View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 114 (2005) 298–311

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Diophantine equations with products of consecutive terms in Lucas sequences

F. Luca[a,*], T.N. Shorey[b]

[a] *Instituto de Matemáticas, UNAM, Campus Morelia, Ap. Postal 61-3 (Xangari) CP 58 089 Morelia, Michoacán, México*

[b] *School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai, 400005, India*

Received 12 February 2004; revised 21 May 2004

Available online 11 November 2004

Communicated by A. Granville

Abstract

In this paper, we show that if $(u_n)_{n\geqslant 1}$ is a Lucas sequence, then the Diophantine equation $u_n \cdot u_{n+1} \cdot \cdots \cdot u_{n+k} = y^m$ in integers $n \geqslant 1$, $k \geqslant 1$, $m \geqslant 2$ and y with $|y| > 1$ has only finitely many solutions. We also determine all such solutions when $(u_n)_{n\geqslant 1}$ is the sequence of Fibonacci numbers and when $u_n = (x^n - 1)/(x - 1)$ for all $n \geqslant 1$ with some integer $x > 1$.
© 2004 Elsevier Inc. All rights reserved.

Keywords: Lucas sequences; Primitive divisors; Arithmetic progressions

1. Introduction

There are several papers in the literature dealing with Diophantine equations involving powers in products of consecutive integers, or in products of consecutive terms in arithmetic progressions. For example, Erdős and Selfridge [6] showed that a product of at least two consecutive integers is never a perfect power. For a survey, see [17].

In this paper, we address a similar question when the product of consecutive terms in arithmetic progressions is replaced by the product of terms in Lucas sequences

* Corresponding author.
E-mail addresses: fluca@matmor.unam.mx (F. Luca), shorey@math.tifr.res.in (T.N. Shorey).

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.08.007

whose indices form an arithmetic progression. To fix the notations and terminology, we assume that r and s are nonzero integers with $\Delta = r^2 + 4s \neq 0$, put $\ell = \gcd(r, s)$, let α and β be the two roots of the equation $x^2 - rx - s = 0$, with the convention that $|\alpha| \geqslant |\beta|$ and write $(u_n)_{n\geqslant 0}$ and $(v_n)_{n\geqslant 0}$ for the Lucas sequences of first and second kind, respectively, of general terms

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{for all } n \geqslant 0 \tag{1.1}$$

and

$$v_n = \alpha^n + \beta^n \qquad \text{for all } n \geqslant 0. \tag{1.2}$$

The sequences $(u_n)_{n\geqslant 0}$ and $(v_n)_{n\geqslant 0}$ have $u_0 = 0$, $u_1 = 1$, $v_0 = 2$ and $v_1 = r$ and they both satisfy the recurrence relation $u_{n+2} = ru_{n+1} + su_n$ and $v_{n+2} = rv_{n+1} + sv_n$ for all $n \geqslant 0$. We shall also assume that these sequences are nondegenerate, i.e., that α/β is not a root of unity. In general, when dealing with such sequences one also assumes that $\ell = 1$ (i.e., that r and s are coprime), but for our purpose we shall not need to impose this restriction. Examples of such sequences which have received considerable interest are when $(r, s) = (1, 1)$ for which the resulting sequences $(u_n)_{n\geqslant 0}$ and $(v_n)_{n\geqslant 0}$ are the sequences of Fibonacci and Lucas numbers denoted from here on by $(F_n)_{n\geqslant 0}$ and $(L_n)_{n\geqslant 0}$, respectively, and when $(r, s) = (x + 1, -x)$ with some positive integer $x > 1$, for which the corresponding general terms of the Lucas sequences of the first and second kind are

$$u_n = \frac{x^n - 1}{x - 1} \qquad \text{and} \qquad v_n = x^n + 1 \qquad \text{for all } n \geqslant 0,$$

respectively.

Closely related to the Lucas sequences are the Lehmer sequences. Given nonzero integers $r > 0$ and s such that $r + 4s \neq 0$, let γ and δ be the two roots of the quadratic equation $x^2 - \sqrt{r}x - s = 0$. Then the Lehmer sequence of roots γ and δ is the sequence of general term

$$w_n = \begin{cases} \dfrac{\gamma^n - \delta^n}{\gamma - \delta} & \text{if } n \equiv 1 \pmod 2, \\ \dfrac{\gamma^n - \delta^n}{\gamma^2 - \delta^2} & \text{if } n \equiv 0 \pmod 2. \end{cases}$$

The number w_n is an integer for all $n \geqslant 0$. We assume that γ/δ is not a root of 1, but we do not assume that r and s are coprime.

For an integer k we write $P(k)$ for the largest prime divisor of k with the convention that $P(0) = P(\pm 1) = 1$. We suppose throughout the paper that n, d, k, m and y are positive integers with $m \geqslant 2$, $\gcd(n, d) = 1$ and $y > 1$ and that b is a nonzero integer. We put

$$f(k, d) = \begin{cases} 2k & \text{if } d > 1, \\ k & \text{if } d = 1. \end{cases}$$

We consider the Diophantine equations

$$u_n u_{n+d} \dots u_{n+(k-1)d} = by^m \tag{1.3}$$

and

$$v_n v_{n+d} \dots v_{n+(k-1)d} = by^m \tag{1.4}$$

in unknowns (n, d, k, b, y, m). Arithmetic properties with products of consecutive terms in binary recurrences were investigated in [15]. For a given b, it follows from results proved independently by Pethö [12] and Shorey and Stewart [18], that either one of Eqs. (1.3) and (1.4) with $k = 1$ or 2 implies that n, d, y and m are bounded by an effectively computable number depending only on r, s and b. In fact, the preceding assertion with b composed only of primes from a given finite set follows from the result of Pethö. For $k \geqslant 3$ we prove the following result.

