Products of members of Lucas sequences with indices in an interval being a power

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

T.N. Shorey
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai, 400005, India
shorey@math.tifr.res.in

October 4, 2007

1 Introduction

Let r and s be coprime nonzero integers with $\Delta = r^2 + 4s \neq 0$. Let α and β be the roots of the quadratic equation

$$x^2 - rx - s = 0,$$

and assume that α/β is not a root of 1. We make the convention that $|\alpha| \geq |\beta|$. Put $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ for the Lucas sequences of the first and second kind of roots α and β whose general terms are given by

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

respectively. Interesting examples of Lucas sequences of the first kind include the Fibonacci sequence $(F_n)_{n\geq 0}$, the sequence of Mersenne numbers $(M_n)_{n\geq 0}$ of general term $M_n = 2^n - 1$ which has roots $(\alpha, \beta) = (2, 1)$, as well as the sequence of rep-units in base x (here, $x > 1$ is an integer) of general term $u_n = (x^n - 1)/(x - 1)$ which has roots $(\alpha, \beta) = (x, 1)$. The Lucas sequence of the second kind obtained for $(r, s) = (1, 1)$ (which is, unfortunately, also known as the *Lucas sequence*) is denoted by $(L_n)_{n\geq 0}$ and is sometimes referred to as the *companion* of the Fibonacci sequence.

Given a Lucas sequence $(u_n)_{n\geq 0}$ or $(v_n)_{n\geq 0}$, Pethő [16], and independently Shorey and Stewart [20], showed that there are only finitely many of its terms that can be perfect powers of exponent > 1 and they are, in principle, effectively computable. Effectively computing them for any given pair (r, s) can be a difficult task, although recently all the perfect powers in the Fibonacci sequence, Lucas sequence and a few others were completely determined (see [4], [5] and [6]).

Inspired by the celebrated result of Erdős and Selfridge [9] to the effect that the product of two or more consecutive integers is never a power, we investigated in previous papers analogues of this problem where the consecutive integers are replaced by consecutive members of a Lucas sequence. For example, in [14], we showed that the Diophantine equation

$$\prod_{i=0}^{k-1} u_{n+i} = y^{\ell}, \tag{1}$$

in integers $n \geq 1, k \geq 2, \ell \geq 2$ and y has only finitely many effectively computable solutions (n, k, ℓ, y). The same result applies when $(u_n)_{n\geq 0}$ is replaced by $(v_n)_{n\geq 0}$. When $u_n = F_n$ or $u_n = (x^n - 1)/(x - 1)$ with any integer $x > 1$, these equations have no such solutions. In [7], it was shown that if $\mathcal{S}$ is any finite set of primes, then there exists a finite set $\mathcal{T}$ of positive integers, depending on $\mathcal{S}$ and the sequence $(u_n)_{n\geq 0}$, such that if

$$\prod_{i=1}^{t} u_{n_i} = by^{\ell} \tag{2}$$

holds with integers $n_1, \ldots, n_t, y$, $\ell > t$ prime and b an integer all whose prime factors are in $\mathcal{S}$, then $n_i \in \mathcal{T}$ for all $i = 1, \ldots, t$. The method presented in [7] is elementary once all the perfect powers in the sequence $(u_n)_{n\geq 0}$ are known,

so as an application $\mathcal{T}$ was computed for the case of $u_n = F_n$ when $\mathcal{S}$ is the set consisting of the first 100 primes.

In this paper, we look again at equation (2) but we remove the restriction that $\ell > t$. However, we ask of the integers $n_1, \ldots, n_t$ to be distinct and close together. More precisely, from now on, we consider equation (2) when $0 < n_1 < n_2 < \cdots < n_t$ are integers in $[n, n+k-1]$ and $P(b) \leq k$, where for a non-zero integer m we write $P(m)$ for the largest prime factor of m with the convention that $P(\pm 1) = 1$. We search for a function $f(k) < k$ for which we can guarantee that equation (2) with $t = f(k)$ has no solution whenever k exceeds a sufficiently large number depending on the sequence $(u_n)_{n\geq 0}$. We note that the variant of this problem with the sequence $(u_n)_{n\geq 0}$ replaced by the linear function n was first investigated by Erdős [8] and we refer to [19] for an account on improvements on this result. In what follows, $c_0,\ c_1,\ \ldots$ are effectively computable positive constants which might depend on our sequence $(u_n)_{n\geq 0}$.

Our first and main result is the following.

Theorem 1. *Let $(u_n)_{n\geq 0}$ be a Lucas sequence of the first kind. There exist numbers $c_0 > 0$ and c_1 such that (2) with*

$$t \geq k - c_0 \frac{k \log\log k}{\log k} \tag{3}$$

implies that $\max\{|b|, k, \ell, n, |y|\} \leq c_1$.

The proof Theorem 1 depends on explicit estimates for the size of the $\mathcal{S}$-integer solutions of super and hyper-elliptic Diophantine equations obtained via the theory of linear forms in logarithm, lower bounds for the number of primes in short intervals, as well as combinatorial techniques of Sylvester and Erdős.

Acknowledgements. The first author worked on this paper during Summer of 2007 when he visited the Tata Institute for Fundamental Research in Mumbai, India with a TWAS Associateship. He thanks the people of that institute for their hospitality and the TWAS for support.

2 Proof of Theorem 1

The proof is a combination between a statement concerning the finiteness of the number of solutions of a certain Diophantine equation together with a

counting argument to bound from below the number of integers in an interval of length k without divisors of a certain shape.

