On members of Lucas sequences which are products of factorials

Mark Sias

SAMS Stellenbosch University

msias@uj.ac.za

December 6, 2022

Overview

Introduction

We determine upper bounds on n when the nth term of a Lucas sequence is expressible as a product of factorials. In fact, we show that if $\{U_n\}_{n\geq 0}$ is a Lucas sequence, then the largest n such that $|U_n| = m_1!m_2!\cdots m_k!$ with $1 \leq m_1 \leq m_2 \leq \cdots \leq m_k$, satisfies $n < 62000$. When the roots of the Lucas sequence are real, we have $n \in \{1, 2, 3, 4, 6, 12\}$.
As a consequence, we formulate and prove a corollary regarding the X-coordinates of Pell equations which are products of factorials. We show that if $\{X_n\}_{n\geq 1}$ is the sequence of X- coordinates of a Pell equation $X^2 - dY^2 = \pm 1$ with a nonsquare integer $d > 1$, then $X_n = m!$ implies $n = 1$.

Motivation

Let

$$\mathcal{P}F := \{\pm \prod_{j=1}^{k} m_j! : k \geq 1 \text{ and } 1 \leq m_1 \leq m_2 \leq \cdots \leq m_k\}$$

be the set of integers which are the product of factorials. Members of $\mathcal{P}F$ are sometimes called *Jordan-Polya* numbers and several recent papers investigate their arithmetic properties.

It was shown by Luca that if $t \geq 1$ is any fixed integer, then the Diophantine equation $\prod_{i=1}^{t} U_{n_i} \in \mathcal{P}F$ has only finitely many positive integer solutions $1 \leq n_1 \leq n_2 \leq \cdots \leq n_t$ and they are all effectively computable.

When $(r, s) = (1, 1)$ then $U_n = F_n$ is the nth Fibonacci number. For this particular case, it was shown by Luca and Stănică that the largest solution of equation in which t is also an indeterminate but with the condition on the indices $1 \leq n_1 < n_2 < \cdots < n_t$ is

$$F_1 F_2 F_3 F_4 F_5 F_6 F_8 F_{10} F_{12} = 11!$$

Definitions

Linear recurrence sequence of order k

Let $k \geq 1$ be an integer. A sequence $\{w_n\}_{n\geq 0} \subseteq \mathbb{C}$ is called linearly recurrent of order k if the recurrence

$$w_{n+k} = a_1 w_{n+k-1} + a_2 w_{n+k-2} + \cdots + a_k w_n$$

holds for all $n \geq 0$ with $a_1, \ldots, a_k \in \mathbb{C}$.
For $k = 2$, the sequence $\{w_n\}_{n\geq 0}$ is called **binary recurrent**.

Characteristic polynomial

Suppose that $a_k \neq 0$. If $a_1, \ldots, a_k \in \mathbb{Z}$ and $w_0, \ldots, w_{k-1} \in \mathbb{Z}$, then, by induction on n, we find that w_n is an integer for all $n \geq 0$. The polynomial

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k \in \mathbb{C}[X]$$

is called the Characteristic polynomial of $\{w_n\}_{n\geq 0}$.

The characteristic polynomial for the binary recurrent sequence is of the form

$$f(X) = X^2 - a_1 X - a_2 = (X - \alpha_1)(X - \alpha_2),$$

where α_1 and α_2 are the roots of the polynomial.

Lucas sequence

A Lucas sequence $\{U_n\}_{n\geq 0}$ is a linear recurrent sequence of order 2 (*or binary recurrence*) defined by

$$U_{n+2} = rU_{n+1} + sU_n \quad n \geq 0,$$

for r and s positive integers such that $\gcd(r, s) = 1$, $U_0 = 0$, $U_1 = 1$ and the ratio α/β of the roots α, β of $x^2 - rx - s = 0$ is not a root of 1.

Companion Lucas sequence
The Companion Lucas sequence $\{V_n\}_{n\geq 0}$ of parameters (r, s) is given by

$$V_n = \alpha^n + \beta^n \qquad \text{for all} \qquad n \geq 0.$$

Alternatively, it can be defined recursively as

$$V_{n+2} = rV_{n+1} + sV_n \qquad \text{for all} \quad n \geq 0$$

with initial conditions $V_0 = 2, \ V_1 = r$.

The Pell equation
This is the Diophantine equation with unknowns $(x, y) \in \mathbb{Z}^2$ defined by

$$x^2 - dy^2 = 1,$$

where d is a positive integer which is not a perfect square.