Theorem 1. *Assume that* $k \geqslant 3$.

(i) *Eq.* (1.3) *with* $P(b) \leqslant f(k, d)$ *implies that k is bounded by an effectively computable number depending only on the sequence* $(u_n)_{n \geqslant 0}$.

(ii) *Let* $P \geqslant 1$. *Then Eq.* (1.3) *with* $P(b) \leqslant P$ *implies that*

$$\max\{n, d, k, |b|, y, m\} < c_1,$$

where c_1 *is an effectively computable number depending only on r, s and P.*

(iii) *Assertions* (i) *and* (ii) *with the sequence* $(u_n)_{n \geqslant 0}$ *replaced either by the sequence* $(v_n)_{n \geqslant 0}$ *or* $(w_n)_{n \geqslant 0}$ *are also valid.*

Here are some particular instances of Theorem 1. We begin with $u_n = F_n$. A long-standing conjecture that F_n is a perfect power only when $n = 0, 1, 2, 6$ and 12 has been recently confirmed by Bugeaud et al. [4]. We prove the following result.

Theorem 2. *Eq.* (1.3) *with* $u_n = F_n$, $n > 1$, $b = 1$ *and* $k \geqslant 2$ *is not possible.*

In particular, a nonzero product of two or more consecutive Fibonacci numbers is never a perfect power except for the trivial case $F_1 \cdot F_2 = 1$.

Theorem 3. *Let* $x > 1$ *be an integer. Then Eq.* (1.3) *with* $(r, s) = (x + 1, -x)$, *for which*

$$u_n = \frac{x^n - 1}{x - 1} \qquad \text{for all } n \geqslant 0,$$

$b = 1$, $n > 1$, $k \geqslant 2$ *and d odd does not hold.*

We note that the sequence $(u_n)_{n \geqslant 0}$ appearing in the statement of Theorem 3 is the sequence of all the *rep-units in base x*, namely the sequence consisting of 0 together will all positive integers whose base x representation consists of a string of 1's.

We recall that the Diophantine equation from Theorem 3 with $k = 1$, $x > 1$, $n > 2$, and $m > 2$ is still unsolved, although several particular instances of this equation have been dealt with (see the survey papers [3,16]).

Throughout the proofs, $c_2, c_3, \ldots$ are effectively computable constants larger than 1 which depend only on the initial data. For a real number $x > 1$ we use $\log x$ for the natural logarithm of x and $\pi(x)$ for the number of prime numbers $p \leqslant x$. For a nonzero integer k and a prime number p we write $\mathrm{ord}_p(k)$ for the exact order at which p appears in the factorization in prime factors of k. For two positive integers m and n we write either $\gcd(m, n)$ or (m, n) for the greatest common divisor of m and n.

2. The proof of Theorem 1.1

We shall prove this theorem only for the case of the Lucas sequence of the first kind $(u_n)_{n \geqslant 0}$ as the proofs for the cases of the Lucas sequence $(v_n)_{n \geqslant 0}$ or the Lehmer sequence $(w_n)_{n \geqslant 0}$ are entirely similar. In order to simplify the presentation, we shall first assume that $\ell = 1$ and we shall treat the general case later. There are three well-known properties of the Lucas sequence $(u_n)_{n \geqslant 0}$ which we will use, namely:

(a) $\gcd(u_m, u_n) = u_{(m,n)}$.
(b) If $m|n$ and p is a prime dividing $\gcd(u_m, u_n/u_m)$, then p divides n/m.
(c) If $n > 30$, then there exists a prime factor p of u_n which does not divide either Δ or u_m for any positive integer $m < n$. Such a prime p is always congruent to ± 1 modulo n (see [1]).

We shall assume that $k > c_2 = \max\{30, P(\Delta)\}$ and we shall write $Q = P(n(n+d) \cdot \ldots \cdot (n+(k-1)d))$. We distinguish two cases:

Case 1: Assume that either $d > 1$, or $d = 1$ but $n \geqslant k + 1$.

When $d = 1$, then $Q > k > c_2$ by a theorem of Sylvester. When $d > 1$, then the same inequality holds except when $(n, d, k) = (2, 7, 3)$ by a result from [20]. Since we are assuming that $k > c_2 \geqslant 30$, it follows that the inequality $Q > k$ always holds. We write i for the unique positive integer in the interval $[0, k-1]$ such that $Q \mid (n+id)$ and we write v for $\mathrm{ord}_Q(n+id)$. Thus, $n + id = Q_1 \cdot m_i$, with $Q_1 = Q^v$ and $P(m_i) < Q$. We rewrite Eq. (1.3) as

$$u_{Q_1} \cdot M_1 = by^m,$$

where

$$M_1 = \frac{u_{n+id}}{u_{Q_1}} \cdot \prod_{\substack{j \in [0,k-1] \\ j \neq i}} u_{n+jd}. \tag{2.1}$$

