

On numbers  $n$  relatively prime to the  $n$ th term of a linear recurrence

*Original*

On numbers  $n$  relatively prime to the  $n$ th term of a linear recurrence / Sanna, C.. - In: BULLETIN OF THE MALAYSIAN MATHEMATICAL SOCIETY. - ISSN 0126-6705. - STAMPA. - 42:2(2019), pp. 827-833. [10.1007/s40840-017-0514-8]

*Availability:*

This version is available at: 11583/2790032 since: 2020-05-03T10:10:59Z

*Publisher:*

Springer

*Published*

DOI:10.1007/s40840-017-0514-8

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*

(Article begins on next page)

# ON NUMBERS $n$ RELATIVELY PRIME TO THE $n$ TH TERM OF A LINEAR RECURRENCE

CARLO SANNA

ABSTRACT. Let  $(u_n)_{n \geq 0}$  be a nondegenerate linear recurrence of integers, and let  $\mathcal{A}$  be the set of positive integers  $n$  such that  $u_n$  and  $n$  are relatively prime. We prove that  $\mathcal{A}$  has an asymptotic density, and that this density is positive unless  $(u_n/n)_{n \geq 1}$  is a linear recurrence.

## 1. INTRODUCTION

Let  $(u_n)_{n \geq 0}$  be a linear recurrence over the integers, that is,  $(u_n)_{n \geq 0}$  is a sequence of integers satisfying

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k},$$

for all integers  $n \geq k$ , where  $a_1, \dots, a_k \in \mathbf{Z}$  and  $a_k \neq 0$ . To avoid trivialities, we assume that  $(u_n)_{n \geq 0}$  is not identically zero. We refer the reader to [4, Ch. 1-8] for the general terminology and theory of linear recurrences.

The set

$$\mathcal{B}_u := \{n \in \mathbf{N} : n \mid u_n\}$$

has been studied by several researchers. Assuming that  $(u_n)_{n \geq 0}$  is nondegenerate and that its characteristic polynomial has only simple roots, Alba González, Luca, Pomerance, and Shparlinski [1, Theorem 1.1] proved that

$$\#\mathcal{B}_u(x) \ll_k \frac{x}{\log x},$$

for all sufficiently large  $x > 1$ . André-Jeannin [2] and Somer [10] studied the arithmetic properties of the elements of  $\mathcal{B}_u$  when  $(u_n)_{n \geq 0}$  is a Lucas sequence, that is,  $(u_0, u_1, k) = (0, 1, 2)$ . In such a case, generalizing a previous result of Luca and Tron [6], Sanna [8] proved the upper bound

$$\#\mathcal{B}_u(x) \leq x^{1 - (\frac{1}{2} + o(1)) \log \log \log x / \log \log x},$$

as  $x \rightarrow +\infty$ , where the  $o(1)$  depends on  $a_1$  and  $a_2$ . Furthermore, Corvaja and Zannier [3] studied the more general set

$$\mathcal{B}_{u,v} := \{n \in \mathbf{N} : v_n \mid u_n\},$$

where  $(v_n)_{n \geq 0}$  is another linear recurrence over the integers. Under some mild hypotheses on  $(u_n)_{n \geq 0}$  and  $(v_n)_{n \geq 0}$ , they proved that  $\mathcal{B}_{u,v}$  has zero asymptotic density [3, Corollary 2], while Sanna [7] gave the bound

$$\#\mathcal{B}_{u,v}(x) \ll_{u,v} x \cdot \left( \frac{\log \log x}{\log x} \right)^{h_{u,v}},$$

for all  $x \geq 3$ , where  $h_{u,v}$  is a positive integer depending only on  $(u_n)_{n \geq 0}$  and  $(v_n)_{n \geq 0}$ .

If  $(F_n)_{n \geq 0}$  is the sequence of Fibonacci numbers, Leonetti and Sanna [5] showed that the set

$$\mathcal{G} := \{\gcd(n, F_n) : n \in \mathbf{N}\}$$

has zero asymptotic density, and that

$$\#\mathcal{G}(x) \gg \frac{x}{\log x},$$

---

2010 *Mathematics Subject Classification*. Primary: 11B37. Secondary: 11A07, 11B39, 11N25.  
*Key words and phrases*. Linear recurrences; greatest common divisor; divisibility.

for all  $x \geq 2$ . Moreover, Sanna and Tron [9] proved that for each positive integer  $m$  the set

$$\{n \in \mathbf{N} : \gcd(n, F_n) = m\}$$

has an asymptotic density. They also gave a criterion to establish when this density is positive, and a formula for the density in terms of an infinite series involving the Möbius function and the rank of appearance.

