Distribution of integral values for the ratio of two linear recurrences

Published version:

DOI:10.1016/j.jnt.2017.04.015

DISTRIBUTION OF INTEGRAL VALUES FOR THE RATIO OF TWO LINEAR RECURRENCES

CARLO SANNA

Abstract. Let F and G be linear recurrences over a number field $\mathbb{K}$, and let $\mathfrak{R}$ be a finitely generated subring of $\mathbb{K}$. Furthermore, let $\mathcal{N}$ be the set of positive integers n such that $G(n) \neq 0$ and $F(n)/G(n) \in \mathfrak{R}$. Under mild hypothesis, Corvaja and Zannier proved that $\mathcal{N}$ has zero asymptotic density. We prove that $\#(\mathcal{N} \cap [1, x]) \ll x \cdot (\log\log x / \log x)^h$ for all $x \geq 3$, where h is a positive integer that can be computed in terms of F and G. Assuming the Hardy–Littlewood k-tuple conjecture, our result is optimal except for the term $\log\log x$.

1. Introduction

A sequence of complex numbers $F(n)_{n\in\mathbb{N}}$ is called a *linear recurrence* if there exist some $c_0, \dots, c_{k-1} \in \mathbb{C}$ $(k \geq 1)$, with $c_0 \neq 0$, such that

$$F(n+k) = \sum_{j=0}^{k-1} c_j F(n+j),$$

for all $n \in \mathbb{N}$. In turn, this is equivalent to an (unique) expression

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

for all $n \in \mathbb{N}$, where $f_1, \dots, f_r \in \mathbb{C}[X]$ are nonzero polynomials and $\alpha_1, \dots, \alpha_r \in \mathbb{C}^*$ are all the distinct roots of the polynomial

$$X^k - c_{k-1}X^{k-1} - \cdots - c_1 X - c_0.$$

Classically, $\alpha_1, \dots, \alpha_r$ and k are called the *roots* and the *order* of F, respectively. Furthermore, F is said to be *nondegenerate* if none the ratios α_i/α_j $(i \neq j)$ is a root of unity, and F is said to be *simple* if all the $f_1, \dots, f_r$ are constant. We refer the reader to [8, Ch. 1–8] for the general theory of linear recurrences.

Hereafter, let F and G be linear recurrences and let $\mathfrak{R}$ be a finitely generated subring of $\mathbb{C}$. Assume also that the roots of F and G together generate a multiplicative torsion-free group. This “torsion-free” hypothesis is not a loss of generality. Indeed, if the group generated by the roots of F and G has torsion order q, then for each $r = 0, 1, \dots, q-1$ the roots of the linear recurrences $F_r(n) = F(qn + r)$ and $G_r(n) = G(qn + r)$ generate a torsion-free group. Therefore, all the results in the following can be extended just by partitioning $\mathbb{N}$ into the arithmetic progressions of modulo q and by studying each pair of linear recurrences F_r, G_r separately. Finally, define the following set of natural numbers

$$\mathcal{N} := \{n \in \mathbb{N} : G(n) \neq 0,\ F(n)/G(n) \in \mathfrak{R}\}.$$

Regarding the condition $G(n) \neq 0$, note that, by the “torsion-free” hypothesis, $G(n)$ is nondegenerate and hence the Skolem–Mahler–Lech Theorem [8, Theorem 2.1] implies that $G(n) = 0$ only for finitely many $n \in \mathbb{N}$. In the sequel, we shall tacitly disregard such integers.

Divisibility properties of linear recurrences have been studied by several authors. A classical result, conjectured by Pisot and proved by van der Poorten, is the Hadamard-quotient

2010 *Mathematics Subject Classification.* Primary: 11B37 Secondary: 11A07, 11N25.
Key words and phrases. linear recurrence; divisibility.

Theorem, which states that if $\mathcal{N}$ contains all sufficiently large integers, then F/G is itself a linear recurrence [13, 21].

Corvaja and Zannier [7, Theorem 2] gave the following wide extension of the Hadamard-quotient Theorem (see also [6] for a previous weaker result by the same authors).

