Canad. Math. Bull. Vol. **66** (1), 2023, pp. 225–231
http://dx.doi.org/10.4153/S0008439522000248

Terms of Lucas sequences having a large smooth divisor

Nikhil Balaji and Florian Luca

Abstract. We show that the Kn–smooth part of $a^n - 1$ for an integer $a > 1$ is $a^{o(n)}$ for most positive integers n.

1 Introduction

It is known that if for every n, the sequence $\binom{2n}{n}$ can be computed in $O(\log^k n)$ arithmetic operations for a fixed constant k, then integers can be factored efficiently [3, 5]. We ask if there exist linearly recurrent sequences which contain many small factors like $\binom{2n}{n}$. If such sequences exist, they can be used instead of $\binom{2n}{n}$ to factor integers. This is because the nth term of any linearly recurrent sequence can be computed in $O(\log n)$ arithmetic operations using repeated squaring of the companion matrix [1]. We first set up some notation to formally state our question.

Let $P(n)$ be the largest prime factor of n and $s_y(n)$ be the largest divisor d of n with $P(d) \le y$. Thus, $s_y(n)$ is the *y-smooth* part of n. Given a sequence $\mathbf{u} = (u_n)_{n\ge0}$ of positive integers we ask whether we can find $c > 1$ and K such that

$$\mathcal{A}_{K,c,\mathbf{u}} = \{n : s_{Kn}(u_n) > c^n\}$$

contains many elements. For example, if $u_n = \binom{2n}{n}$ is the sequence of middle binomial coefficients, then $\mathcal{A}_{2,2,\mathbf{u}}$ contains all the positive integers. The main question we tackle in this paper can be formally stated as follows.

Question 1.1 Does there exist a linearly recurrent sequence $\mathbf{u}$ such that $\mathcal{A}_{K,c,\mathbf{u}}$ is infinite?

Here, we address the problem in the simplest case namely $u_n = a^n - 1$ for some positive integer a. Our results are easily extendable to all Lucas sequences, in particular, the sequence of Fibonacci numbers.

To start we recall the famous ABC-conjecture. Put

$$\text{rad}(n) = \prod_{p|n} p$$

for the algebraic radical of n.

Received by the editors February 18, 2022; revised March 22, 2022; accepted March 22, 2022.
Published online on Cambridge Core March 25, 2022.
AMS subject classification: **11B39**, 11B37, 11B65.
Keywords: Linearly recurrent sequences, Lucas sequences, ABC conjecture.

Conjecture *For all $\varepsilon > 0$ there exists a constant K_ε such that whenever A, B, C are coprime nonzero integers with $A + B = C$, then*

$$\max\{|A|, |B|, |C|\} \le K_\varepsilon \mathrm{rad}(ABC)^{1+\varepsilon}.$$

Throughout this paper, $a > 1$ is an integer and $u_n = a^n - 1$.
We have the following result.

Theorem 1.1 *Assume the ABC conjecture. Then for any $K > 0$, $c > 1$, the set $\mathcal{A}_{K,c,u}$ is finite.*

One can ask what can one prove unconditionally. Maybe we cannot prove that $\mathcal{A}_{K,c,\mathbf{u}}$ is finite but maybe we can prove that it is *thin*, that is that it does not contain too many integers. This is the content of the next theorem.

Theorem 1.2 *We have*

$$\#(\mathcal{A}_{K,c,u} \cap [1, N]) \ll N \exp\left(-\frac{\log N}{156 \log\log N}\right). \tag{1.1}$$

In particular, if one wants to find for all large N an interval starting at N of length k, that is $[N + 1, \ldots, N + k]$ which has nonempty intersection with $\mathcal{A}_{K,c,\mathbf{u}}$ then infinitely often one should take $k > \exp(\log N/(157 \log\log N))$. But if the ABC conjecture is true, one will no longer find elements of $\mathcal{A}_{K,c,\mathbf{u}}$ in the above interval for large N no matter how large k is. Regarding Theorem 1.2, see [6] for a more general result which applies to any linearly recurrent sequence but which gives a slightly weaker bound when specialised to our sequence $\mathbf{u}$.