On the other hand, the set

$$\mathcal{A}_u = \{n \in \mathbf{N} : \gcd(n, u_n) = 1\}$$

does not seem to have attracted so much attention. We prove the following result:

**Theorem 1.1.** *For any nondegenerate linear recurrence of integers  $(u_n)_{n \geq 0}$ , the asymptotic density  $\mathbf{d}(\mathcal{A}_u)$  of  $\mathcal{A}_u$  exists. Moreover, if  $(u_n/n)_{n \geq 1}$  is not a linear recurrence (of rational numbers) then  $\mathbf{d}(\mathcal{A}_u) > 0$ . Otherwise,  $\mathcal{A}_u$  is finite and, a fortiori,  $\mathbf{d}(\mathcal{A}_u) = 0$ .*

We remark that given the initial conditions and the coefficients of a linear recurrence  $(u_n)_{n \geq 0}$ , it is easy to test effectively if  $(u_n/n)_{n \geq 1}$  is a linear recurrence or not (see Lemma 2.1, in §2).

**Notation.** Throughout, the letter  $p$  always denotes a prime number. For a set of positive integers  $\mathcal{S}$ , we put  $\mathcal{S}(x) := \mathcal{S} \cap [1, x]$  for all  $x \geq 1$ , and we recall that the asymptotic density  $\mathbf{d}(\mathcal{S})$  of  $\mathcal{S}$  is defined as the limit of the ratio  $\#\mathcal{S}(x)/x$  as  $x \rightarrow +\infty$ , whenever this exists. We employ the Landau–Bachmann “Big Oh” and “little oh” notations  $O$  and  $o$ , as well as the associated Vinogradov symbols  $\ll$  and  $\gg$ , with their usual meanings. Any dependence of the implied constants is explicitly stated or indicated with subscripts.

## 2. PRELIMINARIES

In this section we give some definitions and collect some preliminary results needed in the later proofs. Let  $f_u$  be the characteristic polynomial of  $(u_n)_{n \geq 0}$ , i.e.,

$$f_u(X) = X^k - a_1 X^{k-1} - a_2 X^{k-2} - \dots - a_k.$$

Moreover, let  $\mathbf{K}$  be the splitting field of  $f_u$  over  $\mathbf{Q}$ , and let  $\alpha_1, \dots, \alpha_r \in \mathbf{K}$  be all the distinct roots of  $f_u$ . It is well known that there exist  $g_1, \dots, g_r \in \mathbf{K}[X]$  such that

$$(1) \quad u_n = \sum_{i=1}^r g_i(n) \alpha_i^n,$$

for all integers  $n \geq 0$ . We define  $B_u$  as the smallest positive integer such that all the coefficients of the polynomials  $B_u g_1, \dots, B_u g_r$  are algebraic integers.

We have the following easy lemma.

**Lemma 2.1.**  *$(u_n/n)_{n \geq 1}$  is a linear recurrence (of rational numbers) if and only if*

$$(2) \quad g_1(0) = \dots = g_r(0) = 0.$$

*In such a case,  $\mathcal{A}_u$  is finite.*

*Proof.* The first part of the lemma follows immediately from the fact that any linear recurrence can be written as a generalized power sum like (1) in a unique way (assuming the roots  $\alpha_1, \dots, \alpha_r$  are distinct, and up to the order of the addends). For the second part, if (2) holds then for all positive integer  $n$  we have that

$$\frac{B_u u_n}{n} = \sum_{i=1}^r \frac{B_u g_i(n)}{n} \alpha_i^n$$

is both a rational number and an algebraic integer, hence it is an integer. Therefore,  $n \mid B_u u_n$ , and so  $\gcd(n, u_n) = 1$  only if  $n \mid B_u$ , which in turn implies that  $\mathcal{A}_u$  is finite.  $\square$