Theorem 1.1. *If $\mathcal{N}$ is infinite, then there exists a nonzero polynomial $P \in \mathbb{C}[X]$ such that both the sequences $n \mapsto P(n)F(n)/G(n)$ and $n \mapsto G(n)/P(n)$ are linear recurrences.*

The proof of Theorem 1.1 makes use of the Schmidt's Subspace Theorem. We refer the reader to [4] for a survey on several applications of the Schmidt's Subspace Theorem in Number Theory.

Let $\mathbb{K}$ be a number field. For the sake of simplicity, from now on we shall assume that $\mathfrak{R} \subseteq \mathbb{K}$ and that F and G have coefficients and values in $\mathbb{K}$. We recall that a set of natural numbers $\mathcal{S}$ has zero asymptotic density if $\#\mathcal{S}(x)/x \to 0$, as $x \to +\infty$, where we define $\mathcal{S}(x) := \mathcal{S} \cap [1, x]$ for all $x \geq 1$. Corvaja and Zannier [7, Corollary 2] proved the following theorem about $\mathcal{N}$.

Theorem 1.2. *If F/G is not a linear recurrence, then $\mathcal{N}$ has zero asymptotic density.*

Corvaja and Zannier also suggested [7, Remark p. 450] that their proof of Theorem 1.2 could be adapted to show that if F/G is not a linear recurrence then

$$\#\mathcal{N}(x) \ll \frac{x}{(\log x)^{\delta}}, \tag{1}$$

for any $\delta < 1$ and for all sufficiently large $x > 1$, where the implied constant depends on $\mathbb{K}$.

In our main result we obtain a more precise upper bound than (1). Before stating it, we mention some special cases of the problem of bounding $\#\mathcal{N}(x)$ that have already been studied.

Alba González, Luca, Pomerance, and Shparlinski [1, Theorem 1.1] proved the following:

Theorem 1.3. *If F is a simple nondegenerate linear recurrence over the integers, $r \geq 2$, $G(n) = n$, and $\mathcal{R} = \mathbb{Z}$, then*

$$\#\mathcal{N}(x) \ll \frac{x}{\log x},$$

for all sufficiently large $x > 1$, where the implied constant depends only on r.

For $G(n) = n$ and $\mathcal{R} = \mathbb{Z}$, a still better upper bound can be given if F is a Lucas sequence, that is, $F(0) = 0$, $F(1) = 1$, and $F(n+2) = aF(n+1) + bF(n)$, for all $n \in \mathbb{N}$ and some fixed integers a and b. In such a case the arithmetic properties of $\mathcal{N}$ were first investigated by André-Jeannin [3] and Somer [18, 19]. Luca and Tron [12] studied the case in which F is the sequence of Fibonacci numbers ($a = b = 1$) and Sanna [15], using some results on the p-adic valuation of Lucas sequences [14], generalized Luca and Tron's result to the following upper bound.

Theorem 1.4. *If F is a nondegenerate Lucas sequences, $G(n) = n$, and $\mathcal{R} = \mathbb{Z}$, then*

$$\#\mathcal{N}(x) \leq x^{1-\left(\frac{1}{2}+o(1)\right)\frac{\log\log\log x}{\log\log x}},$$

as $x \to +\infty$, where the $o(1)$ depends on F.

Now we state the main result of this paper.

Theorem 1.5. *If F/G is not a linear recurrence, then*

$$\#\mathcal{N}(x) \ll_{F,G} x \cdot \left(\frac{\log\log x}{\log x}\right)^h,$$

for all $x \geq 3$, where h is a positive integer depending on F and G.

Both the positive integer h and the implied constant in the bound of Theorem 1.5 are effectively computable, we give the details in §4. In particular, we have the following corollary.