Cyclotomic polynomial

The polynomial

$$\Phi_n(X) = \prod_{\substack{(d,n)=1 \\ d \leq n}} \left(X - e^{\frac{2\pi i d}{n}} \right)$$

is called the nth Cyclotomic polynomial. This polynomial has degree $\varphi(n)$.

Primitive divisor

We say that a prime $p \mid U_n$ is a **primitive divisor** of U_n if $p \nmid U_t$ for $t < n$ and $p \nmid r^2 + 4s$.

Preliminaries

There exists a very useful relationship between primitive divisors of Lucas sequences and Cyclotomic polynomials, which is proved in a paper by Bilu, Hanrot and Voutier. We state this as a lemma.

We note that here, α_p indicate the exponent at which p appears in the factorisation of U_k^1, while $P(n_0)$ denotes the largest prime factor of n_0. Let $m \mid n$. Denote by $U_k^1 := \left(\frac{\alpha_1^k - \beta_1^k}{\alpha_1 - \beta_1}\right)$, where $\alpha_1 = \alpha^{n/m}$ and $\beta_1 = \beta^{n/m}$.

Lemma

For $n > 4, n \notin \{6, 12\}$,

$$\prod_{\substack{p^{\alpha_p} \| U_n^1 \\ p \text{ primitive}}} p^{\alpha_p} = \frac{\Phi_n(\alpha, \beta)}{\delta},$$

where $\delta \in \{2, P(n_0)\}$ *and* $\Phi_n(\alpha, \beta)$ *is the specialisation of the homogenization* $\Phi_n(X, Y)$ *of the nth cyclotomic polynomial* $\Phi_n(X)$ *in the pair* (α, β).

We consider a version of the Primitive Divisor Theorem which is attributed to Zsigmondy.

Theorem

If the roots of the characteristic polynomial of $\{U_n\}_{n\geq 0}$ are coprime positive integers and if $n > 6$, then U_n has a primitive divisor.

It was established by Carmichael that for α and β real and n not equal to 1, 2, 3, 4 and 6, the the Lucas numbers, $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ have one or more primitive divisors excluding $n = 12$, $r = 1$ and $s = -1$ (for the characteristic polynomial

$$f(X) = X^2 - rX - s = (X - \alpha)(X - \beta)).$$

Carmichael's result is in essence an extension of Zsigmondy's theorem.

Bilu, Hanrot and Voutier settled the problem in the case where the roots are complex nonreal by proving that for $n > 30$, every Lucas number has a primitive divisor.

Linear forms in logarithms

A. Baker provided an effective lower bound on the absolute value of a nonzero linear form in logarithms of algebraic numbers; that is, for a nonzero expression of the form

$$\sum_{i=1}^{n} b_i \log \alpha_i,$$

for $\alpha_1, \ldots, \alpha_n$ algebraic numbers and $b_1, \ldots, b_n$ are integers. His findings ushered in the dawn of a new era in the effective resolution of Diophantine equations of certain types. Such Diophantine equations can be reduced to exponential ones; i.e., where the unknown variables are in the exponents.

The height and logarithmic height of an algebraic number

Let α be an algebraic number of degree d. We let

$$f(x) = \sum_{i=0}^{d} a_i x^{d-i} \in \mathbb{Z}[X].$$

be the minimal polynomial of α with $a_0 > 0$ and $(a_0, \ldots, a_d) = 1$. Putting $H(\alpha) := \max\{|a_i| : i = 0, \ldots, d\}$, we let it denote the **height** of α. We now write

$$f(X) = a_0 \prod_{i=1}^{d} (X - \alpha^{(i)}),$$

where $\alpha = \alpha^{(1)}$. The **logarithmic height** of α is

$$h(\alpha) = \frac{1}{d} \left(\log |a_0| + \sum_{i=1}^{d} \log \max\{|\alpha^{(i)}|, 1\} \right).$$

Sieves

A sieve is basically an inclusion-exclusion argument. Many results in the theory of primes can be proved using sieves.

The next lemma follows easily from the Brun-Titchmarsh inequality given by Montgomery and Vaughan since $\pi(1; q, l) = 0$ and $\pi(y; q, l) \leq \pi(y + 1; q, l) - \pi(1; q, l)$. Note that $\pi(y; q, l)$ stands for the number of primes $p \leq y$ and $p \equiv l \pmod{q}$.