We now show that $\gcd(u_{Q_1}, M_1) = 1$. In order to prove this, we first look at the prime factors of $\gcd(u_{Q_1}, u_{n+id}/u_{Q_1})$. By (b) above, these numbers divide $(n+id)/Q_1 = m_i$. Since Q_1 is a power of $Q > P(\Delta)$ and Q is odd, it follows, by (c) above, that all the prime divisors of u_{Q_1} are congruent to ± 1 modulo $2Q_1$. In particular, either $u_{Q_1} = \pm 1$, or any prime divisor of u_{Q_1} is at least $2Q_1 - 1 > P(m_i)$. The instance $u_{Q_1} = \pm 1$ is impossible by (c) above when $Q_1 \geqslant Q > 30$. We now look at $\gcd(u_{Q_1}, u_{n+jd})$ for $j \neq i$. By (a) above, this number equals $u_{(Q_1, n+jd)}$. However, since $j \neq i$, we have

that $P(n+jd) < Q$, therefore $\gcd(Q_1, n+jd) = 1$. Thus, $\gcd(u_{Q_1}, u_{n+jd}) = u_1 = 1$ for $j \neq i$. Now Eq. (2.1) together with the fact that any prime divisor p of u_{Q_1} satisfies $p \geqslant 2Q_1 - 1 \geqslant 2(k+1) - 1 > 2k$ implies that if either condition (i) or (ii) is satisfied and $k > P/2$, then equation $u_{Q_1} = \pm y_1^m$ holds with some integer $y_1 \geqslant 1$. From [19, Corollary 9.2, p. 152], we obtain that $Q_1 < c_3$. Since $k < Q \leqslant Q_1 < c_3$, we have obtained that $k < c_3$. This proves (i) for this case as well as the fact that k is bounded in this case and in instance (ii).

Case 2: Assume that $d = 1$ and that $n \leqslant k$.

In this case, $n(n+1)\dots(n+k-1)$ is a multiple of $k!$. By Bertrand's postulate, there exists a prime number p in the interval $[k/2, k]$. Since we are assuming that $k > 30$, we can infer even more, namely that there exists a prime number in the interval $[2k/3, k]$. Indeed, this assertion is equivalent to the fact that $\pi(k) - \pi(2k/3) \geqslant 1$ holds for $k \geqslant 30$. From [14, Theorem 2], we know that the inequality

$$\frac{x}{\log x - 0.5} < \pi(x) < \frac{x}{\log x - 1.5} \tag{2.2}$$

holds for all $x > 67$. We checked that the inequality

$$\frac{x}{\log x - 0.5} - \frac{(2x/3)}{\log(2x/3) - 1.5} > 1$$

holds for all $x > 150$, which implies that the interval $[2x/3, x]$ contains a prime number whenever $x > 150$. This is also true for $x \in [30, 150]$ and in this range the above assertion can be checked by hand.

Thus, we know that $Q \geqslant 2k/3$. If there exists only one index $i \in [0, k-1]$ such that $Q \mid (n+i)$, then the argument from Case 1 shows that k is bounded in either instance (i) or (ii). Assume therefore that $i_1 < i_2$ are in $[0, k-1]$ and have the property that both $n+i_1$ and $n+i_2$ are multiples of Q. It is clear that $i_2 = i_1 + Q$. Write $n + i_1 = Qm_{i_1}$ and $n + i_2 = Q(m_{i_1} + 1)$. Then $Q(m_{i_1}+1) \leqslant n + k - 1 \leqslant 2k - 1$, therefore $2 \leqslant m_{i_1} + 1 \leqslant \dfrac{(2k-1)}{Q} \leqslant \dfrac{3(2k-1)}{2k} < 3$. Thus, $m_{i_1} = 1$. We therefore get $n + i_1 = Q$ and $n + i_2 = 2Q$. Hence, $u_{n+i_2} = u_{2Q} = u_Q \cdot v_Q$. We rewrite Eq. (1.3) as

$$\frac{v_Q}{v_1} \cdot v_1 \cdot u_Q^2 \cdot \prod_{\substack{j \in [0,k-1] \\ j \neq i_1, i_2}} u_{n+j} = by^m. \tag{2.3}$$

One proves easily that v_Q/v_1 is always odd for $Q > 3$, that $\gcd(v_Q/v_1, v_1) = Q$ or 1 according to whether $Q \mid v_1$ or not, and that $\gcd(v_Q/v_1,\ u_{n+j}) = 1$ holds whenever $j \neq i_1,\ i_2$ is in $[0, k-1]$. Assuming now that Q does not divide $v_1 = r$ (this can be arranged say if $2k/3 > P(r)$, or, equivalently, if $k > c_4 = 3P(r)/2$), we then get that Eq. (2.3) together with the fact that every prime divisor of v_Q/v_1 is $\geqslant 2Q - 1 \geqslant 4k/3 - 1 > k$ imply that

$$v_Q/v_1 = \pm y_1^m$$

holds with some positive integer $y_1 \geqslant 1$. From [19, Corollary 9.2, p. 152], we obtain that $Q < c_3$, and since $2k/3 \leqslant Q < c_3$, we get that $k < c_5 = 3c_3/2$. This completes the proof of (i).

To complete the proof of (ii), assume that P is a given constant and that Eq. (1.3) holds with some integer b such that $P(b) \leqslant P$. By the above arguments, it follows that both $k < c_6$ and $P(n(n+d)\dots(n+(k-1)d)) < c_6$ hold with an effectively computable constant c_6 depending on r, s and P. We assume, of course, that $c_6 > P$. Let $\mathcal{S} = \{n \geqslant 1 \mid P(n) < c_6\}$. We recall that $k \geqslant 3$. We now claim that there exists a computable constant c_7 such that if $n(n+d)(n+2d) \in \mathcal{S}$ then $\max\{n, d\} < c_7$. Indeed, the relation $n(n+d)(n+2d) \in \mathcal{S}$ together with the fact that n and d are coprime implies that the three positive integers $x = n$, $y = n+d$ and $z = n+2d$ have $\gcd(x, y) = \gcd(y, z) = 1$, $\gcd(x, z) \mid 2$, $2y = x + z$ and $x,\ y,\ z \in \mathcal{S}$. This last equation is an S-unit equation and it is well-known that this equation has only finitely many effectively computable such solutions (x, y, z). Since $3 \leqslant k \leqslant c_6$ it follows that $\max\{n, d, k\} < c_7$ holds with some effectively computable constant c_7, which together with the fact that $y > 1$ implies that $|b|$, m and y are also bounded by an effectively computable constant.