Corollary 1.1. *If F/G is not a linear recurrence, $G \in \mathbb{Z}[X]$, and $\gcd(G, f_1, \ldots, f_r) = 1$, then h can be taken as the number of irreducible factors of G in $\mathbb{Z}[X]$ (counted without multiplicity).*

Except for the term $\log\log x$, Corollary 1.1 should be optimal. Indeed, pick a positive integer h and an *admissible* h-tuple $\mathbf{h} = (n_1, \dots, n_h)$, that is, $n_1 < \cdots < n_h$ are positive integers such that for each prime number p there exists a residue class modulo p which does not intersect $\{n_1, \dots, n_h\}$. Assuming the Hardy–Littlewood h-tuple conjecture [9, p. 61], we have that the number $T_{\mathbf{h}}(x)$ of positive integers $n \leq x$ such that $n + n_1, \dots, n + n_h$ are all prime numbers satisfies

$$T_{\mathbf{h}}(x) \sim C_{\mathbf{h}} \cdot \frac{x}{(\log x)^h},$$

as $x \to +\infty$, where $C_{\mathbf{h}} > 0$ depends on $\mathbf{h}$. Therefore, taking $F(n) = (2^{n+n_1} - 2) \cdots (2^{n+n_h} - 2)$ and $G(n) = (n + n_1) \cdots (n + n_h)$, we obtain

$$\#\mathcal{N}(x) \geq T_{\mathbf{h}}(x) \gg \frac{x}{(\log x)^h},$$

for all sufficiently large $x > 1$.

Notation. Hereafter, the letter p always denotes a prime number. 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. If $A \ll B$ and $A \gg B$, we write $A \asymp B$. Any dependence of implied constants is explicitly stated or indicated with subscripts.

2. Preliminaries

First, we need a quantitative form of a result due to Kronecker [11] (see also [20, p. 32]), which states that the average number of zeros modulo p of a nonconstant polynomial $f \in \mathbb{Z}[X]$ is equal to the number of irreducible factors of f in $\mathbb{Z}[X]$.

Lemma 2.1. *Given a nonconstant polynomial $f \in \mathbb{Z}[X]$, for each prime number p let $\eta_f(p)$ be the number of zeros of f modulo p. Then*

$$\sum_{p \leq x} \eta_f(p) \cdot \frac{\log p}{p} = h \log x + O_f(1),$$

for all $x \geq 1$, where h is the number of irreducible factors of f in $\mathbb{Z}[X]$.

Proof. It is enough to prove the claim for irreducible f. Let $\mathbb{L}$ be the splitting field of f over $\mathbb{Q}$ and let $\mathcal{G} := \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. For any coniugacy class C of $\mathcal{G}$, let $\pi_C(x)$ be the number of primes $p \leq x$ which do not ramified in $\mathbb{L}$ and such that their Frobenius substitutions σ_p belong to C. A quantitative version of the Chebotarev's density theorem [17, Theorem 3.4] states that

$$\pi_C(x) = \frac{\#C}{\#\mathcal{G}} \cdot \mathrm{Li}(x) + O_{\mathbb{L}}\left(\frac{x}{\exp(C\sqrt{\log x})}\right),$$

for $x \to +\infty$, where $\mathrm{Li}(x)$ is the logarithmic integral function and $C > 0$ is a constant depending on $\mathbb{L}$. If the elements of C have cycle pattern $d_1, \dots, d_s$, when regarded as permutations of the roots of f, then $\pi_C(x)$ is the number of primes $p \leq x$ not dividing the discriminant of f and such that the irreducible factors of f modulo p have degrees $d_1, \dots, d_s$.

Furthermore, $\mathcal{G}$ acts transitively on the roots of f, since f is irreducible, hence

$$\sum_{g \in \mathcal{G}} \#X^g = \#\mathcal{G},$$

by Burnside's lemma, where X^g is the set of roots of f which are fixed by g. Therefore,

$$\sum_{p \leq x} \eta_f(p) = \mathrm{Li}(x) + O_{\mathbb{L}}\left(\frac{x}{\exp(C\sqrt{\log x})}\right),$$

and the desired result follows by partial summation. ∎

The following lemma [7, Lemma A.2] regards the minimum of the multiplicative orders of some fixed algebraic numbers modulo a prime ideal.

