

Distribution of integral values for the ratio of two linear recurrences

*Original*

Distribution of integral values for the ratio of two linear recurrences / Sanna, Carlo. - In: JOURNAL OF NUMBER THEORY. - ISSN 0022-314X. - STAMPA. - 180:(2017), pp. 195-207. [10.1016/j.jnt.2017.04.015]

*Availability:*

This version is available at: 11583/2722597 since: 2020-05-03T09:53:34Z

*Publisher:*

Academic Press Incorporated

*Published*

DOI:10.1016/j.jnt.2017.04.015

*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)

# 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  $\mathfrak{A}$  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  $F(n)/G(n) \in \mathfrak{A}$ . 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

$$X^k - c_{k-1}X^{k-1} - \dots - c_1X - c_0.$$

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  $\alpha_i/\alpha_j$  ( $i \neq j$ ) 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 [6, Ch. 1–8] for the general theory of linear recurrences.

Hereafter, let  $F$  and  $G$  be linear recurrences and let  $\mathfrak{A}$  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

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

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 [6, 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, 19].

Corvaja and Zannier [5, Theorem 2] gave the following wide extension of the Hadamard-quotient Theorem (see also [4] 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 [3] 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  $\mathbb{K}$ . Corvaja and Zannier [5, Corollary 2] proved also the following theorem about the set  $\mathcal{N}$ .

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

We recall that a set of natural numbers  $\mathcal{S}$  has zero asymptotic density if  $\#\mathcal{S}(x)/x \rightarrow 0$ , as  $x \rightarrow +\infty$ , where we define  $\mathcal{S}(x) := \mathcal{S} \cap [1, x]$  for all  $x \geq 1$ .

Corvaja and Zannier also suggested [5, 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

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

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 state 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 [2] and Somer [16, 17]. Luca and Tron [11] 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  $x \rightarrow +\infty$ , 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*

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

for all  $x \geq 3$ , where  $h$  is a positive integer that can be computed in terms of  $F$  and  $G$ , while the implied constant depends on  $F$  and  $G$ .

The computation of  $h$  will be clear in the proof of Theorem 1.5. In particular, it leads immediately to the following corollary.

**Corollary 1.1.** *If  $F/G$  is not a linear recurrence,  $G \in \mathbb{Z}[X]$ , and  $\gcd(G, f_1, \dots, f_r) = 1$ , 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,  $n_1 < \dots < n_h$  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 Hardy–Littlewood  $h$ -tuple conjecture [7, 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  $x \rightarrow +\infty$ , where  $C_{\mathbf{h}} > 0$  depends on  $\mathbf{h}$ . Therefore, taking  $F(n) = (2^{n+n_1} - 2) \dots (2^{n+n_h} - 2)$  and  $G(n) = (n + n_1) \dots (n + n_h)$ , 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 [10] (see also [18, 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  $\mathbb{Z}[X]$ .

**Theorem 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  $\mathcal{G}$  be the Galois group of  $f$  over  $\mathbb{Q}$ . By a quantitative version of the Chebotarev’s density theorem [12, Ch. 2, Theorem 7.2], the number of primes  $p \leq x$  such that the irreducible factors of  $f$  modulo  $p$  have degrees  $d_1, \dots, d_s$  is

$$\frac{\pi_{\mathcal{G}}(d_1, \dots, d_s)}{\#\mathcal{G}} \cdot \text{Li}(x) + O_f\left(\frac{x}{\exp(C\sqrt{\log x})}\right),$$

for all  $x > 1$ , where  $\text{Li}(x)$  is the logarithmic integral function,  $C > 0$  is a constant depending on  $f$ , and  $\pi_{\mathcal{G}}(d_1, \dots, d_s)$  is the number of  $g \in \mathcal{G}$  that have cycle decomposition with lengths  $d_1, \dots, d_s$  when regarded as permutations of the roots of  $f$ . 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  $g$ . Hence,

$$\sum_{p \leq x} \eta_f(p) = \text{Li}(x) + O_f\left(\frac{x}{\exp(C\sqrt{\log x})}\right),$$

and the desired result follows by partial summation. □

The following lemma [5, 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  $\beta_i$  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  $\beta_1, \dots, \beta_s$ .*