3 Diophantine considerations

We start with the Diophantine part. Let us introduce some notation. For a positive integer n we write $\Phi_n(X) \in \mathbb{Z}[X]$ for the nth cyclotomic polynomial and $\Phi_n(X,Y) \in \mathbb{Z}[X,Y]$ for its homogenization

$$\Phi_n(X,Y) = \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (X - e^{2\pi ik/n}Y).$$

We know that $\Phi_n(\alpha,\beta)$ is an integer which divides u_n. Furthermore, we can write $\Phi_n(\alpha,\beta) = A_nB_n$, say, where B_n is the largest divisor of $\Phi_n(\alpha,\beta)$ such that all its prime factors are primitive for u_n; that is, they divide u_n but no u_m for $0 < m < n$, and A_n is small. In fact, for $n \ge 13$, we certainly have that $A_n \mid n$ (see, for example, Theorem 2.4 in [2]).

Lemma 1. *There exists positive computable numbers c_2, c_3 and c_4 depending on the sequence $(u_n)_{n\ge 0}$ such that equation (2) with $k > c_4$ implies the following:*

(i) $P(n_i) \le (k+1)/2$ *for all* $i = 1,\dots,t$.

(ii) Suppose that n_i with $1 \le i \le t$ has a divisor of the form pq, where q is odd and $p = P(n_i/q)$. Then

$$2dp+1 \text{ or } 2dp-1 \text{ is a prime for some integer } 1 \le d < q, \tag{4}$$

when

$$pq > (k+1)/2 \tag{5}$$

and

$$c_2 < q < c_3(\log k)^{1/15}/\log\log k. \tag{6}$$

Proof. We assume (2) with $k \ge c_4$, where c_4 is some large number to be specified later. We assume that n_i has a divisor of the form pq with $pq > (k+1)/2$ for some $i \in \{1,\dots,t\}$. We show that this is not possible when $q = 1$. Further, we obtain (4) whenever (6) holds.

Let $q < z$. Since $pq > (k+1)/2$, it follows that at most two of the numbers n_i for $i \in \{1, \ldots, k\}$ are multiples of pq. First we assume that there is only one, which we write as $n_i = pqm$. We rewrite (2) as

$$u_p \left(\frac{u_{n_i}}{u_p} \right) \prod_{j \neq i} u_{n_j} = by^\ell,$$

when $q = 1$, and as

$$B_{pq} \left(\frac{u_{pq}}{B_{pq}} \right) \left(\frac{u_{n_i}}{u_{pq}} \right) \prod_{j \neq i} u_{n_j} = by^\ell, \tag{7}$$

when $q > 1$. When $q = 1$, the primes dividing u_p do not divide u_{n_j} for any $j \neq i$. If some prime P divides u_p and u_{n_i}/u_p, then it must divide n_i/p. Indeed, more generally, if $a \mid b$, then all prime factors of $\gcd(u_a, u_b/u_a)$ divide b/a. Thus, $P \leq P(n_i) = p$ giving $P = p$ since $P \equiv 0, \pm 1 \pmod{p}$. Thus, $p \mid u_p$, and so $p \mid \Delta$. But this is not possible since $p > (k+1)/2$ and c_6 is sufficiently large. Hence, $u_p = \pm y_1^\ell$, implying that p is bounded by a number depending only on the sequence $(u_n)_{n \geq 0}$. This is again not possible.

Thus, from now on, we will assume that $q > 1$, and $p \leq (k+1)/2$ provided that there is only one value for i such that $pq \mid n_i$.

We next look at the primes dividing B_{pq}. Let P be such a prime. Such primes are primitive; i.e., do not divide u_m for any positive integer $m < pq$. Since P is primitive, it follows that $P \equiv \pm 1 \pmod{pq}$. Since pq is odd, we have $P \geq 2pq - 1 > k$, therefore P does not divide b. Further, $P \nmid u_{n_j}$ for $j \neq i$ because n_j is not a multiple of pq, and also $P \nmid u_{n_i}/u_{pq}$, because otherwise since $P \mid u_{pq}$ we would get again that $P \mid n_i/pq$, therefore $P \leq P(n_i/q) = p$, which is false. Thus, the primes in B_{pq} must appear at exponents which are multiples of ℓ, and we conclude that $\pm B_{pq}$ is a perfect ℓ-th power. Since

$$\Phi_{pq}(X, Y) = \frac{\Phi_q(X^p, Y^p)}{\Phi_q(X, Y)},$$

we get the Diophantine equation

$$\Phi_q(\alpha^p, \beta^p) = \pm A_{pq} \Phi_q(\alpha, \beta) y_1^\ell, \tag{8}$$

with some positive integer y_1. We know that $A_{pq} \mid pq$. We next show that $A_{pq} \mid q$. Indeed, assume otherwise. Then $p \mid A_{pq}$. Let d be some proper

divisor of pq such that $p \mid u_d$. Then $p \mid \gcd(u_d, u_{pq}/u_d)$, therefore $p \mid pq/d$. If $p \mid d$, then the above relation gives $p \mid q$, and since $k/z \ll p \ll z$, this is impossible when $z = o(k^{1/2})$ as $k \to \infty$, which will be the case. Thus, $d \mid q$, giving $p \mid u_q$ and hence,

$$p \le |u_q| = \exp(O(q)) = \exp(O(z)) = o(k/z) = o(p) \qquad \text{as } k \to \infty$$

provided that $z = o(\log k)$ as $k \to \infty$, which will be the case. Hence, A_{pq} is some divisor of q.