Lemma 2.2. *Let $\beta_1, \dots, \beta_s \in \mathbb{K}$ such that none of them is zero or a root of unity. Then, for all $x \geq 1$, the number of prime numbers $p \leq x$ such that some β_i has order less than $p^{1/4}$ modulo some prime ideal of $\mathcal{O}_\mathbb{K}$ lying above p is $O(x^{1/2})$, where the implied constant depends only on $\beta_1, \dots, \beta_s$.*

Given a multiplicative function g, let Λ_g be its *associated von Mangoldt function*, that is, the unique arithmetic function satisfying

$$\sum_{d \,|\, n} g(n/d)\Lambda_g(d) = g(n) \log n,$$

for all positive integers n (see [10, p. 17]). It is easy to prove that Λ_g is supported on prime powers.

Theorem 2.3. *For each $y > 0$, let g_y be a multiplicative arithmetic function and let $L_y > 0$. Suppose that*

$$\sum_{n \leq x} \Lambda_{g_y}(n) = h \log x + O(L_y) \tag{2}$$

and

$$\sum_{n \leq x} |g_y(n)| \ll (\log x)^h, \tag{3}$$

for all $x, y \geq 2$, where $h > 0$ is some constant. Then

$$\sum_{n \leq x} g_y(n) = (\log x)^h \cdot \left(c_{g_y} + O_h\!\left(\frac{L_y}{\log x}\right)\right),$$

for all $x, y \geq 2$, where

$$c_{g_y} := \frac{1}{\Gamma(h+1)} \prod_p \left(1 + g_y(p) + g_y(p^2) + \cdots\right)\left(1 - \frac{1}{p}\right)^h$$

and Γ is the Euler's Gamma function.

Proof. The proof proceeds exactly as the proof of [10, Theorem 1.1], but using the error term $O(L_y)$ instead of $O(1)$. ◻

Now we state a technical lemma about the cardinality of a sieved set of integers.

Lemma 2.4. *For each prime number p, let $\Omega_p \subsetneq \{0, 1, \dots, p-1\}$ be a set of residues modulo p. Suppose that there exist constants $c, h > 0$ such that $\#\Omega_p \leq c$ for each prime number p and*

$$\sum_{p \leq x} \#\Omega_p \cdot \frac{\log p}{p} = h \log x + O(1), \tag{4}$$

for all $x > 1$. Then we have

$$\#\left\{n \leq x : (n \bmod p) \notin \Omega_p,\ \forall p \in \,]y, z]\right\} \ll_{c,h,\delta_1,\delta_2} x \cdot \left(\frac{\log y}{\log x}\right)^h,$$

for all $\delta_1, \delta_2 > 0$, $x > 1$, $2 \leq y \leq (\log x)^{\delta_1}$, and $z \geq x^{\delta_2}$.

Proof. All the constants in this proof, included the implied ones, may depend on c, h, δ_1, δ_2. Clearly, we can assume $\delta_2 \leq 1/2$. By the large sieve inequality [10, Theorem 7.14], we have

$$\#\left\{n \leq x : (n \bmod p) \notin \Omega_p,\ \forall p \in \,]y, z]\right\} \ll x \cdot \left(\sum_{m \leq w} g_y(m)\right)^{-1}, \tag{5}$$

where $w := x^{\delta_2}$ and g_y is the multiplicative arithmetic function supported on squarefree numbers with all prime factors $> y$ and such that

$$g_y(p) = \frac{\#\Omega_p}{p - \#\Omega_p},$$

for any prime number $p > y$.

For sufficiently large x, we have $y \leq w$, and it follows from (4) and $\#\Omega_p \leq c_1$ that

$$\sum_{p \leq w} g_y(p) \log p = h \log w + O(\log y),$$

which in turn implies that

$$\sum_{n \leq w} \Lambda_{g_y}(n) = h \log w + O(\log y),$$

since Λ_{g_y} is supported on prime powers p^s, with $p > y$, and $\Lambda_{g_y}(p^s) = -(-g_y(p))^s \log p$.