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

**Lemma 2.3.** *For each prime number  $p$ , let  $\Omega_p \subsetneq \{0, 1, \dots, p-1\}$  be a set of residues modulo  $p$ , and denote by  $\Omega$  the whole family of  $\Omega_p$ 's. Suppose that there exist constants  $c, h > 0$  such that  $\#\Omega_p \leq c$  for each prime number  $p$  and*

$$(2) \quad \sum_{p \leq x} \#\Omega_p \cdot \frac{\log p}{p} = h \log x + O(1),$$

for all  $x > 1$ . Then we have

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

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  $\Omega$ ,  $\delta_1$ ,  $\delta_2$ . Clearly, we can assume  $\delta_2 \leq 1/2$ . By the large sieve inequality [8, Theorem 7.14], we have

$$(3) \quad \#\{n \leq x : (n \bmod p) \notin \Omega_p, \forall p \in ]y, z]\} \ll x \cdot \left(\sum_{m \leq w} g_y(m)\right)^{-1},$$

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 (2) that

$$-(A + h \log y) + h \log w \leq \sum_{p \leq w} g_y(p) \log p \leq B + h \log w,$$

for some constants  $A, B > 0$ . Then from [9, Theorem 0.4.1] we obtain that

$$\sum_{m \leq w} g_y(m) = \frac{\mathfrak{S}(w)}{\Gamma(h+1)} \cdot (\log w)^h \cdot \left(1 + O\left(\frac{\log y}{\log w}\right)\right),$$

where  $\Gamma$  is the Euler's Gamma function and

$$\mathfrak{S}(w) := \prod_{p \leq w} (1 + g_y(p)) \left(1 - \frac{1}{p}\right)^h.$$

In particular, since  $y \leq (\log x)^{\delta_1}$ , for sufficiently large  $x$  we get that

$$(4) \quad \sum_{m \leq w} g_y(m) \gg \mathfrak{S}(w) \cdot (\log w)^h.$$

Now from (2) it follows easily that

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

for all  $t \geq 2$ . Hence, also thanks to Mertens' third theorem [8, p. 34, Eq. 2.16], we have

$$(5) \quad \mathfrak{S}(w) = \prod_{p \leq w} \left(1 - \frac{\#\Omega_p}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^h / \prod_{p \leq y} \left(1 - \frac{\#\Omega_p}{p}\right)^{-1} \gg \frac{1}{(\log y)^h}.$$

Putting together (3), (4), and (5), and recalling that  $w = x^{\delta^2}$ , the desired result follows.  $\square$

Finally, we need a lemma about the number of zeros of a simple linear recurrence in a finite field of  $q$  elements  $\mathbb{F}_q$  (see also [6, Theorem 5.10] for a more precise result).

**Lemma 2.4.** *Let  $c_1, \dots, c_r, a_1, \dots, a_r \in \mathbb{F}_q^*$ , and let  $N$  be the minimum of the orders of the  $a_i/a_j$  ( $i \neq j$ ) in  $\mathbb{F}_q^*$ . (If  $r = 1$  then pick an arbitrary positive integer  $N$ .) Then the number of integers  $m \in [0, q-1]$  such that*

$$(6) \quad \sum_{i=1}^r c_i a_i^m = 0$$

is at most  $5(q-1)N^{-1/2^{r-2}}$ .

*Proof.* For  $r = 1$  the claim is obvious since (6) never holds, hence we may assume  $r \geq 2$ . In [5, Proposition A.1] it is stated and proved that for prime  $q$  the number of integers  $m \in [1, q-1]$  satisfying (6) is at most  $4(q-1)N^{-1/2^{r-2}}$ , and the same proof works also for not necessarily prime  $q$ . Thus the claim follows, since  $4(q-1)N^{-1/2^{r-2}} + 1 \leq 5(q-1)N^{-1/2^{r-2}}$ .  $\square$

### 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. 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  $v \notin S$ . 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,  $(G(n), f_1(n), \dots, f_r(n))$  is bounded and, enlarging  $S$ , we may assume that it is an  $S$ -unit for all  $n \in \mathbb{N}$ .