A similar conclusion is reached for the instance when there are two values $i < j$ in $\{1, \dots, t\}$ such that $pq \mid n_i$ and $pq \mid n_j$. Let us explain some of the details of this deduction. In this case, both $n_i = pqm$ and $n_j = pq(m+1)$ hold with some positive integer m, and one of m and $m+1$ is even. Assume say that m is even. Write $m = 2^\gamma pqm_1$, where $\gamma \ge 1$ and m_1 is odd. Assume again that $p = P(n_i/q)$. In this case, we have the relation

$$u_{n_i} = u_{2^\gamma pqm_1} = u_{2^\gamma pq} \left(\frac{u_{2^\gamma pqm_1}}{u_{2^\gamma pq}} \right) = v_{pq} u_{pq} \left(\prod_{\delta=1}^{\gamma-1} v_{2^\delta pq} \right) \left(\frac{u_{2^\gamma pqm_1}}{u_{2^\gamma pq}} \right).$$

We put $w_n = v_n/v_1$. This is an integer when n is odd. In fact, for odd n it coincides with the nth term of the Lehmer sequence of roots $(\alpha, -\beta)$ whose general term is given by $w_n = (\alpha^n + \beta^n)/(\alpha + \beta) = v_n/v_1$ when n is odd and $w_n = (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) = u_n/v_1$ when n is even. The Lehmer sequences share the same nice divisibility properties as the Lucas sequences. In particular, for odd n, $\Phi_n(\alpha, -\beta) = C_n D_n$ is a divisor of w_n, where D_n is divisible only by primitive primes for w_n, and C_n is small; in particular, $C_n \mid n$ for all $n \ge 13$. With these remarks, we get either

$$\left(\frac{v_p}{v_1} \right) v_1 u_p \left(\prod_{\delta=1}^{\gamma-1} v_{2^\delta p} \right) \left(\frac{u_{2^\gamma n_i}}{u_{2^\gamma p}} \right) \prod_{j \ne i} u_{n_j} = by^\ell, \tag{9}$$

when $q = 1$, or

$$D_{pq} \left(\frac{u_{pq}}{D_{pq}} \right) \left(\prod_{\delta=1}^{\gamma-1} v_{2^\delta pq} \right) \left(\frac{u_{2^\gamma pqm_1}}{u_{2^\gamma pq}} \right) \prod_{j \ne i} u_{n_j} = by^\ell, \tag{10}$$

when $q \ne 1$. When $q = 1$ and k is large, we have that $\gcd(v_p/v_1, u_m)$ is 1 unless $p \mid m$ and m/p is even. In particular, v_p/v_1 is coprime to u_{n_j} for

$j \neq i$. Furthermore, $\gcd(v_p/v_1, u_p) = \gcd(v_p, v_{2^\delta p}) = 1$ for all $\delta > 1$, when $p > 3$. Moreover, $\gcd(v_p/v_1, u_{2^\gamma pm_1}/u_{2^\gamma p})$ divides pm_1. For large k, all prime factors of v_p/v_1 are congruent to $\pm 1 \pmod p$, so in particular they are at least $2p - 1 > P(m)$, therefore v_p/v_1 and $u_{2^\gamma pm_1}/u_{2^\gamma p}$ are coprime. Now equation (9) leads easily to the conclusion that $v_p/v_1 = \pm y_1^\ell$, which has only finitely many effectively computable solutions p, so it does not hold. Thus, again it is not possible that $p > (k+1)/2$ in the case when $q = 1$ and there exist $i < j$ with pq dividing both n_i and n_j. Up to now, we dealt with condition (i), so from now on we assume that $q > 1$ in both cases when pq divides only one or two of the n_i's. Furthermore, continuing the argument when there are two values of the n_i's divisible by pq, one sees that divisibility arguments similar to the ones used above applied to equation (10) lead to the conclusion that $\pm D_{pq}$ is an ℓth power of an integer, which is an analogous equation to (8), namely

$$\Phi_q(\alpha^p, -\beta^p) = \pm \Phi_q(\alpha, -\beta) C_{pq} y_1^\ell, \tag{11}$$

where C_{pq} is some divisor of q.

The next step is to bound ℓ. For this, we use a combinatorial argument. Let $\mathcal{I} = \{j : p \mid n_j\}$. Rewrite equation (2) as

$$u_p^{\#\mathcal{I}} \prod_{j \in \mathcal{I}} \left(\frac{u_{n_j}}{u_p} \right) \prod_{j \notin \mathcal{I}} u_{n_j} = b y^\ell. \tag{12}$$

Let P be any prime factor of u_p. Clearly, $P \geq 2p - 1$. If $P \mid u_{n_j}$ for some $j \in \{1, \ldots, t\}$, then certainly $j \in \mathcal{I}$. If additionally $P \mid u_{n_j}/u_p$, then $P \mid n_j/p$. But by (i), $P \leq (k+1)/2$. Assume in fact even less, namely that $P \leq k$. Since $P \equiv \pm 1 \pmod p$, we get that $P = 2dp \pm 1 \leq k$, leading to $d \leq (k+1)/(2p) < q$. Since we are assuming that (4) fails, we conclude that P could not have divided n_j/p for any $j \in \mathcal{I}$. In conclusion, equation (12) together with the fact that all prime factors of u_p are $> k$ leads again to the conclusion that $(u_p)^{\#\mathcal{I}} = \pm y_2^\ell$. Since ℓ is prime, we have that $\ell \leq \#I$ unless $u_p = \pm y_3^\ell$, which is not the case for large values of k. Thus, we deduce that $\ell \leq \#\mathcal{I} \leq k/p + 1 < 2z + 1$, since $p > (k+1)/(2q) \geq (k+1)/(2z)$.