Furthermore, again from (4) and $\#\Omega_p \leq c_1$, we have

$$\prod_{p \leq t} \left(1 - \frac{\#\Omega_p}{p}\right)^{-1} \asymp (\log t)^h, \tag{6}$$

for all $t \geq 2$, so that

$$\sum_{n \leq w} |g_y(n)| \leq \prod_{p \leq w} (1 + g_y(p)) \leq \prod_{p \leq w} \left(1 - \frac{\#\Omega_p}{p}\right)^{-1} \ll (\log w)^h.$$

At this point, we have proved that (2) and (3) hold with $L_y = \log y$. Therefore, by Theorem 2.3 we have

$$\sum_{n \leq w} g_y(n) = (\log w)^h \cdot \left(c_{g_y} + O\left(\frac{\log y}{\log w}\right)\right), \tag{7}$$

where

$$c_{g_y} = \frac{1}{\Gamma(h+1)} \prod_p (1 + g_y(p)) \left(1 - \frac{1}{p}\right)^h.$$

Now using (6) we obtain

$$c_{g_y} = \frac{1}{\Gamma(h+1)} \prod_p \left(1 - \frac{\#\Omega_p}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^h \prod_{p \leq y} \left(1 - \frac{\#\Omega_p}{p}\right) \gg \frac{1}{(\log y)^h}. \tag{8}$$

Hence, recalling that $y \leq (\log x)^{\delta_1}$ and $w = x^{\delta_2}$, by (7) and (8) we find that

$$\sum_{n \leq w} g_y(n) \gg \left(\frac{\log w}{\log x}\right)^h \gg \left(\frac{\log x}{\log y}\right)^h. \tag{9}$$

Putting together (5) and (9), the desired result follows. □

We need a lemma about the number of zeros of a sparse polynomial in a finite field of q elements $\mathbb{F}_q$ [5, Lemma 7].

Lemma 2.5. *Let $c_1, \ldots, c_r \in \mathbb{F}_q^*$ ($r \geq 2$) and $t_1, \ldots, t_r \in \mathbb{Z}$. Then the number T of solutions of the equation*

$$\sum_{i=1}^{r} c_i x^{t_i} = 0, \quad x \in \mathbb{F}_q^* \tag{10}$$

satisfies

$$T \leq 2q^{1-1/(r-1)} D^{1/(r-1)} + O(q^{1-2/(r-1)} D^{2/(r-1)}),$$

where

$$D := \min_{1 \leq i \leq r} \max_{j \neq i} \gcd(t_i - t_j, q - 1).$$

We will use the following corollary of Lemma 2.5, which concerns the number of zeros of a simple linear recurrence in a finite field.

Corollary 2.1. *Let $c_1, \dots, c_r, a_1, \dots, a_r \in \mathbb{F}_q^*$ $(r \geq 2)$, and let N be the minimum of the orders of the a_i/a_j $(i \neq j)$ in $\mathbb{F}_q^*$. Then the number of integers $m \in [0, q-2]$ such that*

$$\sum_{i=1}^{r} c_i a_i^m = 0 \tag{11}$$

is $O\big(qN^{-1/(r-1)}\big)$.

Proof. Let g be a generator of the multiplicative group $\mathbb{F}_q^*$, so that for each $i = 1, \dots, r$ we have $a_i = g^{t_i}$ for some integer t_i. Clearly, m is a solution of (11) if and only if g^m is a solution of (10). Finally, the order of a_i/a_j $(i \neq j)$ is given by $(q-1)/\gcd(t_i - t_j, q-1)$, hence $D \leq (q-1)/N$, and the desidered claim follows. $\square$

Given a finite set S of absolute values of $\mathbb{K}$ containing all the archimedean ones, we write $\mathcal{O}_S$ for the ring of S-integers of $\mathbb{K}$, that is, the set of all $\alpha \in \mathbb{K}$ such that $|\alpha|_v \leq 1$ for all $v \notin S$. We state the following easy lemma.

Lemma 2.6. *Let S be a finite set of absolute values of $\mathbb{K}$ containing all the archimedean ones, and let $g_1, \dots, g_t \in \mathbb{K}[X]$ be polynomials such that $(g_1, \dots, g_t) = 1$. Then there exists a finite set S' of absolute values of $\mathbb{K}$, such that: $S \subseteq S'$, $g_1, \dots, g_t \in \mathcal{O}_{S'}[X]$, and $(g_1(n), \dots, g_t(n)) = 1$ for all positive integers n, that is, the ideal of $\mathcal{O}_{S'}$ generated by $g_1(n), \dots, g_t(n)$ is the whole $\mathcal{O}_{S'}$.*

