Bull. Aust. Math. Soc. **99** (2019), 23–33
doi:10.1017/S0004972718000606

ON NUMBERS n WITH POLYNOMIAL IMAGE COPRIME WITH THE nTH TERM OF A LINEAR RECURRENCE

DANIELE MASTROSTEFANO and CARLO SANNA✉

(Received 15 May 2018; accepted 31 May 2018; first published online 28 August 2018)

Abstract

Let F be an integral linear recurrence, G an integer-valued polynomial splitting over the rationals and h a positive integer. Also, let $\mathcal{A}_{F,G,h}$ be the set of all natural numbers n such that $\gcd(F(n), G(n)) = h$. We prove that $\mathcal{A}_{F,G,h}$ has a natural density. Moreover, assuming that F is nondegenerate and G has no fixed divisors, we show that the density of $\mathcal{A}_{F,G,1}$ is 0 if and only if $\mathcal{A}_{F,G,1}$ is finite.

2010 *Mathematics subject classification*: primary 11B37; secondary 11A07, 11B39, 11N25.

Keywords and phrases: greatest common divisor, linear recurrences, natural densities.

1. Introduction

An *integral linear recurrence* is a sequence of integers $F(n)_{n\geq 0}$ such that

$$F(n) = a_1F(n-1) + \cdots + a_kF(n-k), \tag{1.1}$$

for all integers $n \geq k$, for some fixed $a_1, \ldots, a_k \in \mathbb{Z}$, with $a_k \neq 0$. We recall that F is said to be *nondegenerate* if none of the ratios α_i/α_j $(i \neq j)$ is a root of unity, where $\alpha_1, \ldots, \alpha_r \in \mathbb{C}^*$ are all the pairwise distinct roots of the *characteristic polynomial*

$$\psi_F(X) = X^k - a_1X^{k-1} - \cdots - a_k.$$

Moreover, F is said to be a *Lucas sequence* if $F(0) = 0, F(1) = 1$ and $k = 2$. In particular, the Lucas sequence with $a_1 = a_2 = 1$ is known as the *Fibonacci sequence*. We refer the reader to [8, Chs. 1–8] for the basic terminology and theory of linear recurrences.

Given two integral linear recurrences F and G, the arithmetic relations between the corresponding terms $F(n)$ and $G(n)$ have generated much interest. For instance, finding the positive integers n such that $G(n)$ divides $F(n)$ is a classical problem which goes back to Pisot, and the major results have been given by van der Poorten [23] and Corvaja and Zannier [5, 6]. (See also [14] for a proof of the last remark in [6].) In particular, for the special case in which $G = I$, where I is the identity sequence given

The second author is a member of INdAM group GNSAGA.

by $I(n) = n$ for all integers n, there are results by Alba González *et al.* [2], under the hypothesis that F is simple and nondegenerate, and by André-Jeannin [3], Luca and Tron [13], Sanna [15], Smyth [21] and Somer [22], when F is a Lucas sequence or the Fibonacci sequence.

For large classes of integral linear recurrences F, G, upper bounds for $\gcd(F(n), G(n))$ have been proved by Bugeaud *et al.* [4] and Fuchs [9]. Also, Leonetti and Sanna [12] studied the integers of the form $\gcd(F(n), n)$, when F is the Fibonacci sequence; while Sanna [16] determined all the moments of the function $n \mapsto \log(\gcd(F(n), n))$ for any nondegenerate Lucas sequence F.

For two integral linear recurrences F, G and a positive integer h, let us define

$$\mathcal{A}_{F,G,h} := \{n \in \mathbb{N} : \gcd(F(n), G(n)) = h\}$$

and also put $\mathcal{A}_{F,G} := \mathcal{A}_{F,G,1}$. Sanna [17] proved the following result on $\mathcal{A}_{F,I}$.

Theorem 1.1. *Let F be a nondegenerate integral linear recurrence. Then the set $\mathcal{A}_{F,I}$ has a natural density. Moreover, if F/I is not a linear recurrence (of rational numbers), then $\mathbf{d}(\mathcal{A}_{F,I}) > 0$. Otherwise, $\mathcal{A}_{F,I}$ is finite and, a fortiori, $\mathbf{d}(\mathcal{A}_{F,I}) = 0$.*

In the special case of the Fibonacci sequence, Sanna and Tron [18] gave a more precise result.