For the last step, we give a lower bound for z. For this we shall treat in detail only the case of equation (8) (i.e., when $pq \mid n_i$ for only one value for i), since the case of equation (11) is entirely similar. For the beginning, we

follow Baker's arguments from [1]. We rewrite equation (8) as

$$\prod_{j=1}^{\phi(q)}(\alpha^p - e_j\beta^p) = \pm A_{pq}\Phi_q(\alpha,\beta)y_1^\ell, \tag{13}$$

where $e_1,\ldots,e_{\phi(q)}$ are all the primitive roots of unity of order q. Let $\mathbb{K} = \mathbb{Q}[\alpha, e^{2\pi i/q}]$. Passing to ideals in $\mathcal{O}_\mathbb{K}$ in equation (13) we get

$$(\alpha^p - e_1\beta^p)\mathcal{O}_\mathbb{K} = IJ^\ell, \tag{14}$$

where $I = I'I''$, with $I' \mid A_{pq}\Phi_q(\alpha,\beta)$ and I'' is an ideal whose prime factors divide $\prod_{2\le j\le\phi(q)}(e_j - e_1)$ and whose exponents are $\le \ell - 1$. In particular,

$$N_{\mathbb{K}/\mathbb{Q}}(I') \le |A_{pq}\Phi_q(\alpha,\beta)|^{[\mathbb{K}:\mathbb{Q}]} \le \exp(O(z^2\log z)),$$

and

$$N_{\mathbb{K}/\mathbb{Q}}(I'') \le |\Delta(\mathbb{K})|^\ell \le \exp(O(z^2\log z)),$$

therefore

$$N_{\mathbb{K}/\mathbb{Q}}(I) = N_{\mathbb{K}/\mathbb{Q}}(I'I'') = N_{\mathbb{K}/\mathbb{Q}}(I')N_{\mathbb{K}/\mathbb{Q}}(I'') \le \exp(O(z^2\log z)).$$

Here and in what follows, we use $\Delta(\mathbb{K})$ for the discriminant of the number field $\mathbb{K}$. We let I_1 and J_1 be ideals which are inverses of I and J, respectively, in the ideal class group of $\mathbb{K}$. It is known that they can be chosen such that both $N_{\mathbb{K}/\mathbb{Q}}(I_1)$ and $N_{\mathbb{K}/\mathbb{Q}}(J_1)$ do not exceed $|\Delta(\mathbb{K})|^{1/2} = \exp(O(z\log z))$. Multiplying equation (14) by $I_1J_1^\ell$, we get

$$(I_1J_1^\ell)(\alpha^p - e_1\beta^p)\mathcal{O}_\mathbb{K} = (II_1)(JJ_1)^\ell.$$

Let $II_1 = \eta\mathcal{O}_\mathbb{K}$ and $JJ_1 = \zeta\mathcal{O}_\mathbb{K}$. Note that $I_1J_1^\ell$ is principal and write $I_1J_1^\ell = \eta_1\mathcal{O}_\mathbb{K}$. Then

$$N_{\mathbb{K}/\mathbb{Q}}(\eta) = N_{\mathbb{K}/\mathbb{Q}}(II_1) = N_{\mathbb{K}/\mathbb{Q}}(I)N_{\mathbb{K}/\mathbb{Q}}(I_1) = \exp(O(z^2\log z)), \tag{15}$$

and

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}(\eta_1) &= N_{\mathbb{K}/\mathbb{Q}}(I_1J_1)^\ell = N_{\mathbb{K}/\mathbb{Q}}(I_1)N_{\mathbb{K}/\mathbb{Q}}(J_1)^\ell \le |\Delta(\mathbb{K})|^{(\ell+1)/2} \\ &= \exp(O(z^2\log z)). \end{aligned} \tag{16}$$

Passing to elements we get that

$$\eta_1\alpha^p - \eta_1 e_1\beta^p = \eta\rho\zeta^\ell, \tag{17}$$

where ρ is a unit in $\mathcal{O}_\mathbb{K}$. Furthermore, up to replacing ζ by one of its associates, we may assume that $\rho = \varepsilon\rho_1^{\ell_1}\cdots\rho_r^{\ell_r}$, where ε is a root of unity in $\mathbb{K}$, $\rho_1, \ldots, \rho_r$ are a system of fundamental units in $\mathcal{O}_\mathbb{K}$ and $\ell_1, \ldots, \ell_r$ are nonnegative integers $\leq \ell - 1$. Note that $r = O(z)$. The same argument leads also to the relation

$$\eta_2\alpha^p - \eta_2 e_2\beta^p = \eta'\rho'\zeta'^\ell, \tag{18}$$

where η' and η_2 satisfy the same inequalities (15) and (16) as η and η_1, respectively. Algebraic manipulations with equations (17) and (18) show that

$$\begin{array}{rcl} \delta_1\beta^p & = & \gamma_1\zeta^\ell - \lambda_1\zeta'^\ell, \\ \delta_2\alpha^p & = & \gamma_2\zeta^\ell - \lambda_2\zeta'^\ell, \end{array} \tag{19}$$

where

$$\left\{\begin{array}{ll} \delta_1 & = \eta_1\eta_2(e_2 - e_1), \\ \delta_2 & = \eta_1\eta_2(e_2^{-1} - e_1^{-1}), \end{array}\right. \quad \left\{\begin{array}{ll} \gamma_1 & = \eta\eta_2\rho, \\ \gamma_2 & = -\eta\eta_2\rho e_1^{-1}, \end{array}\right. \quad \left\{\begin{array}{ll} \lambda_1 & = \eta'\eta_1\rho', \\ \lambda_2 & = -\eta'\rho'\eta_1 e_2^{-1}. \end{array}\right.$$