Lemma

Let q be a positive integer, l be coprime to q and $y > q$. Then

$$\pi(y; q, l) \le \frac{2y}{\varphi(q)\log(y/q)} \quad \text{and} \quad \pi(2y; q, l) - \pi(y; q, l) \le \frac{2y}{\varphi(q)\log(y/q)}.$$

The *abc* conjecture

Lemma

Let $\epsilon > 0$. *There exists a constant* κ_ε *depending only on* ε *such that given pairwise coprime positive integers* a, b, c *with* $a + b = c$*, we have*

$$c < \kappa_\varepsilon \cdot \gamma(abc)^{1+\epsilon}.$$

Primes in arithmetic progressions

The next lemma is derived from the work of Bennet et al.

Lemma

Let m be either a prime ≤ 30 *or* $m \in \{8, 9, 12, 16, 24\}$. *Then*

$$\pi(y; m, 1) + \pi(y; m, -1) \leq \frac{y}{\varphi(m)\log y}\left(2 + \frac{5}{\log y}\right) \quad \text{for } y > 1.$$

Also,

$$\pi(y; 12, 1) + \pi(y; 12, 7) \leq \frac{y}{\varphi(12)\log y}\left(2 + \frac{5}{\log y}\right) \quad \text{for } y > 1.$$

The toolbox: a series of lemmas

In the present section we embark on the proof of the main theorem, which we will state formally.

Theorem

The equation
$U_n = \pm m_1! m_2! \cdots m_k! \quad \text{where } k \geq 1 \quad \text{and} \quad 1 \leq m_1 \leq m_2 \leq \cdots \leq m_k,$
implies $n < 62000$. *When* α, β *are real, then* $n \in \{1, 2, 3, 4, 6, 12\}$.

The equation $V_n = \pm m_1! m_2! \cdots m_k, \qquad 1 \leq m_1 \leq m_2 \leq \cdots \leq m_k,$
implies $n = 2$ *or* n *is odd and* $n < 31000$. *Further,* $n \in \{1, 2, 3\}$ *when* α, β *are real.*

For a positive integer m, let $q_0 := q_0(m)$ be the least odd prime divisor of m. We make the convention that $q_0 := 1$ if m is a power of 2. Let $\eta := \eta(m) = 0$ if m is odd and 1 if m is even. Note that $m \equiv \gamma \pmod 2 \equiv 2^\eta \pmod 2$. Put $\gamma_0 := \gamma/(2^\eta q_0)$. We shall assume that $m \geq 4$ whenever m is a power of 2.

Lemma

Let m be a positive integer. We have

$$\log|\Phi_m(\alpha,\beta)| = \varphi(m)\log|\alpha| + \sum_{d|\gamma}\mu(d)\log\left|1-\left(\frac{\beta}{\alpha}\right)^{\frac{m}{d}}\right|.$$

Putting $x=\beta/\alpha$, *we have*

$$\sum_{d|\gamma}\mu(d)\log\left|1-x^{\frac{m}{d}}\right| = \begin{cases} \log\left|1+x^{\frac{m}{2}}\right| \\ \sum_{\substack{\mu(d)=1\\ d|\gamma_0}}\log\left|\frac{1+x^{\frac{m}{2d}}}{1+x^{\frac{m}{2q_0d}}}\right| - \sum_{\substack{\mu(d)=-1\\ d|\gamma_0}}\log\left|\frac{1+x^{\frac{m}{2d}}}{1+x^{\frac{m}{2q_0d}}}\right| & \eta \\ \sum_{\substack{\mu(d)=1\\ d|\gamma_0}}\log\left|\frac{1-x^{\frac{m}{d}}}{1-x^{\frac{m}{q_0d}}}\right| - \sum_{\substack{\mu(d)=-1\\ d|\gamma_0}}\log\left|\frac{1-x^{\frac{m}{d}}}{1-x^{\frac{m}{q_0d}}}\right| & \eta \end{cases}$$

Lemma

Assume that α *and* β *are real and* $|\alpha| \geq |\beta|$. *Let* $m \geq 4$. *Then*

$$\log|\Phi_m(\alpha,\beta)| \geq \varphi(m)\log|\alpha| - \begin{cases} \log 2, & \text{for } \omega(m) \leq 1+\eta, \\ \frac{2^{\omega(m)}}{2^{2+\eta}}(\log 2q_0)\,, & \text{for } \omega(m) \geq 2+\eta. \end{cases} \tag{1}$$

Lemma

Let α and β be complex conjugates with $\log|\alpha| > 4$. For $t \geq 3$, putting $t_* := t/\gcd(t,2)$, we have

$$\log|\alpha^t - \beta^t| \geq \log|\alpha| \left(t - 8(c_1(t_*) + 0.02)\log^2 t_*\right).$$

Furthermore,

$$\log|\alpha^t + \beta^t| \geq \log|\alpha| \left(t - 8(c_1(t) + 0.02)\log^2 t\right).$$

We will use the following consequence of the above lemma.