Proof. Since $(g_1, \dots, g_t) = 1$, by the Bézout's identity there exist $b_1, \dots, b_t \in \mathbb{K}[X]$ such that

$$b_1 g_1 + \cdots + b_t g_t = 1.$$

Clearly, we can pick S' so that $S' \supseteq S$ and $b_i, g_i \in \mathcal{O}_{S'}[X]$ for all $i = 1, \dots, t$. Hence, for each $n \in \mathbb{N}$, we have

$$b_1(n) g_1(n) + \cdots + b_t(n) g_t(n) = 1,$$

which in turn implies that $(g_1(n), \dots, g_t(n)) = 1$. $\square$

3. Proof of Theorem 1.5

The first part of the proof proceeds similarly to the proof of Theorem 1.2. If $\mathcal{N}$ is finite, then the claim is trivial, hence we suppose that $\mathcal{N}$ is infinite. Then, by Theorem 1.1 it follows that $F/G = H/P$, for some linear recurrence H and some polynomial P. As a consequence, without loss of generality, we shall assume that G is a polynomial.

Let S be a finite set of absolute values of $\mathbb{K}$ containing all the archimedean ones. Enlarging $\mathbb{K}$ and S we may assume that $\alpha_1, \dots, \alpha_r$ are S-units, $f_1, \dots, f_r, G \in \mathcal{O}_S[X]$, and $\mathfrak{R} \subseteq \mathcal{O}_S$.

Since F/G is not a linear recurrence, it follows that G does not divide all the $f_1, \dots, f_r$. Moreover, factoring out the greatest common divisor $(G, f_1, \dots, f_r)$ we can even assume that $(G, f_1, \dots, f_r) = 1$ and that G is nonconstant. In particular, by Lemma 2.6 we can enlarge S so that $(G(n), f_1(n), \dots, f_r(n)) = 1$ for all $n \in \mathbb{N}$.

Let $N_{\mathbb{K}}(\alpha)$ denote the norm of $\alpha \in \mathbb{K}$ over $\mathbb{Q}$. It is easy to prove that there exist a positive integer g and a nonconstant polynomial $\widetilde{G} \in \mathbb{Z}[X]$ such that $N_{\mathbb{K}}(G(n)) = \widetilde{G}(n)/g$ for all $n \in \mathbb{N}$. Let h be the number of irreducible factors of $\widetilde{G}$ in $\mathbb{Z}[X]$. Again by enlarging S, we may assume that g is an S-unit.

Let $\mathcal{P}$ be the set of all prime numbers p which do not make $\widetilde{G}$ vanish identically modulo p, such that $p\mathcal{O}_{\mathbb{K}}$ has no prime ideal factor π_v with $v \in S$, and such that the minimum order of the α_i/α_j $(i \neq j)$ modulo any prime ideal above p is at least $p^{1/4}$. Furthermore, let us define

$$\Omega_p := \left\{ \ell \in \{0, \dots, p-1\} : \widetilde{G}(\ell) \equiv 0 \pmod{p} \right\},$$

for any $p \in \mathcal{P}$, and $\Omega_p := \varnothing$ for any prime number $p \notin \mathcal{P}$.

Let $x \geq 3$, $y := (\log x)^{4rh}$, and $z := x^{1/(d+1)}$, where $d := [\mathbb{K} : \mathbb{Q}]$. We split $\mathcal{N}(x)$ into two subsets:

$$\mathcal{N}_1 := \{n \in \mathcal{N}(x) : (n \bmod p) \notin \Omega_p,\ \forall p \in \,]y, z]\},$$
$$\mathcal{N}_2 := \mathcal{N} \setminus \mathcal{N}_1.$$

First, we give an upper bound for $\#\mathcal{N}_1$. Hereafter, all the implied constants may depend on F and G. Clearly, $\#\Omega_p \subsetneq \{0, 1, \dots, p-1\}$ and $\#\Omega_p \leq \deg(\widetilde{G})$ for all prime number p, while from Lemma 2.1 and Lemma 2.2 it follows that

$$\sum_{p \leq x} \#\Omega_p \cdot \frac{\log p}{p} = h \log x + O(1).$$

Therefore, applying Lemma 2.4, we obtain

$$\#\mathcal{N}_1 \ll x \cdot \left(\frac{\log y}{\log x}\right)^h \ll \left(\frac{\log\log x}{\log x}\right)^h.$$