We multiply the two relations (19) and get

$$-\delta_1\delta_2 s^p = (\alpha\beta)^p = F(\zeta, \zeta'). \tag{20}$$

where

$$F(X, Y) = (\gamma_1 X^\ell - \lambda_1 Y^\ell)(\gamma_2 X^\ell - \lambda_2 Y^\ell) \in \mathcal{O}_\mathbb{K}[X, Y]$$

is a homogeneous form of degree $2\ell \geq 4$. It is easy to check that $F(X, Y)$ splits into non-proportional linear factors over $\mathbb{C}[X, Y]$. Indeed, if not, it would then follow that $\gamma_1/\lambda_1 = \gamma_2/\lambda_2$, leading to $e_1 = e_2$, which is not the case. Let $m = \lfloor p/4\ell \rfloor$, write $p = 4\ell m + t$, where $t \leq 4\ell = O(z)$ and put $\zeta_1 = \zeta s^{-m\ell}$, $\zeta_1' = \zeta' s^{-m\ell}$. Then equation (20) implies that

$$-\delta_1\delta_2 s^t = F(\zeta_1, \zeta_1'). \tag{21}$$

Let $\mathcal{S}$ be the finite set of valuations of $\mathbb{K}$ consisting of all the infinite ones together with the ones such that $|s|_\mu \neq 1$. Then ζ_1, ζ_1' are $\mathcal{S}$-integers in $\mathbb{K}$. Let $h(\bullet)$ be the absolute logarithmic height as defined in Section 4 in [11].

It is known that for every algebraic integer τ of degree d, putting $\mathbb{L} = \mathbb{Q}[\tau]$, the inequality

$$h(\tau) \leq \frac{\log(N_{\mathbb{L}/\mathbb{Q}}(\tau))}{d} + \exp(O(d \log d))|\Delta(\mathbb{L})|^{1/2}(\log \Delta_{\mathbb{L}})^{[\mathbb{L}:\mathbb{Q}]} \qquad (22)$$

holds (see, for example, Lemma 1 in [17]). Thus, by inequalities (15) and (16), we have that

$$\begin{aligned} h(-\delta_1\delta_2 s^t) &\leq h(\delta_1) + h(\delta_2) + O(t+z) \leq 2h(\eta_1) + 2h(\eta_2) + O(z) \\ &= \exp(O(z^2 \log z)). \end{aligned}$$

Furthermore, it is also known that a system of fundamental units $\rho_1, \ldots, \rho_r$ of $\mathbb{K}$ can be chosen such that

$$h(\rho_i) \leq \exp(O(z \log z))|\Delta(\mathbb{K})| = \exp(O(z \log z))$$

(see [10]), therefore, by estimate (22), the coefficients of the polynomial $F(X,Y) \in \mathcal{O}_{\mathbb{K}}(X,Y)$ have absolute logarithmic heights $\leq \exp(O(z^2 \log z))$. Let $\mathbb{L} = \mathbb{K}[\gamma_1^{1/\ell}, \lambda_1^{1/\ell}, \gamma_2^{1/\ell}, \lambda_2^{1/\ell}, e^{\pi i/\ell}]$. We next find an upper bound for the degree and discriminant of $\mathbb{L}$. We note that $\mathbb{L}$ is obtained by adjoining to $\mathbb{K}$ five numbers of the form $\tau_j^{1/\ell}$, where each of τ_j is of degree at most $O(z^3)$ over $\mathbb{Q}$ and $N_{\mathbb{K}/\mathbb{Q}}(\tau_j) \leq \exp(O(z^2 \log z))$. Here, we take $\tau_0 = e^{\pi i/\ell}$, $\tau_1 = \gamma_1,\ \tau_2 = \gamma_2,\ \tau_3 = \lambda_1, \tau_4 = \lambda_2$. Thus, $\mathbb{L}_j = \mathbb{Q}[\tau_j^{1/\ell}]$ is of degree $O(z^3)$ for $j = 0, \ldots, 4$, and has discriminant dividing the discriminant of the polynomial

$$\prod_{\mu=1}^{\ell} \prod_{\nu=1}^{[\mathbb{K}:\mathbb{Q}]} (X - (\tau_j^{(\nu)})^{1/\ell} e^{2\pi i \mu/\ell}) \in \mathbb{Z}[X],$$

which is a divisor of

$$N_{\mathbb{K}/\mathbb{Q}}(\tau_j)^{\ell} \Delta(\mathbb{L}_0)^{[\mathbb{K}:\mathbb{Q}]} \leq \exp(O(z^3 \log z)).$$

We record this as,

$$|\Delta(\mathbb{L}_j)| \leq \exp(O(z^3 \log z)) \qquad \text{for } j = 1, \ldots, 4.$$

In particular, by estimate (22), we also have

$$h(\tau_j) \leq \exp(O(z^3 \log z)) \qquad \text{for } j = 1, 2, 3, 4.$$

Furthermore, since $\tau_0 = e^{\pi i/\ell}$, we have that in fact $[\mathbb{L}_0 : \mathbb{Q}] = O(z)$, $|\Delta(\mathbb{L}_0)| = \exp(O(z \log z))$, and $h(\tau_0) \leq \exp(O(z \log z))$. Putting $\mathbb{M}_0 = \mathbb{K}\mathbb{L}_0$, and $\mathbb{M}_j = \mathbb{M}_{j-1}\mathbb{L}_j$ for $i = j, \ldots, 4$, we get that $[\mathbb{M}_0 : \mathbb{Q}] = O(z^3)$ and

$$[\mathbb{M}_j : \mathbb{Q}] \leq [\mathbb{M}_j : \mathbb{M}_{j-1}][\mathbb{M}_{j-1} : \mathbb{Q}] \leq [\mathbb{L}_j : \mathbb{Q}][\mathbb{M}_{j-1} : \mathbb{Q}] \qquad \text{for } j = 1, 2, 3, 4.$$