For the rest of this section, we assume that  $(u_n)_{n \geq 0}$  is nondegenerate and that  $f_u$  has only simple roots, hence, in particular,  $r = k$ . We write  $\Delta_u$  for the discriminant of the polynomial  $f_u$ , and we recall that  $\Delta_u$  is a nonzero integer. If  $k \geq 2$ , then for all integers  $x_1, \dots, x_k$  we set

$$D_u(x_1, \dots, x_k) := \det(\alpha_i^{x_j})_{1 \leq i, j \leq k},$$

and for any prime number  $p$  not dividing  $a_k$  we define  $T_u(p)$  as the greatest integer  $T \geq 0$  such that  $p$  does not divide

$$\prod_{1 \leq x_2, \dots, x_k \leq T} \max\{1, |N_{\mathbf{K}}(D_u(0, x_2, \dots, x_k))|\},$$

where  $N_{\mathbf{K}}(\alpha)$  denotes the norm of  $\alpha \in \mathbf{K}$  over  $\mathbf{Q}$ , and the empty product is equal to 1. It is known that such  $T$  exists [4, p. 88]. If  $k = 1$ , then we set  $T_u(p) := +\infty$  for all prime numbers  $p$  not dividing  $a_1$ . Note that  $T_u(p) = 0$  if and only if  $k = 2$  and  $p$  divides  $\Delta_u$ .

Finally, for all  $\gamma \in ]0, 1[$ , we define

$$\mathcal{P}_{u, \gamma} := \{p : p \nmid a_k, T_u(p) < p^\gamma\}.$$

We are ready to state two important lemmas regarding  $T_u(p)$  [1, Lemma 2.1, Lemma 2.2].

**Lemma 2.2.** *For all  $\gamma \in ]0, 1[$  and  $x \geq 2^{1/\gamma}$  we have*

$$\#\mathcal{P}_{u, \gamma}(x) \ll_u \frac{x^{k\gamma}}{\gamma \log x}.$$

**Lemma 2.3.** *Assume that  $p$  is a prime number not dividing  $a_k B_u \Delta_u$  and relatively prime with at least one term of  $(u_n)_{n \geq 0}$ . Then, for all  $x \geq 1$ , the number of positive integers  $m \leq x$  such that  $u_{pm} \equiv 0 \pmod{p}$  is*

$$O_k\left(\frac{x}{T_u(p)} + 1\right).$$

Actually, in [1] both Lemma 2.2 and Lemma 2.3 were proved only for  $k \geq 2$ . However, one can easily check that they are true also for  $k = 1$ .

### 3. PROOF OF THEOREM 1.1

For all integers  $n \geq 0$ , define

$$v_n := B_u \sum_{i=1}^r \frac{g_i(n) - g_i(0)}{n} \alpha_i^n \quad \text{and} \quad w_n := B_u \sum_{i=1}^r g_i(0) \alpha_i^n.$$

Note that both  $(v_n)_{n \geq 0}$  and  $(w_n)_{n \geq 0}$  are linear recurrences of algebraic integers, and that the characteristic polynomial of  $(w_n)_{n \geq 0}$  has only simple roots.

Let  $\mathcal{G}$  be the Galois group of  $\mathbf{K}$  over  $\mathbf{Q}$ . Since  $u_n$  is an integer, for any  $\sigma \in \mathcal{G}$  we have that

$$(3) \quad nv_n + w_n = B_u u_n = \sigma(B_u u_n) = \sigma(nv_n + w_n) = n\sigma(v_n) + \sigma(w_n),$$

for all integers  $n \geq 0$ . In (3) note that both  $n\sigma(v_n)$  and  $\sigma(w_n)$  are linear recurrences, and the first is a multiple of  $n$ , while the characteristic polynomial of the second has only simple roots. Since the expression of a linear recurrence as a generalized power sum is unique, from (3) we get that  $w_n = \sigma(w_n)$  for any  $\sigma \in \mathcal{G}$ , hence  $w_n$  is an integer.

Thanks to Lemma 2.1, we know that  $(w_n)_{n \geq 0}$  is identically zero if and only if  $(u_n/n)_{n \geq 1}$  is a linear recurrence, and in such a case  $\mathcal{A}_u$  is finite, so that the claim of Theorem 1.1 is obvious. Hence, we assume that  $(w_n)_{n \geq 0}$  is not identically zero.