Lemma

Let α and β be complex conjugates with $\log|\alpha| > 4$. Then

$$\log\left|1 \pm \left(\frac{\beta}{\alpha}\right)^t\right| \geq -\log|\alpha| \quad \textit{for} \quad t = 1, 2.$$

For $t \geq 3$, putting $t_* := t/\gcd(t,2)$, we have

$$\log|\alpha^t - \beta^t| \geq \log|\alpha|\left(t - 44.72\,(\log t_* + 2.36)^2 - 0.16(\log t_*)^2\right),$$

and

$$\log|\alpha^t + \beta^t| \geq \log|\alpha|\left(t - 44.72\,(\log t + 2.36)^2 - 0.16(\log t)^2\right). \quad (2)$$

Lemma

Let α and β be complex conjugates with $\log|\alpha| > 4$. Let

$$f(t) := 44.88 \log^2 t + 211.08 \log t + 249.08.$$

for $t > 1$. Then

$$\log|\Phi_m(\alpha,\beta)| \geq \varphi(m)\log|\alpha| - \max\left\{1, \frac{2^{\omega(m)}}{2^{2+\eta}}\right\}\left(f(m/2^\eta)\log\alpha + \log 2q_0\right). \tag{3}$$

Further, for m with $1 \leq \omega(m) \leq 6+\eta$, we have

$$\begin{aligned}\log|\Phi_m(\alpha,\beta)| \geq & \left(\varphi(m) - f(m/2^\eta) - (m/2^\eta)g_{\omega(m)-1-\eta}\right)\log|\alpha| \\ & - \begin{cases}\log 2, & \text{if} \quad \omega(m) \leq 1+\eta; \\ \frac{2^{\omega(m)}}{2^{2+\eta}}\log 2q_0, & \text{if} \quad \omega(m) \geq 2+\eta,\end{cases}\end{aligned} \tag{4}$$

The $g_{\omega(m)}$ is exhibited in the following table.

$\omega(m) - 1 - \eta$	0	1	2	3	4	5
$g_{\omega(m)-\eta}$	0	0	0.0286	0.0598	0.0934	0.1238

We next determine an upper bound for prime powers dividing a product of factorials by invoking the two lemmas from **Sieves** and **Primes in arithmetic progressions**.

We assume $\mathcal{F} \in \mathcal{P}F$ is such that $\mathcal{F} > 1$. Thus,

$$\mathcal{F} := \mathcal{F}(m_1, m_2, \ldots, m_k) := m_1! m_2! \cdots m_k! \tag{5}$$

for some positive integers $1 < m_1 \leq \cdots \leq m_k$. Let n_0 be a positive integer and let $a_0 = -1$ if $n_0 \neq 12$ and $a_0 \in \{-1, 7\}$ if $n_0 = 12$. Define

$$M_{n_0}(\mathcal{F}) := \log \left(\prod_{\substack{p^{\alpha_p} \| \mathcal{F} \\ p \equiv 1, a_0 \pmod{n_0}}} p^{\alpha_p} \right) = \sum_{\substack{p^{\alpha_p} \| \mathcal{F} \\ p \equiv 1, a_0 \pmod{n_0}}} \alpha_p \log p. \tag{6}$$

We employ analytic methods to establish an upper bound for $M_{n_0}(\mathcal{F})$ and prove the following lemma.

Lemma

(*a*) *For a positive integer* $n_0 \geq 30$ *and* $m_k \geq 3$, *we have*

$$M_{n_0}(\mathcal{F}) < \frac{4}{\varphi(n_0)}(1 + \log\log n_0)\left(\log \mathcal{F} - 1.4 \log m_k\right). \tag{7}$$

(*b*) *Let* $\mathcal{D} := \{8, 9, 12, 16, 24\} \cup \{5 \leq p \leq 30 : p \text{ prime}\}$. *For* $n_0 \in \mathcal{D}$, *we have*

$$M_{n_0}(\mathcal{F}) \leq \frac{2.2}{\varphi(n_0)}\left(\log \mathcal{F} - 1.4 \log m_k\right). \tag{8}$$