Recursively, we get that $[\mathbb{M}_j : \mathbb{Q}] = O(z^{3(j+1)})$ for $j = 0, \ldots, 4$. In particular, since $\mathbb{M}_4 = \mathbb{L}$, we get that $[\mathbb{L} : \mathbb{Q}] = O(z^{15})$. Furthermore, using known inequalities for discriminants of composite fields (see, for example, Proposition 4.9 of [15]), we have

$$|\Delta(\mathbb{M}_0)| \leq |\Delta(\mathbb{K})|^{\ell-1}|\Delta(\mathbb{L}_0)|^{[\mathbb{K}:\mathbb{Q}]} = \exp(O(z^3 \log z)).$$

Using the fact that

$$|\Delta(\mathbb{M}_j)| \leq \Delta(\mathbb{M}_{j-1})^{[\mathbb{L}_j:\mathbb{Q}]}\Delta(\mathbb{L}_j)^{[\mathbb{M}_{j-1}:\mathbb{Q}]} \leq |\Delta(\mathbb{M}_{j-1})|^{O(z^3)} \exp(O(z^{3(j+1)} \log z))$$

recursively, one gets that

$$|\Delta(\mathbb{M}_j)| \leq \exp(O(z^{3(j+1)} \log z))$$

for $j = 0, \ldots, 4$. In particular, $|\Delta(\mathbb{L})| = \exp(O(z^{15} \log z))$.

We now have all the ingredients we need to apply known bounds for solutions of Thue equations whose indeterminantes are $\mathcal{S}$-units. The most recent effective results here are due to Győry and Yu [11]. For example, in our setup, bound (12) from [11] tells us that all solutions of equation (21) have

$$\max\{h(\zeta_1), h(\zeta_1')\} \ll \exp(d \log d)|\Delta(\mathbb{L})|^{5/2}(\log \Delta)^{5d} A,$$

where $d = [\mathbb{L} : \mathbb{Q}]$ and A is an upper bound for both the absolute logarithmic height of the number appearing in the left hand side of equation (21) as well as of the absolute logarithmic heights of the coefficients of $F(X, Y) \in \mathbb{K}[X, Y]$. From our estimates above, it follows that the right hand side of the last expression above is $\exp(O(z^{15} \log z))$. In particular, $h(F(\zeta_1, \zeta_1')) = \exp(O(z^{15} \log z))$ as well, and since $\max\{h(\delta_1), h(\delta_2)\} = \exp(O(z^2 \log z))$, we get from formulas (19) that both $h(\alpha^p)$ and $h(\beta^p)$ are of sizes not exceeding $\exp(O(z^{15} \log z))$. Since at least one of α and β is not a root of unity, we get that $\max\{h(\alpha^p), h(\beta^p)\} \gg p$. Thus, we arrived at $p \leq \exp(O(z^{15} \log z))$. Since $p \gg k/z$, we get that

$$\frac{k}{z} \leq \exp(O(z^{15} \log z));$$

hence, $z \gg (\log k)^{1/15}/\log\log k$, which is what we wanted. This completes the proof of Lemma 1. $\square$

4 Integers with restricted divisors in short interval

We assume that (2) and (3) hold with some c_0 to be chosen later. We keep the notation $z = c_3(\log k)^{1/15}/\log\log k$ of the preceding section. Here, we complete the proof of Theorem 1. We treat various ranges of n versus k.

4.1 The range $n \in [1, k^{3/2}]$

Assume first that $n \in [1, k/2]$. In this case, the interval $\mathcal{K} = ((k+1)/2, k]$ is contained in $[n, \ldots, n+k-1]$. We next find a lower bound for the number of numbers $pq \in \mathcal{K}$ with p prime and $q \in [c_2, z]$. Fix q. Then $p \in ((k+1)/(2q), k/q]$. Thus, the number of choices for p is

$$\begin{aligned}\pi(k/q) - \pi((k+1)/(2q)) &= (1+o(1))\left(\frac{k}{q\log(k/q)} - \frac{(k+1)}{2q\log((k+1)/(2q))}\right)\\ &= (1/2+o(1))\frac{k}{q\log k}\end{aligned}$$

as $k \to \infty$ because $\log(k/q) = (1+o(1))\log k$ when $q \le z$. Hence, the number of the above pairs of primes (p, q) is at least

$$(1/2+o(1))\frac{k}{\log k}\sum_{c_2 \le q \le z}\frac{1}{q} = (1/2+o(1))\frac{k\log z}{\log k} = (1/30+o(1))\frac{k\log\log k}{\log k}. \tag{23}$$

Each one of these pairs creates a number $pq \in ((k+1)/2, k]$ and each such number comes from a unique pair when k is large since $p > (k+1)/(2q) > (k+1)/(2z) > z$.

When $n \in [k/2, k^{3/2}]$, we fix again a number $q \in [c_2, z]$ and we count the number of primes $p \in [n/q, (n+k)/q)$. By standard estimates concerning primes in short intervals (see [13]), we have that the number of such primes is

$$\pi((n+k)/q) - \pi(n/q) \gg \frac{\pi(k)}{q} \tag{24}$$

and the remaining of the argument is similar to the argument used in the range $n \in [1, k/2]$.