Theorem 1.2. *Assume that F is the Fibonacci sequence. Then, for each positive integer h, the natural density of $\mathcal{A}_{F,I,h}$ exists and is given by*

$$\mathbf{d}(\mathcal{A}_{F,I,h}) = \sum_{d=1}^{\infty} \frac{\mu(d)}{\operatorname{lcm}(dh, z(dh))},$$

where μ is the Möbius function and $z(m)$ denotes the least positive integer n such that m divides $F(n)$. Moreover, $\mathbf{d}(\mathcal{A}_{F,I,h}) > 0$ if and only if $\mathcal{A}_{F,I,h} \neq \emptyset$ if and only if $h = \gcd(\ell, F_\ell)$ with $\ell := \operatorname{lcm}(h, z(h))$.

Sanna and Tron also pointed out that their result can be extended to any nondegenerate Lucas sequence F with $\gcd(a_1, a_2) = 1$. Kim [11] gave an analogous result for elliptic divisibility sequences.

Trying to extend the previous result to $\mathcal{A}_{F,G,h}$ for two arbitrary integral linear recurrences is quite tempting. However, already establishing if the set $\mathcal{A}_{F,G}$ is infinite seems too difficult for the current methods. Indeed, the following conjecture of Ailon and Rudnick [1] is still open.

Conjecture 1.3. *Let a, b be two multiplicatively independent nonzero integers with $\gcd(a - 1, b - 1) = 1$. Then, for the linear recurrences $F(n) = a^n - 1$ and $G(n) = b^n - 1$, the set $\mathcal{A}_{F,G}$ is infinite.*

In this paper, we focus on the special case in which the linear recurrence G is an integer-valued polynomial splitting over the rationals. Our main result is the following theorem.

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

THEOREM 1.4. *Let F be an integral linear recurrence, G be an integer-valued polynomial with all roots in $\mathbb{Q}$ and h be a positive integer. Then the set $\mathcal{A}_{F,G,h}$ has a natural density. Moreover, if F is nondegenerate and G has no fixed divisors (and $h = 1$), then $\mathbf{d}(\mathcal{A}_{F,G}) = 0$ if and only if $\mathcal{A}_{F,G}$ is finite.*

It would be interesting to prove Theorem 1.4 for any integer-valued polynomial G, dropping the hypothesis that all the roots of G must be rational or allowing the presence of a fixed divisor. However, doing so presents some difficulties, which we will highlight in the final section.

Notation. Throughout, the letter p will always denote a prime number and we write ν_p for the p-adic valuation. 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 natural density $\mathbf{d}(\mathcal{S})$ of $\mathcal{S}$ is defined as the limit of the ratio $\#\mathcal{S}(x)/x$ as $x \to +\infty$, whenever this exists. We employ the Landau–Bachmann 'big oh' and 'little oh' notation 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. Preliminary results

In this section, we collect some definitions and preliminary results needed in the later proofs. Let F be a nondegenerate integral linear recurrence satisfying (1.1) and let ψ_F be its characteristic polynomial. To avoid trivialities, we assume that F is not identically zero. Let $\mathbb{K}$ be the splitting field of ψ_F over $\mathbb{Q}$ and let $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$ be all the distinct roots of ψ_F.

It is well known that there exist nonzero polynomials $f_1, \ldots, f_r \in \mathbb{K}[X]$ such that

$$F(n) = \sum_{i=1}^{r} f_i(n)\, \alpha_i^n \tag{2.1}$$

for all integers $n \geq 0$. The expression (2.1) is known as the *generalised power sum* representation of F and is unique (assuming that the roots $\alpha_1, \ldots, \alpha_r$ are distinct), up to the order of the summands.

Let G be an integer-valued polynomial and let h be a positive integer. We begin with two basic lemmas about $\mathcal{A}_{F,G,h}$.

LEMMA 2.1. *We can decompose $\mathcal{A}_{F,G,h}$ as the disjoint union of a finite set and finitely many sets of the form $a\mathcal{A}_{\widetilde{F},\widetilde{G}} + b$, where a, b are positive integers, $\widetilde{F}$ is a nondegenerate integral linear recurrence and $\widetilde{G}$ is an integer-valued polynomial.*

PROOF. First, it is well known and easy to prove that there exists a positive integer c such that, setting $F_j(m) := F(cm + j)$ for all nonnegative integers m and $j < c$, each F_j is an integral linear recurrence which is nondegenerate or identically zero. Then $\mathcal{A}_{F,G,h}$ is the disjoint union of the sets $\mathcal{A}_{F_j,G_j,h}$, where $G_j(m) := G_j(cm + j)$. Thus, without loss of generality, we can assume that F is nondegenerate.