Now we give an upper bound for $\#\mathcal{N}_2$. If $n \in \mathcal{N}_2$ then there exist $p \in \mathcal{P} \cap \,]y, z]$ and $\ell \in \Omega_p$ such that $n \equiv \ell \pmod p$. In particular, p divides $N_{\mathbb{K}}(G(\ell))$ in $\mathcal{O}_S$ and, since $p\mathcal{O}_{\mathbb{K}}$ has no prime ideal factor π_v with $v \in S$, it follows that there exists some prime ideal π of $\mathcal{O}_S$ lying above p and dividing $G(\ell)$. Let $\mathbb{F}_q := \mathcal{O}_S/\pi$, so that q is a power of p. Write $n = \ell + mp$, for some integer $m \geq 0$. Since π divides $G(n)$ and $F(n)/G(n) \in \mathcal{O}_S$, we have that $F(n)$ is divisible by π too. As a consequence, we obtain that

$$\sum_{i=1}^{r} f_i(\ell)\, \alpha_i^\ell \left(\alpha_i^p\right)^m \equiv \sum_{i=1}^{r} f_i(n)\, \alpha_i^n \equiv F(n) \equiv 0 \pmod \pi. \tag{12}$$

Note that $f_1(\ell), \dots, f_r(\ell)$ cannot be all equal to zero modulo π, since π divides $G(\ell)$ and $(G(\ell), f_1(\ell), \dots, f_r(\ell)) = 1$. Note also that the minimum order N of the α_i^p/α_j^p $(i \neq j)$ modulo π is equal to the minimum order of the α_i/α_j $(i \neq j)$ modulo π, since $(p, q-1) = 1$. In particular, $N \geq p^{1/4}$, in light of the definition of $\mathcal{P}$.

Therefore, we can apply Corollary 2.1 to the congruence (12), getting that the number of possible values of m modulo $q-1$ is $O(q/p^\gamma)$, where $\gamma := 1/(4r)$. Consequently, the number of possible values of $n \leq x$ is

$$\left(\frac{x}{p(q-1)} + 1\right) \cdot O\!\left(\frac{q}{p^\gamma}\right) = O\!\left(\frac{x}{p^{1+\gamma}}\right),$$

since $p(q-1) < p^{d+1} \leq z^{d+1} \leq x$. Hence, we have

$$\#\mathcal{N}_2 \ll \sum_{p \in \mathcal{P} \cap \,]y,z]} \frac{x}{p^{1+\gamma}} \ll \int_y^{+\infty} \frac{\mathrm{d}t}{t^{1+\gamma}} \ll \frac{x}{y^\gamma} = \frac{x}{(\log x)^h}.$$

In conclusion,

$$\#\mathcal{N}(x) = \#\mathcal{N}_1 + \#\mathcal{N}_2 \ll x \cdot \left(\frac{\log\log x}{\log x}\right)^h$$

as claimed.

4. Computation of h and effectiveness of Theorem 1.5

Let us briefly explain the computation of h. First, we have an effective procedure to test if there exists a nonzero polynomial $P \in \mathbb{C}[X]$ such that the sequences $n \mapsto P(n)F(n)/G(n)$ and $n \mapsto G(n)/P(n)$ are linear recurrences, and in such a case P can be determined (see [7, p. 435, Remark 1]).

On the one hand, if P does not exist, then Theorem 1.1 implies that $\mathcal{N}$ is finite, hence h can be any positive integer. Moreover, using any effective bound for the number of zeros of a nondegenerate linear recurrence (see, e.g., [2, 16, 22]) at the end of the proof of [7, Proposition 2.1] (precisely, where it is said: "By the Skolem-Mahler-Lech Theorem again, this relation holds identically...”), it is possible to effectively bound $\#\mathcal{N}$. Therefore, if P does not exist then the implied constant in Theorem 1.5 is effectively computable.