Let  $N_{\mathbb{K}}(\alpha)$  denotes 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  $\tilde{G} \in \mathbb{Z}[X]$  such that  $N_{\mathbb{K}}(G(n)) = \tilde{G}(n)/g$  for all  $n \in \mathbb{N}$ . Let  $h$  be the number of irreducible factors of  $\tilde{G}$  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  $\tilde{G}$  vanish identically modulo  $p$ , such that  $p\mathcal{O}_{\mathbb{K}}$  has no prime ideal factor  $\pi_v$  with  $v \in S$ , and such that the minimum order of the  $\alpha_i/\alpha_j$  ( $i \neq j$ ) modulo any prime ideal above  $p$  is at least  $p^{1/4}$ . Furthermore, let us define

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

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

Let  $x \geq 3$ ,  $y := (\log x)^{2^r h}$ , and  $z := x^{1/(d+1)}$ , where  $d := [\mathbb{K} : \mathbb{Q}]$ . We split  $\mathcal{N}(x)$  into two subsets:

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

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  $\#\Omega_p \leq \deg(\tilde{G})$  for all prime number  $p$ , while from Theorem 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 2.3, 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  $\pi_v$  with  $v \in S$ , it follows that there exists some prime ideal  $\pi$  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  $\pi$  divides  $G(n)$  and  $F(n)/G(n) \in \mathcal{O}_S$ , we have that  $F(n)$  is divisible by  $\pi$  too. As a consequence, we obtain that

$$(7) \quad \sum_{i=1}^r f_i(\ell) \alpha_i^\ell (\alpha_i^p)^m \equiv \sum_{i=1}^r f_i(n) \alpha_i^n \equiv F(n) \equiv 0 \pmod{\pi}.$$

Note that  $f_1(\ell), \dots, f_r(\ell)$  cannot be all equal to zero modulo  $\pi$ , since  $\pi$  divides  $G(\ell)$  and  $(G(\ell), f_1(\ell), \dots, f_r(\ell))$  is an  $S$ -unit. Note also that the minimum order of the  $\alpha_i^p/\alpha_j^p$  ( $i \neq j$ ) modulo  $\pi$  is equal to the minimum order of the  $\alpha_i/\alpha_j$  ( $i \neq j$ ) modulo  $\pi$ , since  $(p, q-1) = 1$ .

Therefore, we can apply Lemma 2.4 to the congruence (7). The positive integer  $r$  may decrease, and  $N$  can be taken  $\geq p^{1/4}$ , in light of the definition of  $\mathcal{P}$ . It follows that the number of possible values of  $m$  modulo  $q-1$  is at most  $5(q-1)p^{-1/2^r}$ . Consequently, the number of possible values of  $n \leq x$  is at most

$$5(q-1)p^{-1/2^r} \left( \frac{x}{p(q-1)} + 1 \right) \ll \frac{x}{p^{1+1/2^r}},$$

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

$$\#\mathcal{N}_2 \ll \sum_{p \in \mathcal{P} \cap ]y, z]} \frac{x}{p^{1+1/2^r}} \ll \int_y^{+\infty} \frac{dt}{t^{1+1/2^r}} \ll \frac{x}{y^{1/2^r}} = \frac{x}{(\log x)^h}.$$

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.

**Acknowledgements.** The author thanks Umberto Zannier for a fruitful conversation on Theorem 1.2.

## 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. 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.
4. P. Corvaja and U. Zannier, *Diophantine equations with power sums and universal Hilbert sets*, Indag. Math. (N.S.) **9** (1998), no. 3, 317–332.
5. P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), no. 2, 431–451.
6. 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.
7. 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.
8. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
9. D. Koukoulopoulos, *Sieve methods*, 2015, <http://www.dms.umontreal.ca/~koukoulo/>.
10. L. Kronecker, *Über die Irreduzibilität von Gleichungen*, Monatsberichte Königl. Preußisch. Akad. Wissenschaft. Berlin (1880), 155–162.

11. F. Luca and E. Tron, *The distribution of self-Fibonacci divisors*, Advances in the theory of numbers, Fields Inst. Commun., vol. 77, pp. 149–158.
12. M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*, Modern Birkhäuser Classics, Birkhäuser/Springer Basel AG, Basel, 1997.
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. 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.
17. 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.
18. P. Stevenhagen and H. W. Lenstra, Jr., *Chebotařev and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.
19. 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.

UNIVERSITÀ DEGLI STUDI DI TORINO, DEPARTMENT OF MATHEMATICS, TURIN, ITALY  
E-mail address: carlo.sanna.dev@gmail.com