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

Clearly, if $n \in \mathcal{A}_{F,G,h}$, then h divides both $F(n)$ and $G(n)$. Since integral linear recurrences (and, in particular, integer-valued polynomials) are ultimately periodic modulo any positive integer, there exist a finite set $\mathcal{E}$ and positive integers $a, b_1, \dots, b_t$ such that $h \mid \gcd(F(n), G(n))$ if and only if $n \in \mathcal{E}$ or $n = am + b_i$, for some positive integer m and some $i \in \{1, \dots, t\}$. Moreover, if $n = am + b_i$, for some integers $m \geq 1$ and $i \in \{1, \dots, t\}$, then $n \in \mathcal{A}_{F,G,h}$ if and only if $m \in \mathcal{A}_{\widetilde{F}_j, \widetilde{G}_j}$, where $\widetilde{F}_i(\ell) := F(a\ell + b_i)/h$ and $\widetilde{G}_i(\ell) := G(a\ell + b_i)/h$ for all integers $\ell \geq 0$. In particular, $\widetilde{F}_i$ is a nondegenerate integral linear recurrence and $\widetilde{G}_i$ is an integer-valued polynomial. So, we have proved that $\mathcal{A}_{F,G,h}$ is the disjoint union of the finite set $\mathcal{E}$ and $a\mathcal{A}_{\widetilde{F}_i, \widetilde{G}_i} + b_i$, for $i = 1, \dots, t$, as desired. □

Lemma 2.2. *If $G, f_1, \dots, f_r$ have a nontrivial common factor, then $\mathcal{A}_{F,G}$ is finite.*

Proof. Suppose that $X - \beta$ divides each of $G, f_1, \dots, f_r$ for some algebraic number β. Let $g \in \mathbb{Q}[X]$ be the minimal polynomial of β over $\mathbb{Q}$. Clearly, g divides G. Also, if $\mathbb{L}$ is the splitting field of $gGf_1 \cdots f_r$, then, for each $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$,

$$F(n) = \sigma(F(n)) = \sum_{i=1}^{r} (\sigma f_i)(n)(\sigma(\alpha_i))^n$$

for all positive integers n. In particular, $\sigma(\beta)$ is a root of each σf_i, since β is a root of each f_i. Therefore, by the uniqueness of the generalised power sum expression of a linear recurrence, $\sigma(\beta)$ is a root of each f_i and, as a consequence, g divides each f_i. Now let B be a positive integer such that all the polynomials $BG/g, Bf_1/g, \dots, Bf_r/g$ have coefficients which are algebraic integers. Then it follows easily that $BF(n)/g(n)$ and $BG(n)/g(n)$ are both integers for all positive integers n. (Note that $g(n) \neq 0$, since g is irreducible in $\mathbb{Q}[X]$.) Hence, $n \in \mathcal{A}_{F,G}$ implies that $g(n) \mid B$, which is possible only for finitely many positive integers n. □

For $r \geq 2$ and for all integers $x_1, \dots, x_r$, we set

$$D_F(x_1, \dots, x_r) := \det(\alpha_i^{x_j})_{1 \leq i,j \leq r}$$

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

$$\prod_{1 \leq x_2, \dots, x_r \leq T} \max\{1, |N_{\mathbb{K}}(D_F(0, x_2, \dots, x_r))|\},$$

where the empty product is equal to 1 and $N_{\mathbb{K}}(\alpha)$ denotes the norm of $\alpha \in \mathbb{K}$ over $\mathbb{Q}$. It is known that such T exists [8, page 88]. If $r = 1$, then we set $T_F(p) := +\infty$ for all prime numbers p not dividing a_1.

Finally, for all $\gamma > 0$, we define

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

The next lemma shows that $T_F(p)$ is usually larger than a power of p.

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

LEMMA 2.3 [2, Lemma 2.1]. *For all $\gamma \in (0, 1/r]$ and $x \geq 2^{1/\gamma}$,*

$$\#\mathcal{P}_{F,\gamma}(x) \ll_F \frac{x^{r\gamma}}{\gamma \log x}.$$

From the previous estimate, is easy to deduce the following bound.

LEMMA 2.4. *We have*

$$\sum_{p>y} \frac{1}{pT_F(p)} \ll_F \frac{1}{y^{1/(r+1)}}$$

for all sufficiently large y.