For the sake of convenience, put  $\mathcal{C}_u := \mathbf{N} \setminus \mathcal{A}_u$ . Thus we have to prove that the asymptotic density of  $\mathcal{C}_u$  exists and is less than 1. For each  $y > 0$ , we split  $\mathcal{C}_u$  into two subsets:

$$\begin{aligned} \mathcal{C}_{u, y}^- &:= \{n \in \mathcal{C}_u : p \mid \gcd(n, u_n) \text{ for some } p \leq y\}, \\ \mathcal{C}_{u, y}^+ &:= \mathcal{C}_u \setminus \mathcal{C}_{u, y}^-. \end{aligned}$$

It is well known that  $(u_n)_{n \geq 0}$  is definitively periodic modulo  $p$ , for any prime number  $p$ . Therefore, it is easy to see that  $\mathcal{C}_{u, y}^-$  is an union of finitely many arithmetic progressions and a

finite subset of  $\mathbf{N}$ . In particular,  $\mathcal{C}_{u,y}^-$  has an asymptotic density. If we put  $\delta_y := \mathbf{d}(\mathcal{C}_{u,y}^-)$ , then it is clear that  $\delta_y$  is a bounded nondecreasing function of  $y$ , hence the limit

$$(4) \quad \delta := \lim_{y \rightarrow +\infty} \delta_y$$

exists finite. We shall prove that  $\mathcal{C}_u$  has asymptotic density  $\delta$ . Hereafter, all the implied constants may depend on  $(u_n)_{n \geq 0}$  and  $k$ . If  $n \in \mathcal{C}_{u,y}^+(x)$  then there exists a prime  $p > y$  such that  $p \mid n$  and  $p \mid u_n$ . Furthermore,  $B_u u_n = n v_n + w_n$  implies that  $p \mid w_n$ . Hence, we can write  $n = pm$  for some positive integer  $m \leq x/p$  such that  $w_{pm} \equiv 0 \pmod{p}$ . For sufficiently large  $y$ , we have that  $p$  does not divide  $f_w(0)B_w \Delta_w$  (actually,  $B_w = 1$ ) and is coprime with at least one term of  $(w_s)_{s \geq 0}$ , since  $(w_s)_{s \geq 0}$  is not identically zero.

Therefore, by applying Lemma 2.3 to  $(w_s)_{s \geq 0}$ , we get that the number of possible values of  $m$  is at most

$$O\left(\frac{x}{pT_w(p)} + 1\right).$$

As a consequence,

$$(5) \quad \#\mathcal{C}_{u,y}^+(x) \ll \sum_{y < p \leq x} \left(\frac{x}{pT_w(p)} + 1\right) \ll x \cdot \left(\sum_{p > y} \frac{1}{pT_w(p)} + \frac{1}{\log x}\right),$$

where we also used the Chebyshev's bound for the number of primes not exceeding  $x$ . Setting  $\gamma := 1/(k+1)$ , by partial summation and Lemma 2.2, we have

$$(6) \quad \sum_{\substack{p > y \\ p \in \mathcal{P}_{w,\gamma}}} \frac{1}{pT_w(p)} \leq \sum_{\substack{p > y \\ p \in \mathcal{P}_{w,\gamma}}} \frac{1}{p} = \left[\frac{\#\mathcal{P}_{w,\gamma}(t)}{t}\right]_{t=y}^{+\infty} + \int_y^{+\infty} \frac{\#\mathcal{P}_{w,\gamma}(t)}{t^2} dt \ll \frac{1}{y^{1-k\gamma}} = \frac{1}{y^\gamma}.$$

On the other hand,

$$(7) \quad \sum_{\substack{p > y \\ p \notin \mathcal{P}_{w,\gamma}}} \frac{1}{pT_w(p)} \leq \sum_{\substack{p > y \\ p \notin \mathcal{P}_{w,\gamma}}} \frac{1}{p^{1+\gamma}} \ll \int_y^{+\infty} \frac{dt}{t^{1+\gamma}} \ll \frac{1}{y^\gamma}$$