Assume now that $\ell > 1$, suppose that k satisfies $k > \max\{30, P(\Delta), 3P(r)/2, P(\ell)\}$ and write $\ell_1 = \gcd(r^2, s)$. Notice that every prime number dividing ℓ_1 divides ℓ as well. Put $r_1 = r/\sqrt{\ell_1}$, $s_1 = s/\ell_1$ and put α_1 and β_1 for the roots of the quadratic equation $x^2 - r_1 x - s_1 = 0$ with the convention that $|\alpha_1| \geqslant |\beta_1|$. Clearly, $\alpha_1 = \alpha/\sqrt{\ell_1}$ and $\beta_1 = \beta/\sqrt{\ell_1}$. Moreover, notice that $s_1 \in \mathbf{Z}$ and $r_1^2 = r^2/\ell_1 \in \mathbf{Z}$. Write $(w_n)_{n \geqslant 0}$ for the sequence of Lehmer numbers of roots α_1 and β_1 whose general term is given by

$$w_n = \begin{cases} \dfrac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1} & \text{if } n \equiv 1 \pmod 2, \\ \dfrac{\alpha_1^n - \beta_1^n}{\alpha_1^2 - \beta_1^2} & \text{if } n \equiv 0 \pmod 2. \end{cases} \tag{2.4}$$

It is well-known that w_n is an integer for all $n \geqslant 0$. Moreover (see [19, Lemma A.10]), the two ideals $[\alpha_1^2] = [\alpha^2/\ell_1]$ and $[\beta_1^2] = [\beta^2/\ell_1]$ are coprime in $\mathcal{O}_{\mathbf{K}}$ where $\mathbf{K} = \mathbf{Q}[\alpha]$. It is also easy to see that the formula

$$u_n = \begin{cases} \ell^{\lfloor n/2 \rfloor} w_n & \text{if } n \equiv 1 \pmod 2, \\ r\ell^{\lfloor n/2 \rfloor - 1} w_n & \text{if } n \equiv 0 \pmod 2, \end{cases} \tag{2.5}$$

holds for all $n \geqslant 0$. Since we are assuming that $k > \max\{P(\ell), 3P(r)/2\}$, it follows that every solution of Eq. (1.3) leads to a solution of

$$w_n w_{n+d} \cdot \ldots \cdot w_{n+(k-1)d} = b_1 y^m, \tag{2.6}$$

with the same value of y and with some different nonzero integer b_1 satisfying $P(b_1) \leqslant f(k, d)$. The sequence $(w_n)_{n \geqslant 0}$ enjoys the same divisibility properties as the

Lucas sequence of the first kind and its nth term has primitive divisors for $n > 30$ by the result from [1]. Moreover, since the ideals $[\alpha_1^2]$ and $[\beta_1^2]$ are coprime in $\mathcal{O}_{\mathbf{K}}$, one may now employ the same arguments as the ones used in the proof of the case in which $\ell = 1$ to conclude that both (i) and (ii) hold in this instance as well.

The proofs for the cases of the sequences $(v_n)_{n\geqslant 0}$ and $(w_n)_{n\geqslant 0}$ are entirely similar and we give no further details here. Theorem 1 is therefore proved.

Remark 1. Note that the condition $k > P(\Delta)$ appearing in the above arguments can be relaxed in the following sense. There exists a constant k_0 which depends only on $\omega(\Delta)$ such that if $k > k_0$, then Eq. (1.3) with $P(b)\leqslant k$ implies that there exists a prime number Q (with $Q > k$ if $d > 1$, or $n\geqslant k+1$ and $Q > 2k/3$ otherwise) and which does not divide Δ, such that the equation $u_{Q_1} = \pm y_1^m$ holds with Q_1 a power of Q and some positive integer y_1. Indeed, a close analysis of our arguments shows that the only relevant feature of our choice of the number $Q = P(n(n+d)\dots(n+(k-1)d))$ is that $Q > k$ and that Q does not divide Δ. Assume that $d > 1$. Then a recent result from [8] confirming a conjecture of Moree from [11] shows that the inequality $\omega(n(n+d)\dots(n+(k-1)d)) > \pi(2k)-1$ holds save for the exceptional triple $(n, d, k) = (1, 3, 10)$. In particular, imposing that $k > k_0$ where k_0 is the smallest solution to the inequality $\pi(2k) - \pi(k) - 1 > \omega(\Delta)$, it follows that up to the above exception Eq. (1.3) with such a value of k will lead to an equation of the form $u_{Q_1} = \pm y_1^m$ with Q_1 a power of some prime $Q > k$ and some positive integer y_1 (which could be 1 and then u_{Q_1} will have no primitive divisors). A similar argument can be employed in the case when $d = 1$ and $n\geqslant k+1$ by a result from [7] where it is shown that the inequality $\omega(n(n+1)\dots(n+k-1)) > \pi(k) + \lfloor 3\pi(k)/4\rfloor - 1$ holds for all $n\geqslant k+1$ with finitely many exceptions (n, k) which are all explicitly known. Such observations can be useful when trying to find all the solutions of an equation like (1.3) with an explicitly given sequence $(u_n)_{n\geqslant 0}$. We also offer the following conjecture.

Conjecture 1. *Let $(u_n)_{n\geqslant 0}$ be a Lucas sequence of the first kind. Then the Diophantine equation*

$$u_n u_{n+d} \cdot \dots \cdot u_{n+(k-1)d} = by^m \tag{1.5}$$

in integer unknowns (n, d, k, b, y, m) with $n\geqslant 1$, $d\geqslant 1$ and coprime to n, $k\geqslant 1$, $m\geqslant 2$, $y > 1$, and $P(b)\leqslant k$ implies that k is bounded by an absolute constant. A similar conjecture can be made for the sequences $(v_n)_{n\geqslant 0}$ and $(w_n)_{n\geqslant 0}$.