PROOF. We split the series into two parts, separating between prime numbers which belong to $\mathcal{P}_{F,\gamma}$ and those which do not. In the first case, by partial summation and Lemma 2.3, for a fixed $\gamma \in (0, 1/r)$,

$$\sum_{\substack{p>y \\ p\in\mathcal{P}_{F,\gamma}}} \frac{1}{pT_F(p)} \leq \sum_{\substack{p>y \\ p\in\mathcal{P}_{F,\gamma}}} \frac{1}{p} = \left[\frac{\#\mathcal{P}_{F,\gamma}(t)}{t}\right]_{t=y}^{+\infty} + \int_y^{+\infty} \frac{\#\mathcal{P}_{F,\gamma}(t)}{t^2}\, dt \ll_{F,\gamma} \frac{1}{y^{1-r\gamma}}. \tag{2.2}$$

On the other hand, in the second case,

$$\sum_{\substack{p>y \\ p\notin\mathcal{P}_{F,\gamma}}} \frac{1}{pT_F(p)} \leq \sum_{p>y} \frac{1}{p^{1+\gamma}} \ll \int_y^{+\infty} \frac{dt}{t^{1+\gamma}} \ll_\gamma \frac{1}{y^\gamma}. \tag{2.3}$$

If we put $\gamma := 1/(r+1)$ and collect together the estimates (2.2) and (2.3), we obtain the result. □

The next lemma is an upper bound in terms of $T_F(p)$ for the number of solutions of a certain congruence modulo p involving F. The proof proceeds essentially like the one of [2, Lemma 2.2], which in turn relies on previous arguments given in [20] (see also [8, Theorem 5.11]). We include it for completeness.

LEMMA 2.5. *Let p be a prime number dividing neither a_k nor the denominator of any of the coefficients of $f_1, \dots, f_r$. Moreover, let $\ell \geq 0$ be an integer such that $f_1(\ell), \dots, f_r(\ell)$ are not all zero modulo some prime ideal of $\mathcal{O}_\mathbb{K}$ lying over p. Then, for all $x > 0$, the number of integers $m \in [0, x]$ such that $F(pm + \ell) \equiv 0 \pmod p$ is*

$$O_r\left(\frac{x}{T_F(p)} + 1\right).$$

PROOF. For $r = 1$, the claim can be proved quickly using (2.1). Hence, assume that $r \geq 2$. Let $\mathcal{I}$ be an interval of $T_F(p)$ consecutive nonnegative integers, and let $m_1 < \cdots < m_s$ be all the integers $m \in \mathcal{I}$ such that $F(pm + \ell) \equiv 0 \pmod p$. Also, let π be a prime ideal of $\mathcal{O}_\mathbb{K}$ lying over p. Then, by (2.1), and since no denominator of the coefficients of $f_1, \dots, f_r$ belongs to π,

$$\sum_{i=1}^{r} f_i(\ell)(\alpha_i)^{\ell+pm_1} (\alpha_i^p)^{m_j-m_1} \equiv \sum_{i=1}^{r} f_i(pm_j + \ell)\, \alpha_i^{pm_j+\ell} \equiv 0 \pmod \pi \tag{2.4}$$

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

for $j = 1, \dots, s$. By a result of Schlickewei [19], there exists a constant $C(r)$, depending only on r, such that for any $B_1, \dots, B_r \in \mathbb{K}$, not all zero, the exponential equation

$$\sum_{i=1}^{r} B_i \alpha_i^x = 0$$

has at most $C(r)$ solutions in positive integers x. Suppose that $s \geq C(r) + r$. Put $x_1 := 0$ and, setting $\mathcal{X}_2 := \{m_j - m_1 : j = 2, \dots, s\}$, pick some $x_2 \in \mathcal{X}_2$ such that

$$\det(\alpha_i^{x_j})_{1 \leq i,j \leq 2} \neq 0.$$

This is possible by the same result of Schlickewei, since

$$\#\mathcal{X}_2 = s - 1 \geq C(r) + r - 1 > C(r).$$

For $r \geq 3$, set $\mathcal{X}_3 := \mathcal{X}_2 \setminus \{x_2\}$ and pick $x_3 \in \mathcal{X}_3$ such that

$$\det(\alpha_i^{x_j})_{1 \leq i,j \leq 3} \neq 0. \tag{2.5}$$

Again, this is still possible since, by the choice of x_2, (2.5) is a nontrivial exponential equation and

$$\#\mathcal{X}_3 = s - 2 \geq C(r) + r - 2 > C(r).$$

Continuing in this way, after $r - 1$ steps, we obtain integers $x_2, \dots, x_r \in [1, T_F(p))$ such that

$$D_F(0, x_2, \dots, x_r) \neq 0. \tag{2.6}$$

Now, since $f_i(\ell)$ are not all zero modulo π, by (2.4),

$$\det(\alpha_i^{px_j})_{1 \leq i,j \leq r} \equiv 0 \pmod{\pi},$$

so that

$$N_{\mathbb{K}}(D_F(0, x_2, \dots, x_r))^p = N_{\mathbb{K}}(\det(\alpha_i^{x_j}))^p \equiv N_{\mathbb{K}}(\det(\alpha_i^{px_j})) \equiv 0 \pmod{p},$$

which is impossible by the definition of $T_F(p)$ and condition (2.6). Hence, $s < C(r) + r$ and the desired claim follows easily. □

Our final lemma is a consequence of Bézout's theorem.

