Czechoslovak Mathematical Journal

Artūras Dubickas; Aivaras Novikas

Linear recurrence sequences without zeros

Czechoslovak Mathematical Journal, Vol. 64 (2014), No. 3, 857–865

Persistent URL: http://dml.cz/dmlcz/144064

Terms of use:

© Institute of Mathematics AS CR, 2014

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

Czechoslovak Mathematical Journal, 64 (139) (2014), 857–865

LINEAR RECURRENCE SEQUENCES WITHOUT ZEROS

Artūras Dubickas, Aivaras Novikas, Vilnius

(Received October 14, 2013)

Abstract. Let $a_{d-1}, \ldots, a_0 \in \mathbb{Z}$, where $d \in \mathbb{N}$ and $a_0 \neq 0$, and let $X = (x_n)_{n=1}^{\infty}$ be a sequence of integers given by the linear recurrence $x_{n+d} = a_{d-1}x_{n+d-1} + \ldots + a_0 x_n$ for $n = 1, 2, 3, \ldots$. We show that there are a prime number p and d integers $x_1, \ldots, x_d$ such that no element of the sequence $X = (x_n)_{n=1}^{\infty}$ defined by the above linear recurrence is divisible by p. Furthermore, for any nonnegative integer s there is a prime number $p \geqslant 3$ and d integers $x_1, \ldots, x_d$ such that every element of the sequence $X = (x_n)_{n=1}^{\infty}$ defined as above modulo p belongs to the set $\{s+1, s+2, \ldots, p-s-1\}$.

Keywords: linear recurrence sequence; period modulo p; polynomial splitting in $\mathbb{F}_p[z]$

MSC 2010: 11B37, 11B50, 11T06

1. Introduction

The sequence of integers $X = (x_n)_{n=1}^{\infty}$ is called a *linear recurrence sequence* of order $d \in \mathbb{N}$ if for some $a_{d-1}, \ldots, a_0 \in \mathbb{Z}$, $a_0 \neq 0$, we have

$$x_{n+d} = a_{d-1}x_{n+d-1} + \ldots + a_0 x_n \tag{1.1}$$

for $n = 1, 2, 3, \ldots$. The polynomial

$$f_X(z) := z^d - a_{d-1}z^{d-1} - \ldots - a_1 z - a_0 \in \mathbb{Z}[z] \tag{1.2}$$

is called a *characteristic polynomial* of the sequence X satisfying (1.1). Clearly, the sequence X satisfying (1.1) is ultimately periodic modulo l for every $l \in \mathbb{N}$ and, furthermore, X is purely periodic if $\gcd(a_0, l) = 1$ (see, e.g., page 45 in [6]).

There is a variety of problems related to linear recurrence sequences. They appear in number theory [6] (e.g., in Diophantine equations [14]), cryptography and finite

The research of the first named author was supported by the Research Council of Lithuania grant No. MIP-068/2013/LSS-110000-740.

fields [11], [22], etc. In particular, the papers [2], [13], [16], [18], [17] investigate which elements and how often appear in the period of the sequence X modulo l. See also [10] for a summary on the periodic structure of linear recurrent sequences over a finite field.

The motivation for this note comes from the papers [4], [3], [23] and [24]. In [4] we proved an estimate for the difference between the largest and the smallest limit points of the sequence of fractional parts $\{\xi\alpha^n\}_{n=1}^{\infty}$, where $\alpha > 1$ is a real algebraic number and $\xi \neq 0$ is a real number (see also subsequent papers [5], [8], [7]). The exceptions of the theorem proved in [4] are the pairs ξ, α, where α is a Pisot number or a Salem number and ξ lies in the field $\mathbb{Q}(\alpha)$. The case of Salem numbers α and $\xi \in \mathbb{Q}(\alpha)$ has been consider by Zaïmi in [21].

As for the distribution of the sequence $\{\xi\alpha^n\}_{n=1}^{\infty}$ and also of the sequence of distances to the nearest integer $\|\xi\alpha^n\|_{n=1}^{\infty}$ for Pisot numbers α, the important case turns out to be exactly when $\xi \in \mathbb{Q}(\alpha)$ which was not considered in [4]. For instance, for the golden section number $\alpha = (1+\sqrt{5})/2$, the maximal value of $\liminf_{n\to\infty} \|\xi\alpha^n\|$ taken over every real ξ was proved to be equal to $1/5$ when the respective ξ lies in the field $\mathbb{Q}(\alpha)$ (see [23], and also [24] for a subsequent work on this problem). This is the first example of $\alpha \notin \mathbb{N}$, where such maximal value was not just evaluated, but calculated explicitly. In [3] we gave some related results and explained why the constant $1/5$ appears for the golden section number. The reason is that the sequence given by $x_{n+2} = x_{n+1} + x_n$, $n = 1, 2, 3, \ldots$, with initial values $x_1 = 1$, $x_2 = 3$ is periodic modulo 5 and, what is the most important, the period $1, 3, 4, 2$ does not contain zeros. Similar constants ($1/5$ and $3/17$) come for Pisot numbers which are roots of $x^3 - x - 1 = 0$ and $x^4 - x^3 - 1 = 0$, by considering their respective recurrence sequences $x_{n+3} = x_{n+1} + x_n$ and $x_{n+4} = x_{n+3} + x_n$, $n = 1, 2, 3, \ldots$ (see [24]). We proved in [3] that this constant is at least $(s+1)/l$ if for some initial values $x_1, \ldots, x_d \in \mathbb{Z}$ the sequence X defined by (1.1) modulo l does not contain any of the numbers $\{0, 1, \ldots, s\} \cup \{l-s, l-s+1, \ldots, l-1\}$.