Remark 2. We note that the conclusion of Theorem 1 remains valid if we replace the assumption that $\gcd(n, d) = 1$ by the assumption that $\gcd(n, d)$ is bounded by a fixed constant.

3. The proof of Theorem 2

Just to eliminate the small solutions, we used Mathematica to show that

$$F_n \dots F_{n+(k-1)d} = y^m \tag{3.1}$$

does not have any integer solutions $n > 0$, $k > 1$, $d \geqslant 1$ and coprime to n and with $n + (k-1)d \leqslant 190$ except for the trivial one $F_1 \cdot F_2 = 1$. What we did was to check computationally that if $p > 17$ is a prime number and $0 < \ell \leqslant 190$ then p^2 does not divide F_ℓ. Since for $\ell > 12$ the number F_ℓ has primitive divisors which are larger than or equal to $\ell - 1$, it follows that if $18 < n + (k-1)d \leqslant 190$, then $F_{n+(k-1)d}$ has a primitive divisor p such that p^2 does not divide $F_{n+(k-1)d}$. This certainly shows that Eq. (3.1) is impossible when $n + (k-1)d > 18$. The fact that Eq. (3.1) has no solutions with $n > 0$, $k > 1$, $d \geqslant 1$ and coprime to n and $3 \leqslant n + (k-1)d \leqslant 18$ other than $F_1 \cdot F_2 = 1$ can be checked by hand.

From now on, we shall assume that $n + (k-1)d > 190$. We may certainly assume that $m = q$ is a prime number. We split the argument into two steps.

Step 1: Assume that $d = 1$ and that $n \leqslant k$.

In this case, it is easy to see that the interval $[0, k-1]$ contains a number i such that $n + i$ is a power of 2. Indeed, this is clearly so when $n = k$ because in this case the interval $[n, n+k-1]$ is simply $[k, 2k-1]$, while when $n \leqslant k-1$ then

$$I = \left(\frac{n+k-1}{2}, n+k-1 \right] \subset [n, n+k-1]$$

and the interval I clearly contains a unique power of 2. Let us write this power of 2 as $n + i = 2^\mu$. Thus, if $j \neq i \in [0, k-1]$, then $\mathrm{ord}_2(n+j) < \mu$. Notice also that $2k - 1 \geqslant n + k - 1 \geqslant 191$ therefore $k \geqslant 96$. Since $2^\mu > \dfrac{n+k-1}{2} \geqslant \dfrac{k}{2} \geqslant 48$, we deduce that $\mu \geqslant 6$. Thus, we may rewrite Eq. (3.1) as

$$L_{2^{\mu-1}} \cdot F_{2^{\mu-1}} \cdot \prod_{\substack{j \in [0,k-1] \\ j \neq i}} F_{n+j} = y^q. \tag{3.2}$$

It follows immediately that $\gcd(L_{2^{\mu-1}}, F_j) = 1$ for $j \neq i \in [0, k-1]$ and $\gcd(F_{2^{\mu-1}}, L_{2^{\mu-1}}) = 1$. Thus, Eq. (3.2) implies that $L_{2^{\mu-1}} = y_1^q$ holds with some integer $y_1 > 1$ and some prime number $q \geqslant 2$. Since $2^{\mu-1} \geqslant 32$, it follows, by the results from [4], that this equation is impossible.

From now on, we assume that $n \geqslant k+1$ if $d = 1$.

Step 2: The final contradiction.

By Sylvester's theorem, we have that $Q = P(n(n+d)\ldots(n+(k-1)d)) > k$ when $d = 1$, because $n \geqslant k+1$ in this case. The same is true when $d > 1$ (without the restriction that $n \geqslant k+1$) by the result from [20] which says that the only exception to the above inequality is the instance $(n, d, k) = (2, 7, 3)$ for which $n + (k-1)d = 16 < 190$. It is also clear that in our range we have $Q \geqslant 5$. Indeed, for if $Q \leqslant 3$, it would then follow that $k = 3$ and that each one of the three positive integers n, $n+d$ and $n+2d$ is either 1, or is divisible only by primes from the set $\{2, 3\}$. Thus, either $n = 1$ and $\{n+d, n+2d\} = \{2^a, 3^b\}$, or $n + d = 3^b$ and $\{n, n+2d\} = \{2^{a_1}, 2^{a_2}\}$. In the first instance we get the Diophantine equation $3^b - 2^{a+1} = 1$, while in the second

instance we get the Diophantine equation $2^{a_2} - 2^{a_1} = 2 \cdot 3^b$. The largest solution of such equations is $n + 2d = 9 < 190$.

It now follows that there exists a unique value of the index $i \in [0, k-1]$ such that $Q \mid (n + id)$. Write $n + id = Q_1 m_i$, where $Q_1 = Q^\mu$ holds with some positive integer μ and some positive integer m_i coprime to Q. We may therefore rewrite Eq. (3.1) as

$$F_{Q_1} \cdot \frac{F_{n+id}}{F_{Q_1}} \cdot \prod_{\substack{j \in [0,k-1] \\ j \neq i}} F_{n+jd} = y^q. \tag{3.2}$$

By the argument from the proof of Theorem 1, we have that $\gcd(F_{Q_1}, F_{n+jd}) = F_{\gcd(Q_1, n+jd)} = F_1 = 1$ when $j \neq i$ and that $\gcd(F_{Q_1}, F_{n+id}/F_{Q_1}) = \gcd(F_{Q_1}, m_i) = 1$, because m_i is coprime to $Q \geqslant 5$. Moreover, all the prime divisors of F_{Q_1} are congruent to $\pm 1 \pmod{2Q}$ and therefore at least as large as $2Q - 1 > P(m_i)$ when $Q > 5$, or they are at least as large as 5 when $Q = 5$, but in this case we have again that $P(m_i) < Q = 5$. Eq. (3.2) now implies that $F_{Q_1} = y_1^q$ must hold with some positive integer y_1, which is impossible by the result of [4].