Lemma 2.6. *If* $\gcd(G, f_1, \dots, f_r) = 1$, *then there are only finitely many prime numbers* p *such that* $p \mid G(\ell)$, *for some integer* ℓ, *and* $f_1(\ell), \dots, f_r(\ell)$ *are all zero modulo some prime ideal of* $O_{\mathbb{K}}$ *lying over* p.

Proof. By Bézout's theorem for polynomials in $\mathbb{K}[X]$, there exist $h_0, \dots, h_r \in \mathbb{K}[X]$ such that

$$Gh_0 + f_1 h_1 + \cdots + f_r h_r = 1.$$

Let B be a positive integer such that all the coefficients of $Bh_0, \dots, Bh_r$ are algebraic integers. If π is a prime ideal of $O_{\mathbb{K}}$ lying over p such that $f_1(\ell), \dots, f_r(\ell)$ are all zero modulo π, then

$$B \equiv BG(l)h_0(l) + Bf_1(l)h_1(l) + \cdots + Bf_r(l)h_r(l) \equiv 0 \pmod{\pi},$$

since $p \mid G(\ell)$. Hence, $p \mid B$ and this is possible only for finitely many primes p. □

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

3. Proof of Theorem 1.4

We begin by proving that $\mathcal{A}_{F,G,h}$ has a natural density. First, in light of Lemma 2.1, without loss of generality, we can assume that F is nondegenerate and not identically zero, and that $h = 1$. By Lemma 2.2, if $G, f_1, \dots, f_r$ share a nontrivial common factor, then $\mathcal{A}_{F,G}$ is finite and, obviously, $\mathbf{d}(\mathcal{A}_{F,G}) = 0$. Therefore, we can also assume that $\gcd(G, f_1, \dots, f_r) = 1$.

Put $C_{F,G} := \mathbb{N} \setminus \mathcal{A}_{F,G}$, so that, equivalently, we have to prove that the natural density of $C_{F,G}$ exists. For each $y > 0$, we split $C_{F,G}$ into two subsets:

$$C^-_{F,G,y} := \{n \in C_{F,G} : p \mid \gcd(G(n), F(n)) \text{ for some } p \le y\},$$
$$C^+_{F,G,y} := C_{F,G} \setminus C^-_{F,G,y}.$$

Recalling that F, G are ultimately periodic modulo p, for any prime number p, we see that $C^-_{F,G,y}$ is a union of finitely many arithmetic progressions and a finite subset of $\mathbb{N}$. In particular, $C^-_{F,G,y}$ has a natural density. If we put $\delta_y := \mathbf{d}(C^-_{F,G,y})$, then it is clear that δ_y is a bounded nondecreasing function of y. Hence, the limit

$$\delta := \lim_{y \to +\infty} \delta_y \tag{3.1}$$

exists and is finite. We shall prove that $C_{F,G}$ has natural density δ. If $n \in C^+_{F,G,y}(x)$, then there exists a prime $p > y$ such that $p \mid G(n)$ and $p \mid F(n)$. In particular, we can write $n = pm + \ell$, for some nonnegative integers $m \le x/p$ and $\ell < p$, with $p \mid G(\ell)$. For sufficiently large y, how large depending only on F, G, we see that p divides neither a_k nor any of the denominators of the coefficients of $f_1, \dots, f_r$ and that, by Lemma 2.6, the terms $f_1(\ell), \dots, f_2(\ell)$ are not all zero modulo some prime ideal of $\mathcal{O}_{\mathbb{K}}$ lying over p. On the one hand, by Lemma 2.5, the number of possible values for m is

$$O_r\left(\frac{x}{pT_F(p)} + 1\right).$$

On the other hand, for sufficiently large y, depending on G, the number of possible values for ℓ is at most $\deg(G)$. Furthermore, we have $p \ll_G x$, since all the roots of G are in $\mathbb{Q}$. (Note that this property is preserved by the reduction to $\widetilde{G}$ in Lemma 2.1.) Therefore, setting $\gamma := 1/(r+1)$,

$$\#C^+_{F,G,y}(x) \ll_{F,G} \sum_{y < p \ll_G x} \left(\frac{x}{pT_F(p)} + 1\right) \ll_{F,G} \frac{x}{y^\gamma} + \frac{x}{\log x}, \tag{3.2}$$

