $2 + \sqrt{3} > 2$, which is a contradiction.

Assume that (60) is trivial. In this case, whenever $\varrho \in \mathcal{A}$ then also $-\varrho \in \mathcal{A}$. But if this is so, since $k/2 \geq 3$, we may equate the coefficients of X^2 on both sides of (59), and since both $\mathcal{A}$ and $\mathcal{B}$ have the property that once they contain an element they also contain its negative, we get

$$\sum_{\varrho' \in \mathcal{B}} \frac{1}{\varrho'^2} = \sum_{\varrho \in \mathcal{A}} \frac{1}{\varrho^2}. \tag{62}$$

With $\alpha_2 = \alpha^2$, equation (62) yields

$$\alpha_2^{k-1} = \sum_{i=0}^{k-2} \varepsilon_i \alpha_2^i \quad \text{with some } \varepsilon_i \in \{\pm 1\} \text{ for } i = 0, \ldots, k-2,$$

which again leads to the conclusion that $\alpha_2 < 2$, which is impossible.

This completes the analysis of the case $\alpha \notin \mathbb{Q}$, and Theorem 1 is proved.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. 65 (1969), 439–444.

[2] Yu. F. Bilu, M. Kulkarni and B. Sury, *The Diophantine equation $x(x+1)\cdots(x+(m-1))+r=y^n$*, Acta Arith. 113 (2004), 303–308.

[3] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, *Perfect powers from products of terms in Lucas sequences*, J. Reine Angew. Math. 611 (2007), 109–129.

[4] P. Corvaja and U. Zannier, *Diophantine equations with power sums and universal Hilbert sets*, Indag. Math. (N.S.) 9 (1998), 317–332.

[5] M. N. Deshpande and A. Dujella, *An interesting property of a recurrence related to the Fibonacci sequence*, Fibonacci Quart. 40 (2002), 157–160.

[6] C. Fuchs, *Polynomial-exponential equations and linear recurrences*, Glas. Mat. Ser. III 38 (58) (2003), 233–252.

[7] F. Luca and T. N. Shorey, *Diophantine equations with products of consecutive terms in Lucas sequences*, J. Number Theory 114 (2005), 298–311.

[8] T. N. Shorey and C. L. Stewart, *Pure powers in recurrence sequences and some related Diophantine equations*, ibid. 27 (1987), 324–352.

[9] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, Cambridge, 1986.

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai, 400005, India
E-mail: shorey@math.tifr.res.in

Received on 17.5.2007
and in revised form on 29.10.2007 (5446)