This completes the proof of Theorem 2.

4. The proof of Theorem 3

We start with a couple of well-known facts. For a proof of the Lemma 1 below, we refer the reader to Ribenboim's book [13].

Lemma 1. *The Diophantine equation*

$$X^{2p} + 1 = \delta Y^q \tag{4.1}$$

with $\delta \in \{1, 2\}$ *does not admit any solution in positive integers* (X, Y, p, q) *with* $X > 1$, $Y > 1$ *and* p *and* q *prime numbers.*

We shall also need the following result due to Ljunggren [9].

Lemma 2. *The only solutions of the Diophantine equation*

$$\frac{x^n - 1}{x - 1} = y^2 \tag{4.2}$$

in positive integers $x > 1$, $y > 1$, $n > 2$ *are* $(x, y, n) = (3, 5, 11)$, $(7, 4, 20)$.

Proof of Theorem 3. For any nonnegative integer m we write $u_m = (x^m - 1)/(x - 1)$ and $v_m = x^m + 1$. As in the proof of the Theorem 2, we shall achieve our goal in a few steps. We let $\mathcal{A} = \{n, n + d, \ldots, n + (k-1)d\}$. The Diophantine equation

to be proved impossible is

$$\prod_{j=0}^{k-1} \frac{x^{n+jd}-1}{x-1} = y^q. \tag{4.3}$$

Step 1: Assume that the interval $[0, k-1]$ contains a number i with the following properties:
(1) $n + id > 4$;
(2) $4|n + id$;
(3) either $n + id = 2^\mu$ is a power of 2, and there is no other number $j \neq i$ in the interval $[0, k-1]$ such that $n + jd$ is a multiple of 2^μ, or $Q = P(n + id) > 2$, and $n + id$ is the only positive integer in $\mathcal{A}$ which is a multiple of $4Q$.
Then Eq. (4.3) is impossible.

The argument we shall use here is somewhat similar to the one used in the proof of Theorem 2.

For example, if $n + id = 2^\mu$ is the only number which is a multiple of $2^\mu \geqslant 8$ in $\mathcal{A}$, then Eq. (4.3) can be rewritten as

$$v_{2^{\mu-1}} \cdot u_{2^{\mu-1}} \cdot \prod_{\substack{j\in[0,k-1]\\ j\neq i}} u_{n+jd} = y^m. \tag{4.4}$$

One proves immediately that $\mathrm{ord}_2(v_{2^{\mu-1}}) \leqslant 1$ and that 2 is the only prime which can divide either $\gcd(v_{2^{\mu-1}}, u_{2^{\mu-1}})$ or $\gcd(v_{2^{\mu-1}}, u_{n+jd})$ with some $j \neq i$. Thus, we get that $x^{2^{\mu-1}} + 1 = \delta y_1^q$ holds with $\delta \in \{1, 2\}$ and $y_1 > 1$.

Assume now that $n + id = 2^\mu Q^v m_i$, where $\mu \geqslant 2$, $v \geqslant 1$, m_i is coprime to $2Q$ and $n + id$ is the only multiple of $4Q$ in $\mathcal{A}$. In this case, with $Q_1 = Q^v$, one may rewrite Eq. (4.3) as

$$v_{2^{\mu-1}Q_1} \cdot u_{2^{\mu-1}Q_1} \cdot \left(\frac{u_{n+id}}{u_{2^\mu Q_1}}\right) \cdot \prod_{\substack{j\in[0,k-1]\\ j\neq i}} u_{n+jd} = y^q. \tag{4.5}$$

From the conditions we have imposed on $n + id$ one checks immediately that the only prime number that can divide either one of the following four numbers:

$$\gcd(v_{2^{\mu-1}Q_1}, u_{2^{\mu-1}Q_1}), \quad \gcd\left(v_{2^{\mu-1}Q_1}, \frac{u_{n+id}}{u_{2^\mu Q_1}}\right), \quad \gcd(v_{2^{\mu-1}Q_1}, u_{n+jd}),$$
$$\text{with } j \neq i \in [0, k-1]$$

is 2 (or some of these numbers are 1) and since $\mu \geqslant 2$, we have that $\mathrm{ord}_2(v_{2^{\mu-1}Q_1}) \leqslant 1$. With Eq. (4.5), we get again that there exist integers $\delta \in \{1, 2\}$ and $y_1 > 1$ such that

$$x^{2^{\mu-1}Q_1} + 1 = \delta y_1^q$$

holds.

Thus, we always obtain a diophantine equation of the form $X^{2p}+1=\delta Y^q$ with $\delta\in\{1,2\}$ in positive integers $X>1$ and $Y>1$ and prime numbers p and q and such an equation is impossible by Lemma 1.

Step 2: If the set $\mathcal{A}$ contains a multiple of 4 larger than 4, then the hypotheses from Step 1 are satisfied.