where we used Lemma 2.4 and Chebyshev's estimate for the number of primes not exceeding x. Thus,

$$\begin{aligned}\limsup_{x \to +\infty} \left|\frac{\#C_{F,G}(x)}{x} - \delta_y\right| &= \limsup_{x \to +\infty} \left|\frac{\#C_{F,G}(x)}{x} - \frac{\#C^-_{F,G,y}(x)}{x}\right| \\ &= \limsup_{x \to +\infty} \frac{\#C^+_{F,G,y}(x)}{x} \ll_{F,G} \frac{1}{y^\gamma}.\end{aligned} \tag{3.3}$$

Hence, letting $y \to +\infty$ in (3.3) and using (3.1), we see that $C_{F,G}$ has natural density δ.

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

At this point, assuming that G has no fixed divisors, it remains only to prove that the natural density of $A_{F,G}$ is positive. In turn, this is equivalent to $\delta < 1$. Clearly,

$$C^-_{F,G,y} \subseteq \{n \in \mathbb{N} : p \mid G(n) \text{ for some } p \le y\}.$$

Hence, by standard sieving arguments (see, for example, [10, Section 1.2.3, Equation (3.3)]),

$$\frac{\#C^-_{F,G,y}(x)}{x} \le 1 - \prod_{p \le y}\left(1 - \frac{\rho_G(p)}{p}\right) + O_G\Big(\frac{1}{x}\sum_{d \mid P(y)} \rho_G(d)\Big),$$

where $P(y) := \prod_{p \le y} p$, while ρ_G is the completely multiplicative function supported on squarefree numbers and satisfying

$$\rho_G(p) := \frac{\#\{z \in \{1, \dots, p^{1+\nu_p(B)}\} : BG(z) \equiv 0 \pmod{p^{1+\nu_p(B)}}\}}{p^{\nu_p(B)}},$$

for all prime numbers p, where B is a positive integer such that $BG \in \mathbb{Z}[X]$. Since G has no fixed divisors, $\rho_G(p) < p$ for all prime numbers p. Also, $\rho_G(p) \le \deg(G)$ for all sufficiently large prime numbers p. Therefore,

$$\prod_{p \le y}\left(1 - \frac{\rho_G(p)}{p}\right) \gg_G \frac{1}{(\log y)^{\deg(G)}}$$

if y is large enough, which implies that

$$\limsup_{x \to +\infty} \frac{\#C^-_{F,G,y}(x)}{x} \le 1 - \frac{c_1}{(\log y)^{\deg(G)}}, \tag{3.4}$$

where $c_1 > 0$ is a constant depending on G. Recall that δ is defined by (3.1) and that we proved that δ is equal to the natural density of $C_{F,G}$. Hence, putting together (3.3) and (3.4),

$$\begin{aligned}\delta = \lim_{x \to +\infty} \frac{\#C_{F,G}(x)}{x} &\le \limsup_{x \to +\infty} \frac{\#C^-_{F,G,y}(x)}{x} + \limsup_{x \to +\infty} \frac{\#C^+_{F,G,y}(x)}{x} \\ &\le 1 - \left(\frac{c_1}{(\log y)^{\deg(G)}} - \frac{c_2}{y^\gamma}\right),\end{aligned} \tag{3.5}$$

where $c_2 > 0$ is a constant depending on F, G. Finally, picking a sufficiently large y, depending on c_1 and c_2, the bound (3.5) yields $\delta < 1$, as desired. The proof of Theorem 1.4 is complete.

4. Concluding remarks

4.1. The case in which G has a fixed divisor. Suppose that F is a nondegenerate integral linear recurrence and that G is an integer-valued polynomial with all roots in $\mathbb{Q}$ and having a fixed divisor $d > 1$. In order to study $\mathcal{A}_{F,G}$, one could try to

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

reduce from this general situation to the one where there is no fixed divisor, so that Theorem 1.4 can be applied. However, the strategy used in Lemma 2.1, that is, writing $\mathcal{A}_{F,G}$ as the disjoint union of a finite set and finitely many sets of the form $a\mathcal{A}_{\widetilde{F},\widetilde{G}} + b$, now does not work. The issue is that the resulting polynomials $\widetilde{G}$ may have fixed divisors. For example, let F be the Fibonacci sequence and $G(n) = n(n+1)$, so that $d = 2$. Then $2 \nmid F(n)$ if and only if $n \equiv 1, 2 \pmod 3$, so that $\mathcal{A}_{F,G}$ is the disjoint union of $\mathcal{A}_{\widetilde{F}_1,\widetilde{G}_1}$ and $\mathcal{A}_{\widetilde{F}_2,\widetilde{G}_2}$, where $\widetilde{F}_i(m) = F(3m+i)$ and $\widetilde{G}_i(m) = G(3m+i)/2$ for $i = 1, 2$. Now, $G_1(m) = (9m^2 + 9m + 2)/2$ has no fixed divisors, but $G_2(m) = (9m^2 + 15m + 6)/2$ gained 3 as a new fixed divisor.