2 Proofs

2.1 The proof of Theorem 1.1

We apply the ABC conjecture to the equation

$$a^n - 1 = st, \quad s := s_{Kn}(u_n), \quad t = (a^n - 1)/s$$

for $n \in \mathcal{A}_{K,c,\mathbf{u}}$ with the obvious choices. Note that

$$\mathrm{rad}(s) = \prod_{\substack{p \le Kn \\ p \mid a^n - 1}} p \quad \text{and} \quad t < (a/c)^n.$$

We then have

$$a^n \ll_\varepsilon (a \cdot \mathrm{rad}(s)t))^{1+\varepsilon} \ll \left(\prod_{\substack{p \le Kn \\ p \mid a^n - 1}} p\right)^{1+\varepsilon} (a/c)^{n(1+\varepsilon)}.$$

https://doi.org/10.4153/S0008439522000248 Published online by Cambridge University Press

We may of course assume that $1 < c < a$. Then

$$\sum_{\substack{p \le Kn \\ p \mid a^n - 1}} \log p \ge \frac{n}{1+\varepsilon}(\log a - (1+\varepsilon)\log(a/c)) + O_\varepsilon(1).$$

We choose $\varepsilon > 0$ small enough so that $\log a - (1+\varepsilon)\log(a/c) > 0$. Then, we get

$$S_{a,K}(n) := \sum_{\substack{p \le Kn \\ p \mid a^n - 1}} \log p \gg_\varepsilon n. \tag{2.1}$$

The next lemma shows that the left–hand side above is $\le n^{2/3+o(1)}$ as $n \to \infty$. This is unconditional and finishes the proof of Theorem 1.1.

Lemma 2.1 *We have*

$$S_{K,a}(n) \le K^{1/2} n^{1/2+o(1)}$$

as $n \to \infty$.

Proof Let ℓ_p be the order of a modulo p; that is the smallest positive integer k such that $a^k \equiv 1 (\bmod\ p)$. Since primes p participating in $S_{K,a}(n)$ have $p \mid a^n - 1$, it follows that $\ell_p \mid n$. Since also such primes are $O(n)$, it follows that

$$S_{K,a} \ll \#P_{K,n} \log n,$$

where $P_{K,a}(n) := \{p \le Kn : \ell_p \mid n\}$. To estimate $P_{K,a}(n)$ we fix a divisor d of n and look at primes $p \le Kn$ such that $\ell_p = d$. Such primes p have the property that $p \equiv 1$ $(\bmod\ d)$ by Fermat's Little Theorem. In particular, the number of such (without using results on primes in progressions) is at most

$$\left\lfloor \frac{Kn}{d} \right\rfloor \le \frac{Kn}{d}.$$

However, since these primes divide $a^d - 1$, the number of them is $O(d)$. Thus, for a fixed d the number of such primes is

$$\ll \min\left\{\frac{Kn}{d}, d\right\} \ll (Kn)^{1/2}.$$

Summing this up over all divisors d of n we get that

$$\#P_{K,a}(n) \ll d(n)(Kn)^{1/2} \le K^{1/2} n^{1/2+o(1)}$$

as $n \to \infty$, where we used $d(n)$ for the number of divisors of n and the well-known estimate $d(n) = n^{o(1)}$ as $n \to \infty$ (see Theorem 315 in [2]). Hence,

$$S_{K,a}(n) \ll \#P_{K,a}(n) \log n \le K^{1/2} n^{1/2+o(1)}$$

as $n \to \infty$, which is what we wanted. □

Remark 2.2 The current Lemma 2.1 was supplied by the referee. Our initial statement was weaker. The combination between Lemma 2.1 and estimate (2.1) shows that

https://doi.org/10.4153/S0008439522000248 Published online by Cambridge University Press

we can even take K growing with n such as $K = n^{1-\varepsilon}$ in the hypothesis of Theorem 1.1 and retain its conclusion. This has been also noticed in [4].

2.2 The proof of Theorem 1.2

It is enough to prove an upper bound comparable to the upper bound from the right–hand side of (1.1) for $\#(\mathcal{A}_{K,c,\mathbf{u}} \cap (N/2, N])$ as then we can replace N by $N/2$, then $N/4$, etc. and sum up the resulting inequalities. So, assume that $n \in (N/2, N]$. We estimate

$$Q_N := \prod_{n\in(N/2,N]} s_{KN}(u_n).$$

On the one hand, since $s_{KN}(u_n) \geq s_{Kn}(u_n) \geq c^n \geq c^{N/2}$ for all $n \in \mathcal{A}_{K,c,\mathbf{u}}$, we get that

$$\log Q_N \gg N(\#\mathcal{A}_{K,c,\mathbf{u}} \cap (N/2, N]).$$

Next, writing $v_p(m)$ for the exponent of p in the factorisation of m, we have

$$\log Q_N = \sum_{n\in(N/2,N]} \sum_{p\leq KN} v_p(u_n) \log p \leq \sum_{p\leq KN} \log p \sum_{n\in(N/2,N]} v_p(u_n). \tag{2.2}$$