Let $n_1=4n_2$ be the smallest multiple of 4 in $\mathcal{A}$, and let t be the number of multiples of 4 in $\mathcal{A}$. Clearly, these multiples of 4 in $\mathcal{A}$ are precisely $4n_2,\ 4(n_2+d),\ \ldots,\ 4(n_2+(t-1)d)$. If $t=1$, then $n_1>4$ and the hypotheses from Step 1 are satisfied. If $t\geqslant 2$ and $d>1$, then $Q=P(n_2(n_2+d)\ldots(n_2+(t-1)d))>t$, except when $(n_2,d,t)=(2,7,3)$. In this exceptional case, we have that $4(n_2+(t-1)d)=4\cdot 16=2^6$. Thus, the hypotheses from Step 1 are satisfied when $d>1$.

Assume now that $d=1$. If $n_2\geqslant t+1$, then $Q>t$ by Sylvester's Theorem, and so the hypotheses from Step 1 are satisfied. Finally, when $n_2\leqslant t$, then the argument from the beginning of Step 1 of the proof of Theorem 2 shows that the interval $[n_2,\ldots,n_2+t-1]$ contains a unique power of 2 and so the hypothesis from Step 1 are satisfied in this instance as well, which completes the proof of Step 2.

Step 3: The final contradiction.

From Steps 1–2, it follows that the only case in which Eq. (4.3) might have a solution is either when $\mathcal{A}$ does not contain a multiple of 4, or when $4\in\mathcal{A}$ is the only multiple of 4 in $\mathcal{A}$.

Assume first that 4 in $\mathcal{A}$ is the only multiple of 4 in $\mathcal{A}$. Since $n>1$, it follows that either $d>1$ and $n=4$ or $d=1$.

Assume first that $d>1$ and that $n=4$. Clearly, $k\leqslant 4$. Arguments similar to the ones employed before show that $\gcd(v_2,u_2)\mid 2$ and that $\gcd(v_2,u_{n+jd})\mid 2$ for all $j\in[1,k-1]$. Thus, Eq. (4.3) implies that

$$x^2+1=v_2=\delta y_1^q \tag{4.6}$$

holds with some positive integers $\delta\in\{1,2\}$ and $y_1>1$. The case $\delta=1$ does not lead to a solution of Eq. (4.6) while in the case $\delta=2$ only $q=2$ is possible. Since $k\in[2,4]$ and d is odd, it follows easily that u_{4+d} is coprime to u_4, u_{4+d} and to u_{4+3d}, and since we now know that $q=2$, Eq. (4.3) implies an equation of the form

$$u_{4+d}=\frac{x^{4+d}-1}{x-1}=y_2^2, \tag{4.7}$$

with some positive integer y_2. The above equation does not have any positive integer solution (x,d,y_2) and $d\geqslant 3$ by Lemma 2.

We shall now assume that $d=1$. It then follows that $\mathcal{A}\subseteq[2,7]$. Writing $u_4=u_2\cdot v_2$, it follows that we may write Eq. (4.3) as

$$v_2\cdot u_2\cdot\prod_{\substack{j\in[0,k-1]\\ n+j\neq 4}}u_{n+j}=y^q. \tag{4.8}$$

Arguments similar to the ones employed above show once again that $\gcd(v_2, u_{n+j}) \mid 2$ holds for all $n + j \in \mathcal{A}$ distinct from 4 and that $\mathrm{ord}_2(v_2) \leqslant 1$. Thus, Eq. (4.8) implies that Eq. (4.6) must hold, and now we know that the only possibility in Eq. (4.6) is $\delta = q = 2$. Thus, Eq. (4.6) becomes

$$x^2 + 1 = 2y_1^2. \tag{4.9}$$

Since $k \geqslant 2$, it follows that $\mathcal{A}$ contains either the number 5 or 3. If $5 \in \mathcal{A}$, it then follows that $\gcd(u_5, u_{n+j}) = u_{\gcd(5,n+j)} = 1$ holds for all $n + j \neq 5$ in $\mathcal{A}$ and therefore Eq. (4.3) implies that

$$\frac{x^5 - 1}{x - 1} = y_2^2$$

holds with some integer $y_2 > 1$. By Lemma 2, this last equation has only one integer solution (x, y_2) with $x > 1,\ y_2 > 1$, namely $(x, y_2) = (3, 11)$. However, with $x = 3$, Eq. (4.9) becomes $2y_1^2 = 3^2 + 1 = 10$, which is impossible.

Thus, $5 \notin \mathcal{A}$ therefore $3 \in \mathcal{A}$ and $\mathcal{A} \subseteq [2, 4]$. But in this case $3 \in \mathcal{A}$ and $\gcd(u_3, u_{n+j}) = u_{\gcd(3,n+j)} = 1$ holds for all $n + j \neq 3$ in $\mathcal{A}$ therefore Eq. (4.3) implies that

$$x^2 + x + 1 = u_3 = y_3^2 \tag{4.10}$$

holds with some integer $y_3 > 1$. Obviously, Eq. (4.10) does not admit any solution in integers $x > 1,\ y_3 > 1$.

From now on, we assume that $\mathcal{A}$ does not contain any multiple of 4. In particular, $k \in \{2, 3\}$ and if $k = 3$ then $n + d$ is even but not a multiple of 4. Let $i \in [0, k-1]$ be such that $n + id$ is the only even number in $\mathcal{A}$. In this case, u_{n+id} is coprime to u_{n+jd} for all $j \in [0, k-1]$ distinct from i therefore Eq. (4.3) implies that $u_{n+id} = y_1^q$ holds with some integer $y_1 > 1$. Thus, $u_{(n+id)/2} \cdot v_{(n+id)/2} = y_1^q$. Since $(n + id)/2$ is odd, it follows that $u_{(n+id)/2}$ is odd, therefore $u_{(n+id)/2}$ and $v_{(n+id)/2}$ are coprime. Thus, there exists an integer $y_2 > 1$ so that