4.2. The case in which G does not split over the rationals. We note that there are examples of integral linear recurrences F and integer-valued polynomials G, not splitting over the rationals, such that $\mathcal{A}_{F,G}$ has a positive density for elementary reasons. For instance, for the following pair

$$F(n) = (n^2+1)5^n + (n^2+2)3^n, \quad G(n) = (n^2+1)(n^2+2),$$

we have $\mathcal{A}_{F,G} = \mathbb{N}$. Indeed, suppose by contradiction that there exists a prime p dividing both $F(n)$ and $G(n)$. Then $p \mid (n^2+1)$ or $p \mid (n^2+2)$, exclusively. In the first case, since $p \mid F(n)$, we get $p \mid 3^n$, that is, $p = 3$, which is not possible, since $n^2 + 1$ is never a multiple of 3. The second case is similar.

However, except for those easy situations, we think that if G does not split over the rationals, then the study of $\mathcal{A}_{F,G}$ requires different methods to those employed in this paper. In fact, if $p \mid G(n)$, we can only say that $p \ll_G x^{\deg(G)}$ and, for $\deg(G) \geq 2$, this does not allow one to conclude that $\limsup_{x\to+\infty} C^+_{F,G,y}(x)/x = o((\log y)^{-\deg(G)})$ as $y \to +\infty$, which is a key step in the proof of Theorem 1.4. In the following, we provide a heuristic for the claim that $C^+_{F,G,y}(x) \gg x$ for all y. First, we can split $C^+_{F,G,y}(x)$ into two parts: the first one is

$$\{n \leq x : \gcd(F(n), G(n)) \neq 1 \text{ and } p \mid \gcd(F(n), G(n)) \Rightarrow y < p \leq x\},$$

which can be handled as in (3.2), whereas the second one is

$$\{n \leq x : \exists p \mid \gcd(F(n), G(n)) \text{ with } p > x\}, \tag{4.1}$$

which, by our heuristic, we believe should have cardinality $\gg x$.

For the sake of simplicity, we consider only the case where F is the Fibonacci sequence and $G(n) = n^2 + 1$. By a result of Everest and Harman about the existence of primitive divisors of quadratic polynomials [7, Theorem 1.4],

$$\#\{n \leq x : \exists p > x \text{ with } p \mid G(n)\} \gg x,$$

so that

$$\mathbb{P}_x[\exists p > x \text{ with } p \mid G(n)] \gg 1,$$

where we consider the events in the probability space $([x], \mathcal{P}[x], \mathbb{P}_x)$, with $[x] = \{n \leq x\}$ and $\mathbb{P}_x$ is the discrete uniform measure on $[x]$. Let $z_F(m)$ be the least positive integer n

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

such that $m \mid F(n)$. It is well known that $p \mid F(n)$ if and only if $z_F(p) \mid n$. This means that $\mathbb{P}_x[p \mid F(n)]$ is roughly $1/z_F(p)$. Therefore, interpreting the events of being divisible by different prime numbers as independent, we expect that

$$\begin{aligned}\mathbb{P}_x[\exists p > x \text{ with } p \mid F(n)] &\geq 1 - \mathbb{P}_x[p \nmid F(n) \text{ for all } p \text{ with } x < p \ll x^2] \\ &= 1 - \prod_{p:\ x<p\ll x^2} \left(1 - \frac{1}{z_F(p)}\right) > 1 - \prod_{p:\ x<p\ll x^2} \left(1 - \frac{1}{p+1}\right) > 1/2 + o(1)\end{aligned}$$

as $x \to +\infty$, since $z_F(p) \leq p + 1$ and thanks to Mertens' theorem. Assuming independence between the events that a prime divides $F(n)$ or $G(n)$, we deduce that the expected value of the cardinality of (4.1) is

$$\begin{aligned}&\sum_{n\leq x} \mathbb{P}_x[\exists p > x \text{ with } p \mid \gcd(F(n), G(n))] \\ &\quad = \sum_{n\leq x} \mathbb{P}_x[\exists p > x \text{ with } p \mid F(n)] \cdot \mathbb{P}_x[\exists p > x \text{ with } p \mid G(n)] \gg x,\end{aligned}$$

as claimed.