Let $o_p := v_p(u_{\ell_p})$. It is well-known that if p is odd then

$$v_p(u_n) = \begin{cases} o_p + v_p(n), & \text{if} \quad \ell_p \mid n; \\ 0, & \text{otherwise} \end{cases}$$

(see, for example, (66) in [7]). In particular, if $p \mid u_n$, then $p^{o_p} \mid u_n$. Furthermore, for each $k \geq 0$, the exact power of p in u_n is $o_p + k$ if and only if $\ell_p p^k$ divides n and $\ell_p p^{k+1}$ does not divide n. When $p = 2$, we may assume that a is odd (otherwise $v_2(u_n) = 0$ for all $n \geq 1$), and the right–hand side of the above formula needs to be ammended to

$$v_2(u_n) = \begin{cases} o_2, & \text{if} \quad 2 \nmid n; \\ o_p + v_2(a+1) + v_2(n/2), & \text{if} \quad 2 \mid n. \end{cases}$$

Thus, for odd p,

(2.3)
$$\sum_{n\in(N/2,N]} v_p(u_n) = o(p)\#\{N/2 < n \leq N : \ell_p \mid n\} + \sum_{k\geq 1} \#\{N/2 < n \leq N : \ell_p p^k \mid n\}.$$

A similar formula holds for $p = 2$. In particular, for $p = 2$, we have

$$\sum_{n\in(N/2,N]} v_2(u_n) = O(N).$$

Thus, the prime $p = 2$ contributes a summand of size $O(N)$ to the right-hand side of (2.2). From now on, we assume that p is odd. The first cardinality in the right-hand side of formula (2.3) above is

$$\#\{N/2 < n \leq N : \ell_p \mid n\} \leq \left\lfloor \frac{N}{2\ell_p} \right\rfloor + 1 \ll \frac{N}{\ell_p}.$$

The remaining cardinalities on the right-above can be bounded as

$$\#\{N/2 < n \le N : \ell_p p^k \mid n\} \le \left\lfloor \frac{N}{2\ell_p p^k} \right\rfloor + 1 \ll \frac{N}{\ell_p p^k}.$$

Thus,

$$\sum_{n\in(N/2,N]} \nu_p(u_n) \ll \frac{N o_p}{\ell_p} + \sum_{k\ge1} \frac{N}{\ell_p p^k} \ll \frac{N o_p}{\ell_p} + \frac{N}{\ell_p p}.$$

We thus get

$$\log Q_N \ll N \sum_{p\le Kn} \frac{o_p \log p}{\ell_p} + N \sum_{p\le Kn} \frac{\log p}{\ell_p p} \ll N \sum_{p\le Kn} \frac{o_p \log p}{\ell_p} := S.$$

It remains to bound S. Since $p^{o_p} \mid a^{\ell_p} - 1$, we get that $p^{o_p} < a^{\ell_p}$ so $o_p \log p \ll \ell_p$. Hence,

$$S = N \sum_{p\le KN} \frac{o_p \log p}{\ell_p} \ll N\pi(KN) \ll_K \frac{N^2}{\log N}.$$

We get the first nontrivial upper bound on $\#(\mathcal{A}_{K,c,\mathbf{u}} \cap (N/2, N]$, namely

$$N\#(\mathcal{A}_{K,c,\mathbf{u}} \cap (N/2, N]) \ll \log Q_N \ll S \ll \frac{N^2}{\log N} + N \log\log N \ll_K \frac{N^2}{\log N},$$

so

$$\#(\mathcal{A}_{K,c,\mathbf{u}} \cap (N/2, N]) \ll_K \frac{N}{\log N}.$$

To do better, we need to look more closely at $o_p \log p/\ell_p$ for primes $p \le KN$. We split the sum S over primes $p \le KN$ in two subsums. The first is over the primes in the set Q_1 consisting of p such that $o_p \log p/\ell_p < 1/y_N$, where y_N is some function of N which we will determine later. We let Q_2 be the complement of Q_1 in the set of primes $p \le Kn$. The sum over primes $p \in Q_1$ is

$$S_1 = N \sum_{p\in Q_1} \frac{o_p \log p}{\ell_p} \le \frac{N}{y_N}\pi(KN) \ll_K \frac{N^2}{y_N \log N}.$$