In particular, when $n \in [1, k^{2/3}]$, we have

$$\#\{m = pq \in [n, n+k] : m \text{ satisfies (5) and (6) of Lemma 1}\} \gg \frac{k \log\log k}{\log k}. \tag{25}$$

From the totality of the integers pq that we have created, we may have to remove some of them because of the condition (ii) of Lemma 1. To deal with this condition, let $\mathcal{P}$ be the set of primes p such that $2pd \pm 1$ is a prime for some $d \le z$. For a real number $t > 1$ we put $\mathcal{P}(t) = \mathcal{P} \cap [1, t]$. Assume that $p \in \mathcal{P}(t)$. Then there is $d \le z$ such that $2pd \pm 1$ is prime. With a fixed value of d, we have that the linear forms p and $2pd \pm 1$ are both primes. By the Brun sieve (see, for example, Theorem 2.3 in [12]), the number of such primes $p \le t$ is

$$\ll \frac{d}{\phi(d)} \frac{t}{(\log t)^2}.$$

Summing this up over all values of $d \le z$, we get that

$$\#\mathcal{P}(t) \ll \frac{t}{(\log t)^2} \sum_{d \le z} \frac{d}{\phi(d)} \ll \frac{tz}{(\log t)^2}$$

(see, for example, [18] for the last estimate above). By applying the Abel summation formula, we deduce that uniformly for $1 < a \le b$, we have

$$\begin{aligned} \sum_{\substack{p \in \mathcal{P} \\ a < p \le b}} \frac{1}{p} &= \int_a^b \frac{d(\#\mathcal{P}(t))}{t} \ll \left(\frac{\#\mathcal{P}(t)}{t} \Big|_{t=a}^{t=b} \right) + \int_a^b \frac{\#\mathcal{P}(t)}{t^2} \\ &\ll \frac{z}{(\log a)^2} + \int_a^b \frac{z dt}{t(\log t)^2} \ll z \left(\frac{1}{(\log a)^2} + \left(\frac{1}{\log t} \Big|_{t=a}^{t=b} \right) \right) \\ &\ll z \frac{(1 + \log(b/a))}{(\log a)^2}. \end{aligned} \tag{26}$$

We now return to the set of numbers $pq \in [n, n+k-1]$ that we have created. According to Lemma 1, none of the indices n_i participating in equation (2) can equal one of these numbers unless $p \in \mathcal{J} = ((k+1)/(2z), (k+1)/2]$ and $p \in \mathcal{P}$. For each such p, the number of $m \in [n, n+k-1]$ which are divisible by p is at most $k/p + 1 \le 2k/p$. Thus, the total number of such integers m

is bounded above by

$$\begin{aligned} \leq \sum_{\substack{p\in\mathcal{P}\\ p\in\mathcal{J}}} \frac{2k}{p} &\ll kz\frac{1+\log(2z)}{(\log((k+1)/(2z)))^2} \ll \frac{k}{(\log k)^{23/12}} \\ &= o\left(\frac{k\log\log k}{\log k}\right), \qquad \text{as } k\to\infty, \end{aligned} \tag{27}$$

where in the above estimates we used the estimate (26) with the parameters $a=(k+1)/(2z)$ and $b=(k+1)/2$. By (25) and (27), we see that there are at least $c_5 k\log\log k/\log k$ integers n_i satisfying the assumptions (5), (6) of Lemma 1 (ii) which do not satisfy (4) of Lemma 1 (ii), where c_5 is a positive constant. We see from Lemma 1 (ii) that these n_i do not participate in (2). This is not possible by (3) with $c_0=c_5$.

4.2 The range $n > k^{3/2}$

This is easy. Let $\mathcal{N}=\{n_1,\dots,n_t\}$. We remove some numbers from $\mathcal{N}$ as follows. For each $p\leq k$ let $i_p\in\{1,\dots,t\}$ be such that the exponent of p in the factorization of n_{i_p} is maximal. Let $\mathcal{N}_1=\{n_{i_p}: p\leq k\}$. Let $\mathcal{M}=\mathcal{N}\backslash\mathcal{N}_1$. On the one hand,

$$\#\mathcal{M}\geq k+O\left(\frac{k\log\log k}{\log k}+\pi(k)\right)\geq (1+o(1))k \qquad \text{as } k\to\infty,$$

therefore

$$T=\prod_{n_i\in\mathcal{M}} n_i \geq k^{3/2\#\mathcal{M}}=k^{(3/2+o(1))k},$$

or

$$\log T\geq (3/2+o(1))k\log k \qquad \text{as } k\to\infty. \tag{28}$$

On the other hand, all primes p dividing T have the property that $p\leq (k+1)/2$. Furthermore, if $p^\alpha \mid n_i$ for some $n_i\in\mathcal{M}$, then since $p^\alpha\mid n_{i_p}\notin\mathcal{M}$

also, we get that $p^\alpha \mid n_{i_p} - n_i \neq 0$, therefore $p^\alpha \leq k$. Hence,

$$\begin{aligned}
\log T &= \sum_{p \leq (k+1)/2} \sum_{1 \leq \alpha \leq \log k/\log p} \log p \, \#\{n_i \in \mathcal{M} : n_i \equiv 0 \pmod{p^\alpha}\} \\
&= \sum_{p \leq (k+1)/2} \log p \sum_{1 \leq \alpha \leq \log k/\log p} \frac{k}{p^\alpha} \\
&= k \sum_{p \leq (k+1)/2} \frac{\log p}{p} \left(1 + \frac{1}{p} + \ldots\right) \leq k \sum_{p \leq (k+1)/2} \frac{\log p}{p-1} \\
&= (1 + o(1)) k \log k \qquad \text{as } k \to \infty, \qquad (29)
\end{aligned}$$

which contradicts (28). This completes the proof of Theorem 1.