$$x^{(n+id)/2} + 1 = y_2^q \tag{4.11}$$

holds. Eq. (4.11) is the Catalan equation which has been completely solved by Mihăilescu (see [2]) and its only solution in integers $x_1 > 1,\ y_1 > 1,\ (n + id) > 2$ is $(x, n + id, y_2, q) = (2, 6, 3, 2)$. Assume first that $d > 1$. If $i > 0$, then since $n > 1$ and d is odd, the only possibility would seem to be $d = n = 3$, but this is again not convenient because we are assuming that n and d are coprime. So, $i = 0$ and therefore $n = 6$ and $k = 2$. Moreover, d is coprime to 6 and $q = 2$. We then get that $u_{n+d} = 2^{6+d} - 1$ must be a perfect square and this is impossible for $d \geqslant 5$. Thus, we may assume that $d = 1$. In this case, if $n + i > 2$ then $n + i = 6$. In particular,

either $5 \in \mathcal{A}$ or $7 \in \mathcal{A}$. When $5 \in \mathcal{A}$ we get that u_5 must be a perfect square but $u_5 = 2^5 - 1 = 31$ is not, while when $7 \in \mathcal{A}$ we get that u_7 must be a perfect square but $u_7 = 2^7 - 1 = 127$ is not. Thus, the instance $n + i > 2$ is impossible, and therefore $n + i = 2$ leading to $n = 2,\ i = 0$ and $\mathcal{A} = [2, 3]$. Since u_2 and u_3 are coprime, we get again that u_3 must be a perfect power. Hence, there exists $y_1 > 1$ such that the relation

$$x^2 + x + 1 = u_3 = y_1^q \tag{4.12}$$

holds. The above equation has no integer solutions $x > 1,\ y_1 > 1$ when $q = 2$. When $q > 2$ then, with $x_1 = 2x + 1$, the above Eq. (4.12) can be rewritten as

$$x_2^2 + 3 = 4y_1^q. \tag{4.13}$$

The fact that this equation has no integer solutions with $q \geqslant 5$ is known (see, for example, [5, Corollary 4]), while for $q = 3$ the only solution of Eq. (4.13) with $y_1 > 1$ is $(x_2, y_1) = (37, 7)$ (see, for example, [10]). Thus, we get that $2x + 1 = 37$ therefore $x = 18$, but $u_2 = x + 1 = 19$ is not a perfect cube in this case.

Theorem 3 is therefore completely proved. □

Acknowledgments

This work started when the first author visited the Tata Institute for Fundamental Research in Mumbai, India during the summer of 2001. This author would like to thank the people of this Institute for their warm hospitality as well as the Third World Academy of Sciences for support. Both authors would like to thank the referee for comments which improved the quality of this paper.

References

[1] Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte, J. Reine Angew. Math. 539 (2001) 75–122.
[2] Y. Bilu, Catalan's conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé 909, 55éme année (2002–2003).
[3] Y. Bugeaud, M. Mignotte, *L'*équation de Nagell–Ljunggren $\frac{x^n-1}{x-1} = y^q$, Enseign. Math. 48 (2002) 147–168.
[4] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas powers, Preprint, 2003.
[5] Y. Bugeaud, T.N. Shorey, On the number of solutions of the generalized Ramanujan–Nagell equation, J. Reine Angew. Math. 539 (2001) 55–74.
[6] P. Erdős, J.L. Selfridge, The product of consecutive integers is never a power, Illinois J. Math. 19 (1975) 292–301.
[7] S. Laishram, T.N. Shorey,, Number of prime divisors in a product of consecutive integers, Acta. Arith. 113 (2004) 327–341.

[8] S. Laishram, T.N. Shorey, Number of prime divisors in a product of terms of an arithmetic progression, Indag. Math. (2003) in press.
[9] W. Ljunggren, Some theorems on indeterminate equations of the form $\frac{x^n-1}{x-1} = y^q$ (Norwegian), Norsk Mat. Tidsskr. 25 (1943) 17–20.
[10] F. Luca, On the Diophantine equation $y^2 = 4q^m - 4q^n + 1$, Proc. Amer. Math. Soc. 131 (2003) 1339–1345.
[11] P. Moree, On arithmetical progressions having only few prime factors in comparison with their length, Acta Arith. 70 (1995) 295–312.
[12] A. Pethő, Perfect powers in second order linear recurrences, J. Number Theory 15 (1982) 5–13.
[13] P. Ribenboim, Catalan's Conjecture. Are 8 and 9 the Only Consecutive Powers?, Academic Press, Inc., Boston, 1994.
[14] J.B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64–94.
[15] T.N. Shorey, Applications of linear forms in logarithms to binary recursive sequences, Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Progress of Mathematics, vol. 38, Birkhäuser, Boston, 1983, pp. 287–301.
[16] T.N. Shorey, Exponential Diophantine equations involving products of consecutive integers and related equations, in: R.P. Bambah, V.C. Dumir, R.J. Hans-Gill (Eds.), Number Theory, Hindustan Book Agency, 1999, pp. 463–495.
[17] T.N. Shorey, Powers in arithmetic progression, in: A Panorama of Number Theory or the View from Baker's Garden (Zürich, 1999), Cambridge University Press, Cambridge, 2002, pp. 325–336.
[18] T.N. Shorey, C.L. Stewart, On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, Math. Scand. 52 (1983) 24–36.
[19] T.N. Shorey, R. Tijdeman, Exponential Diophantine Equations, Cambridge University Press, Cambridge, 1986.
[20] T.N. Shorey, R. Tijdeman, On the greatest prime factor of an arithmetical progression, in: A tribute to Paul Erdős, Cambridge University Press, Cambridge, 1990, pp. 385–389.