On the other hand, if P exists, then we can write the linear recurrences $H = PF/G$ as

$$H(n) = \sum_{i=1}^{s} h_i(n)\, \beta_i^n,$$

for some $\beta_1, \dots, \beta_s \in \mathbb{C}^*$ and $h_1, \dots, h_s \in \mathbb{C}[X]$. Setting $Q := P/(P, h_1, \dots, h_s)$, we have that $\widetilde{Q}(n) = N_{\mathbb{K}}(Q(n))$ is a polynomial in $\mathbb{Q}[X]$ and h can be taken as the number of irreducible factors of $\widetilde{Q}$. Furthermore, all the implied constants of the results used in the proof of Theorem 1.5 are effectively computable, hence also when P exists the implied constant in Theorem 1.5 is effectively computable.

5. Proof of Corollary 1.1

Let us follow the instruction (and notation) for the computation of h given in §4. Clearly, $P = G$ and, consequently, $H = F$, $s = r$, $h_i = f_i$. Furthermore, we have $Q = G$, since $(G, f_1, \dots, f_r) = 1$. Finally, recalling that $G \in \mathbb{Z}[X]$, we get that $N_{\mathbb{K}}(G(n)) = G(n)^{[\mathbb{K}:\mathbb{Q}]}$ for all positive integers n, hence $\widetilde{Q}(X) = G(X)^{[\mathbb{K}:\mathbb{Q}]}$. At this point, h can be taken as the number of irreducible factors of $\widetilde{Q}$, which is also the number of irreducible factors of G (recalling that we are counting them without multiplicity). The proof is complete.

Acknowledgements. The author thanks Umberto Zannier for a fruitful conversation on Theorem 1.2, and also the anonymous referee for useful comments which improved the quality of the paper.

References

1. 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** (2012), no. 2, 271–289.
2. F. Amoroso and E. Viada, *On the zeros of linear recurrence sequences*, Acta Arith. **147** (2011), no. 4, 387–396.
3. R. André-Jeannin, *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Quart. **29** (1991), no. 4, 364–366.
4. Y. F. Bilu, *The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]*, Astérisque (2008), no. 317, Exp. No. 967, vii, 1–38, Séminaire Bourbaki. Vol. 2006/2007.
5. R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. Shparlinski, *On the statistical properties of Diffie-Hellman distributions*, Israel J. Math. **120** (2000), no. 1, 23–46.
6. P. Corvaja and U. Zannier, *Diophantine equations with power sums and universal Hilbert sets*, Indag. Math. (N.S.) **9** (1998), no. 3, 317–332.
7. P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), no. 2, 431–451.
8. 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.
9. G. H. Hardy and J. E. Littlewood, *Some problems of ‘Partitio numerorum’; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70.
10. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
11. L. Kronecker, *Über die Irreductibilität von Gleichungen*, Monatsberichte Königl. Preußisch. Akad. Wissenschaft. Berlin (1880), 155–162.
12. 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.
13. R. Rumely, *Notes on van der Poorten’s proof of the Hadamard quotient theorem. I, II*, Séminaire de Théorie des Nombres, Paris 1986–87, Progr. Math., vol. 75, Birkhäuser Boston, Boston, MA, 1988, pp. 349–382, 383–409.
14. C. Sanna, *The p-adic valuation of Lucas sequences*, Fibonacci Quart. **54** (2016), no. 2, 118–124.
15. C. Sanna, *On numbers n dividing the nth term of a Lucas sequence*, Int. J. Number Theory **13** (2017), no. 3, 725–734.
16. W. M. Schmidt, *Zeros of linear recurrence sequences*, Publ. Math. Debrecen **56** (2000), no. 3-4, 609–630.

17. J.-P. Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012.
18. 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.
19. L. Somer, *Divisibility of terms in Lucas sequences of the second kind by their subscripts*, Applications of Fibonacci numbers, Vol. 6 (Pullman, WA, 1994), Kluwer Acad. Publ., Dordrecht, 1996, pp. 473–486.
20. P. Stevenhagen and H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.
21. 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** (1988), no. 3, 97–102.
22. A. J. van der Poorten and H. P. Schlickewei, *Zeros of recurrence sequences*, Bull. Austral. Math. Soc. **44** (1991), no. 2, 215–223.

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