Thus, putting together (5), (6), and (7), we obtain

$$\frac{\#\mathcal{C}_{u,y}^+(x)}{x} \ll \frac{1}{y^\gamma} + \frac{1}{\log x},$$

so that

$$(8) \quad \limsup_{x \rightarrow +\infty} \left| \frac{\#\mathcal{C}_u(x)}{x} - \delta_y \right| = \limsup_{x \rightarrow +\infty} \left| \frac{\#\mathcal{C}_u(x)}{x} - \frac{\#\mathcal{C}_{u,y}^-(x)}{x} \right| = \limsup_{x \rightarrow +\infty} \frac{\#\mathcal{C}_{u,y}^+(x)}{x} \ll \frac{1}{y^\gamma},$$

hence, by letting  $y \rightarrow +\infty$  in (8) and by using (4), we get that  $\mathcal{C}_u$  has asymptotic density  $\delta$ .

It remains only to prove that  $\delta < 1$ . Clearly,

$$\mathcal{C}_{u,y}^- \subseteq \{n \in \mathbf{N} : p \mid n \text{ for some } p \leq y\},$$

so that, by Eratosthenes' sieve and Mertens' third theorem [11, Ch. I.1, Theorem 11], we have

$$(9) \quad \limsup_{x \rightarrow +\infty} \frac{\#\mathcal{C}_{u,y}^-(x)}{x} \leq 1 - \prod_{p \leq y} \left(1 - \frac{1}{p}\right) \leq 1 - \frac{c_1}{\log y},$$

for all  $y \geq 2$ , where  $c_1 > 0$  is an absolute constant. Furthermore, the last part of (8) says that

$$(10) \quad \limsup_{x \rightarrow +\infty} \frac{\#\mathcal{C}_{u,y}^+(x)}{x} \leq \frac{c_2}{y^\gamma},$$

for all sufficiently large  $y$ , where  $c_2 > 0$  is an absolute constant.

Therefore, putting together (9) and (10), we get

$$(11) \quad \delta = \lim_{x \rightarrow +\infty} \frac{\#\mathcal{C}_u(x)}{x} \leq \limsup_{x \rightarrow +\infty} \frac{\#\mathcal{C}_{u,y}^-(x)}{x} + \limsup_{x \rightarrow +\infty} \frac{\#\mathcal{C}_{u,y}^+(x)}{x} \leq 1 - \left(\frac{c_1}{\log y} - \frac{c_2}{y^\gamma}\right),$$

for all sufficiently large  $y$ .

Finally, picking a sufficiently large  $y$ , depending on  $c_1$  and  $c_2$ , the bound (11) yields  $\delta < 1$ . The proof of Theorem 1.1 is complete.

#### REFERENCES

1. J. J. Alba González, F. Luca, C. Pomerance, and I. E. Shparlinski, *On numbers  $n$  dividing the  $n$ th term of a linear recurrence*, Proc. Edinb. Math. Soc. (2) **55** (2012), no. 2, 271–289.
2. R. André-Jeannin, *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Quart. **29** (1991), no. 4, 364–366.
3. P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), no. 2, 431–451.
4. G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003.
5. P. Leonetti and C. Sanna, *On the greatest common divisor of  $n$  and the  $n$ th Fibonacci number*, Rocky Mountain J. Math. (accepted).
6. F. Luca and E. Tron, *The distribution of self-Fibonacci divisors*, Advances in the theory of numbers, Fields Inst. Commun., vol. 77, Fields Inst. Res. Math. Sci., Toronto, ON, 2015, pp. 149–158.
7. C. Sanna, *Distribution of integral values for the ratio of two linear recurrences*, <https://arxiv.org/abs/1703.10047>.
8. C. Sanna, *On numbers  $n$  dividing the  $n$ th term of a Lucas sequence*, Int. J. Number Theory **13** (2017), no. 3, 725–734.
9. C. Sanna and E. Tron, *The density of numbers  $n$  having a prescribed G.C.D. with the  $n$ th Fibonacci number*, <https://arxiv.org/abs/1705.01805>.
10. L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 515–525.
11. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

UNIVERSITÀ DEGLI STUDI DI TORINO, DEPARTMENT OF MATHEMATICS, TURIN, ITALY

E-mail address: [carlo.sanna.dev@gmail.com](mailto:carlo.sanna.dev@gmail.com)

URL: <http://orcid.org/0000-0002-2111-7596>