Further for $n_0 \in \{8, 12\}$, we have

$$M_{n_0}(\mathcal{F}) \leq \begin{cases} 0.23 \log \mathcal{F} & \text{when } n_0 = 8 \text{ and } 7 \leq m_k < 17; \\ 0.3 \log \mathcal{F} & \text{when } n_0 = 8 \text{ and } 17 \leq m_k \leq 47; \\ 0.28 \log \mathcal{F} & \text{when } n_0 = 12 \text{ and } 7 \leq m_k \leq 16. \end{cases} \tag{9}$$

Lemma

Let $N = m_1! \cdots m_k!$. *Then* $\gamma(N) = N^{o(1)}$ *as* $N \to \infty$.

Theorem

Let α, β be real. Then the first equation of the main theorem with $n \in \{2, 3, 4\}$ has infinitely many solutions. Further under the abc conjecture, this same equation with $n \in \{6, 12\}$ has only finitely many solutions. There are infinitely many solutions of the second equation for real α, β and $n \in \{1, 2, 3\}$.

We present a corollary regarding X-coordinates of Pell equations which are in $\mathcal{P}F$. For a positive integer d which is square-free, let (X_n, Y_n) be the nth solution of the Pell equation $X^2 - dY^2 = \pm 1$ in positive integers (X, Y) (namely, the positive integers $X,\ Y$ satisfy either $X^2 - dY^2 = 1$ or $X^2 - dY^2 = -1$).
Firstly, we provide a lemma.

Lemma

Let $s \in \{-1, 1\}$ *and* $r \geq 1$. *Then* $V_n \in \mathcal{P}F$ *with* $n > 1$ *implies*

$$\begin{aligned} n = 2 &: (r, s) = (2, 1), \quad V_2 = 3!; \\ n = 3 &: (r, s) = (1, 1), \quad V_3 = 2!2!; \\ n = 3 &: (r, s) = (3, 1), \quad V_3 = 3!3!. \end{aligned} \tag{10}$$

Theorem

Let (X_n, Y_n) be the nth solution in positive integers of the equation $X^2 - dY^2 = \pm 1$ for some square-free integer d. Then $X_n \in \mathcal{PF}$ implies $n = 1$. Similarly, let (W_n, Z_n) be the nth solution in positive integers of the equation
$W^2 - dZ^2 = \pm 4$ for some square-free integer d. Then $W_n \in \mathcal{PF}$ implies $n = 1$ except for the cases $(n, d) = (2, 2),\ (3, 5),\ (3, 13)$ for which $W_2 = 3!$, $W_3 = 2!2!$ and $W_3 = 3!3!$, respectively, with solutions

$$3!^2 - 2 \cdot 4^2 = 4, \quad (2!2!)^2 - 5 \cdot 2^2 = -4 \quad \textit{and} \quad (3!3!)^2 - 13 \cdot 10^2 = -4.$$

M. A. Bennett, G. Martin, K. O'Bryant and A. Rechnitzer, *Explicit Bounds for Primes in Arithmetic Progressions*, Illinois J. Math., **62** (2018), no. 1-4, 427–532.

A. Bérczes, A. Dujella, L. Hajdu, N. Saradha and R. Tijdeman, *Products of factorials which are powers*, Acta Arith. **190** (2019), 339–350.

Y. Bilu, G. Hanrot and 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.

J.M. de Koninck, N. Doyon, A. A. B. Razandrasoanaivolala and W. Verrault, *Bounds for the counting function of Jordan-Pólya numbers*, Archivum Math. **56** (2020), 141-152 .

W. Ljunggren, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturvid. **45** (1942), 61–70.

F. Luca, *Products of factorials in binary recurrence sequences*, Rocky Mtn. J. of Math. **29** (1999), 1387–1411.

F. Luca and P. Stănică, $F_1 F_2 F_3 F_4 F_5 F_6 F_8 F_{10} F_{12} = 11!$, Portugaliae Math., **63** (2006), 251–260.

F. Luca, *Fibonacci numbers with the Lehmer property*, Bull. Pol. Acad. Sci. Math., **55** (2007), 7–15.

H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika, **20** (1973), 119–134.

Q. Sun and P. Z. Yuan, *A note on the Diophantine equation* $x^4 - Dy^2 = 1$, Sichuan Daxue Xuebao **34** (1997), 265–268.

P. Voutier, *Primitive divisors of Lucas and Lehmer sequences, III*, Math. Proc. Cambridge Philos. Soc., **123** (1998), 407–419.

Thank you!