References

[1] N. Ailon and Z. Rudnick, 'Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$', *Acta Arith.* **113**(1) (2004), 31–38.

[2] J. J. Alba González, F. Luca, C. Pomerance and I. E. Shparlinski, 'On numbers n dividing the nth term of a linear recurrence', *Proc. Edinb. Math. Soc. (2)* **55**(2) (2012), 271–289.

[3] R. André-Jeannin, 'Divisibility of generalized Fibonacci and Lucas numbers by their subscripts', *Fibonacci Quart.* **29**(4) (1991), 364–366.

[4] Y. Bugeaud, P. Corvaja and U. Zannier, 'An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$', *Math. Z.* **243**(1) (2003), 79–84.

[5] P. Corvaja and U. Zannier, 'Diophantine equations with power sums and universal Hilbert sets', *Indag. Math. (N.S.)* **9**(3) (1998), 317–332.

[6] P. Corvaja and U. Zannier, 'Finiteness of integral values for the ratio of two linear recurrences', *Invent. Math.* **149**(2) (2002), 431–451.

[7] G. Everest and G. Harman, 'On primitive divisors of $n^2 + b$', in: *Number Theory and Polynomials*, London Mathematical Society Lecture Note Series, 352 (eds. J. McKee and C. Smyth) (Cambridge University Press, Cambridge, 2008), 142–154.

[8] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, 104 (American Mathematical Society, Providence, RI, 2003).

[9] C. Fuchs, 'An upper bound for the G.C.D. of two linear recurring sequences', *Math. Slovaca* **53**(1) (2003), 21–42.

[10] G. Greaves, *Sieves in Number Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 43 (Springer, Berlin, 2001).

[11] S. Kim, 'The density of the terms in an elliptic divisibility sequence having a fixed G.C.D. with their index', Preprint, 2017, arXiv:1708.08357.

[12] P. Leonetti and C. Sanna, 'On the greatest common divisor of n and the nth Fibonacci number', *Rocky Mountain J. Math.* to appear.

[13] F. Luca and E. Tron, 'The distribution of self-Fibonacci divisors', in: *Advances in the Theory of Numbers*, Fields Institute Communications, 77 (Fields Institute for Research in Mathematical Sciences, Toronto, ON, 2015), 149–158.

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press

[14] C. Sanna, 'Distribution of integral values for the ratio of two linear recurrences', *J. Number Theory* **180** (2017), 195–207.
[15] C. Sanna, 'On numbers n dividing the nth term of a Lucas sequence', *Int. J. Number Theory* **13**(3) (2017), 725–734.
[16] C. Sanna, 'The moments of the logarithm of a G.C.D. related to Lucas sequences', *J. Number Theory* **191** (2018), 305–315.
[17] C. Sanna, 'On numbers n relatively prime to the nth term of a linear recurrence', *Bull. Malays. Math. Sci. Soc.* (online ready), https://doi.org/10.1007/s40840-017-0514-8.
[18] C. Sanna and E. Tron, 'The density of numbers n having a prescribed G.C.D. with the nth Fibonacci number', *Indag. Math. (N.S.)* **29**(3) (2018), 972–980.
[19] H. P. Schlickewei, 'Multiplicities of recurrence sequences', *Acta Math.* **176**(2) (1996), 171–243.
[20] I. E. Shparlinski, 'The number of different prime divisors of recurrent sequences', *Mat. Zametki* **42**(4) (1987), 494–507, 622; English translation, *Math. Notes* **42**(4) (1987), 773–780.
[21] C. Smyth, 'The terms in Lucas sequences divisible by their indices', *J. Integer Seq.* **13**(2) (2010), Article 10.2.4, 18 pages.
[22] L. Somer, 'Divisibility of terms in Lucas sequences by their subscripts', in: *Applications of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992)* (Kluwer Academic, Dordrecht, 1993), 515–525.
[23] A. J. van der Poorten, 'Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles', *C. R. Acad. Sci. Paris Sér. I Math.* **306**(3) (1988), 97–102.

DANIELE MASTROSTEFANO, Mathematics Institute,
Zeeman Building, University of Warwick, Coventry, CV4 7AL, UK
e-mail: danymastro93@hotmail.it

CARLO SANNA, Department of Mathematics,
Università degli Studi di Torino, Turin, Italy
e-mail: carlo.sanna.dev@gmail.com

https://doi.org/10.1017/S0004972718000606 Published online by Cambridge University Press