5 A conditional result

For a nonzero integer n we put $N(n) = \prod_{p \mid n} p$. Recall that the ABC conjecture is the following statement.

Conjecture 1. *(ABC) For every ε, there exists a constant $K = K_\varepsilon$ depending on ε such that whenever A, B, C are coprime nonzero integers with $A + B = C$, then*

$$\max\{|A|, |B|, |C|\} \leq K_\varepsilon N(ABC)^{1+\varepsilon}$$

It is natural to ask what can one prove about our problem when ABC is assumed. Here is the result.

Theorem 2. *Assume the ABC conjecture. Then there exists a number c_6 such that equation (2) with $t > 0$ and $n \geq k^{1+c_6/\log\log k}$ does not hold.*

Proof. Put $n = n_1$. For every prime p dividing both u_n and u_{n_i} for some $i > 1$, we have that $p \mid u_{(n,n_i)}$. Note that $(n, n_i) \leq n_i - n < k$. Hence, if we write $\mathcal{D}$ for the set of divisors $< k$ of n, then (2) implies that

$$u_n = \pm A_1 y^\ell,$$

where A_1 is a number divisible only by primes dividing

$$\prod_{p \leq k} p \prod_{d \in \mathcal{D}} u_d.$$

Let $B = N(A_1)$. Since $|u_d| \leq 2|\alpha|^d$ and $\#\mathcal{D} \leq \tau(n)$, where $\tau(n)$ is the number of divisors of n, we get that

$$\begin{aligned} B &\leq \exp\left((1+o(1))k + (\log 2)\#\mathcal{D} + \log|\alpha| \sum_{d\in\mathcal{D}} d\right) \\ &\leq \exp\left((1+o(1))k + (\log 2)\tau(n) + k\tau(n)\log|\alpha|\right). \end{aligned} \tag{30}$$

Since

$$v_n^2 - \Delta u_n^2 = \pm 4s^n \tag{31}$$

and $\gcd(u_n, v_n) \mid 2$, it follows that we can apply the ABC conjecture with some small $\varepsilon > 0$ to equation (31) getting

$$\begin{aligned} |u_n|^2 &\ll N(u_n v_n s)^{1+\varepsilon} \ll (|v_n|B|y|)^{1+\varepsilon} \ll (|v_n|B|u_n|^{1/2})^{1+\varepsilon} \\ &\ll |\alpha|^{(1+\varepsilon)3n/2} B^{1+\varepsilon}. \end{aligned}$$

The constant implied above depends on both $\varepsilon > 0$ and the sequence $(u_n)_{n\geq 0}$. We now take $\varepsilon = 1/9$ and use the well-known fact that $|u_n| \geq |\alpha|^{n - c_7 \log n}$ for some constant c_7, and arrive at

$$|\alpha|^{2n - 2c_7 \log n} \ll |\alpha|^{5n/3} B^{10/9},$$

so implying

$$n \ll k\tau(n).$$

Now we use

$$\tau(n) \leq n^{c_8/\log\log n} \leq n^{1+c_8/\log\log k} \qquad \text{for some constant } c_8.$$

Therefore,

$$n^{1-c_8/\log\log k} \ll k,$$

which is not possible if $n \geq k^{1+c_6/\log\log k}$ with c_6 sufficiently large. This completes the proof of Theorem 2.

□

References

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

[2] Yu. F. 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.

[3] B. Brindza, 'On S-integral solutions of the equation $y^m = f(x)$,' *Acta Math. Hungar.* **44** (1984), 133–139.

[4] Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers,' *Ann. of Math. (2)* **163** (2006), 969–1018.

[5] Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation,' *Compos. Math.* **142** (2006), 31–62.

[6] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, 'On perfect powers in Lucas sequences,' *Int. J. Number Theory* **1** (2005), 309–332.

[7] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, 'Perfect powers from products of terms in Lucas sequences', *J. reine angew. Math.*, to appear.

[8] P. Erdős, 'On the product of consecutive integers. III,' *Indag. Math.* **17**, (1955), 85–90.

[9] P. Erdős, J. L. Selfridge, 'The product of consecutive integers is never a power,' *Illinois J. Math.* **19** (1975), 292–301.

[10] K. Győry, 'On the solutions of linear Diophantine equations in algebraic integers of bounded norm', *Ann. Univ. Sci. Budapest. Eőtvős Sect. Math.* **22/23** (1979/80), 225–233.

[11] K. Győry and K. R. Yu, 'Bounds for the solutions of S-unit equations and decomposable form equations', *Acta Arith.* **123** (2006), 9–41.

[12] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[13] M. N. Huxley, 'On the difference between consecutive primes', *Invent. Math.* **15** (1972), 164–170.

[14] F. Luca and T. N. Shorey, 'Diophantine equations with products of consecutive terms in Lucas sequences,' *J. Number Theory* **114** (2005), 298–311.

[15] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Springer-Verlag, Berlin, 1990.

[16] A. Pethő, 'Perfect powers in second order linear recurrences', *J. Number Theory* **15** (1982), 5–13.

[17] D. Poulakis, 'Solutions entiéres de l'équation $Y^m = f(X)$', *Sém. Théor. Nombres Bordeaux (2)* **3** (1991), 187–199.

[18] R. Sitaramachandra Rao, 'On an error term of Landau. II', in "Number theory (Winnipeg, Man., 1983)", *Rocky Mountain J. Math.* **15** (1985), 579–588.

[19] T. N. Shorey, 'Exponential Diophantine equations involving products of consecutive integers and related equations' in *Number theory*, 463–495, Trends Math., Birkhuser, Basel, 2000.

[20] 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. Scand.* **52** (1983), 24–36.