For Q_2, we use the trivial estimate

$$S_2 = N \sum_{p\in Q_2} \frac{o_p \log p}{\ell_p} \ll N\#Q_2,$$

and it remains to estimate the cardinality of Q_2. Note that Q_2 consists of primes p such that $o_p > \ell_p/(y_N \log p) \gg \ell_p/(y_N \log N)$. We put ℓ_p in dyadic intervals. That is $\ell_p \in (2^i, 2^{i+1}]$ for some $i \ge 0$. Then primes $p \le KN$ in Q_2 with such ℓ_p have the property that $o_p \gg 2^i/(y_N \log N)$. Hence,

https://doi.org/10.4153/S0008439522000248 Published online by Cambridge University Press

$$\frac{2^i\#(Q_2\cap(2^i,2^{i+1}])}{y_N\log N} \ll \sum_{p\in Q_2\cap(2^i,2^{i+1}]} v_p(a^{\ell_p}-1)\log p \le \sum_{\ell\in(2^i,2^{i+1}]}\log(a^\ell-1)$$
$$\ll \sum_{\ell\in(2^i,2^{i+1}]}\ell \ll 2^{2i},$$

which gives

$$\#(Q_2\cap(2^i,2^{i+1}]) \ll 2^i y_N\log N.$$

Summing up over all the i, we get

$$\#Q_2 \le 2^I y_N\log N,$$

where I is maximal such that $(2^I,2^{I+1}]$ contains an element p of Q_2. By a result of Stewart (see Lemma 4.3 in [7]),

$$2^I < \ell_p < o_p y_N\log N < p\exp\left(-\frac{\log p}{51.9\log\log p}\right)y_N\log N\log\ell_p$$
$$\ll KN\exp\left(-\frac{\log(Kn)}{51.9\log\log(KN)}\right)y_N\log(KN)^2$$
$$\ll_K N\exp\left(-\frac{\log N}{51.95\log\log N}\right)y_N(\log N)^2.$$

Thus,

$$\#Q_2 \ll 2^I y_N\log N \ll_K N\exp\left(-\frac{\log N}{51.95\log\log N}\right)y_N^2(\log N)^3$$
$$\ll N\exp\left(-\frac{\log N}{52\log\log N}\right)y_N^2.$$

Choosing $y_N := \exp\left(c\frac{\log N}{\log\log N}\right)$ with a positive constant c to be determined later, we get

$$N\#(\mathcal{A}_{K,c,\mathbf{u}}\cap(N/2,N]) \ll N\#Q_2 + \frac{N}{y_N\log N}$$
$$\ll_K N\left(\exp\left(\left(2c-\frac{1}{52}\right)\frac{\log N}{\log\log N}\right)+\exp\left(-\frac{c\log N}{\log\log N}\right)\right).$$

Choosing $c := 1/156$, we get

$$\#(\mathcal{A}_{K,c,\mathbf{u}}\cap(N/2,N]) \ll N\log N\exp\left(-\frac{\log N}{156\log\log N}\right),$$

which is what we wanted.

Acknowledgement We thank the referee for suggesting the current Lemma 2.1 with its proof and for pointing out reference [4] and Professor Igor E. Shparlinski for pointing out reference [6]. F.L. worked on this paper while visiting the Max Planck

Institute for Software Systems in Saarbrücken, Germany in Fall of 2020. F.L. thanks the Institute for hospitality and support.

References

[1] A. Bostan and R. Mori, *A simple and fast algorithm for computing the N-th term of a linearly recurrent sequence*. SOSA 2021, 118–132.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp.

[3] R. J. Lipton, *Straight-line complexity and integer factorization*. ANTS 1994, 71–79.

[4] R. Murty and S. Wong, *The ABC conjecture and prime divisors of the Lucas and Lehmer sequences*. In Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 43–54.

[5] A. Shamir, *Factoring numbers in O(logn) arithmetic steps*. Inf. Process. Lett. **8**(1979), no. 1, 28–31.

[6] I. E. Shparlinski, *Some arithmetic properties of recurrence sequences*. Math. Zam. **47**(1990), 124–131; Translation in Math. Notes 47 (1990), 612–617.

[7] C. L. Stewart, *On divisors of Lucas and Lehmer numbers*. Acta Math. **211**(2013), 291–314.

Department of Computer Science and Engineering, Indian Institute of Technology Delhi,
New Delhi 110016, India
e-mail: nbalaji@cse.iitd.ac.in

School of Maths Wits University, 1 Jan Smuts, Braamfontein, Johannesburg 2000, South Africa

Research Group in Algebric Structures and Applications, King Abdulaziz University, Abdulah Sulayman, Jeddah 22254, Saudi Arabia

and

Centro de Ciencias Matemáticas UNAM, Morelia, Mexico
e-mail: florian.luca@wits.ac.za

https://doi.org/10.4153/S0008439522000248 Published online by Cambridge University Press