In this note we will first show that one can always avoid zeros in a period modulo p for some prime number p. This is true for any X defined by (1.1), not just for those X which define the Pisot polynomial f_X in (1.2). To state this result, we use the following notation. Given a polynomial f with integer coefficients, let $P(f)$ be the set of primes p such that $f(x) \equiv 0 \pmod{p}$ has a solution in integers x satisfying $p \nmid x$.

Theorem 1.1. *For any $a_{d-1}, \ldots, a_0 \in \mathbb{Z}$, where $d \in \mathbb{N}$ and $a_0 \neq 0$, there are a prime number p and d integers $x_1, \ldots, x_d$ such that no element of the sequence $X = (x_n)_{n=1}^{\infty}$ defined by (1.1) is divisible by p. Furthermore, we can take any prime p in the infinite set $P(f_X)$.*

The proof of Theorem 1.1 given in Section 2 is elementary. We remark that the smallest prime p for which the congruence $f(x) \equiv 0 \pmod{p}$ has a solution in positive integers x had been investigated earlier in connection with the Chebotarev density theorem. An upper bound on the smallest such p can be extracted from Lemma 3 of [1] under the generalized Riemann hypothesis and also from [20] without extra assumptions (see also [9]).

We also remark that the main part of Theorem 1.1 is nontrivial only if $S := \sum_{j=0}^{d-1} a_j$ is equal to 0 or 2. Otherwise, if $S \notin \{0, 2\}$ we can select any prime number p dividing $|S-1|$ (for example, $p = 2$ for $S = 1$) and choose the first d elements of X as follows: $x_1 = \ldots = x_d = 1$. Then by induction (1.1) implies that x_n modulo p equals $S \equiv (S - 1 + 1) \pmod{p} \equiv 1 \pmod{p}$ for each $n \in \mathbb{N}$.

In the next theorem we state a more general result asserting that by appropriate choice of $x_1, \ldots, x_d$ and p we can avoid modulo p not only 0 but also any finite subset of the set $\mathbb{N} \cup \{0\}$.

Theorem 1.2. *For any $a_{d-1}, \ldots, a_0 \in \mathbb{Z}$, where $d \in \mathbb{N}$ and $a_0 \neq 0$, and any nonnegative integer s there are a prime number $p \geqslant 3$ and d integers $x_1, \ldots, x_d$ such that every element of the sequence $X = (x_n)_{n=1}^{\infty}$ defined by* (1.1) *modulo p belongs to the set $\{s+1, s+2, \ldots, p-s-1\}$.*

We shall derive Theorem 1.2 from the following (stronger) result:

Theorem 1.3. *For any $a_{d-1}, \ldots, a_0 \in \mathbb{Z}$, where $d \in \mathbb{N}$ and $a_0 \neq 0$, and any positive integer $M \geqslant 2$ there are a prime number p satisfying $M \mid (p-1)$ and d integers $x_1, \ldots, x_d$ such that every element of the sequence $X = (x_n)_{n=1}^{\infty}$ defined by* (1.1) *modulo p is a quadratic nonresidue modulo p.*

The proof of Theorem 1.3 is more involved. More precisely, we shall prove that there are two positive integers t and c (here t is a quadratic nonresidue modulo p and c is not divisible by p) such that the elements of the sequence defined in (1.1) modulo p all belong to the set $\{t, tc^2, tc^4, \ldots, tc^{2(l-1)}\}$ modulo p, where l is the smallest positive integer satisfying $c^{2l} \equiv 1 \pmod{p}$. In the proof we will use a version of the Chebotarev density theorem (see, e.g., [19] or [12]), Hilbert's irreducibility theorem (see, e.g., [15]) and the next lemma taken from [11].

Lemma 1.4. *Let $\Phi_M(z)$ be the Mth cyclotomic polynomial and let p be a prime number which is coprime to M. If t is the minimal positive integer satisfying $p^t \equiv 1 \pmod{M}$ then $\Phi_M(z)$ in $\mathbb{F}_p[z]$ splits into $\varphi(M)/t$ distinct monic irreducible polynomials of the same degree t.*

Now, in Sections 2 and 3 we prove Theorems 1.1 and 1.3, respectively. (Even though Theorem 1.1 is a direct consequence of Theorem 1.2, we give its separate much simpler proof.) Then, in Section 4 we derive Theorem 1.2 from Theorem 1.3.

2. Proof of Theorem 1.1

Assume that there are only finitely many primes $p_1, p_2, \dots, p_s$ that divide the values of $f_X(j)$, where j runs through $\mathbb{Z}$. Since $f_X(0) = -a_0$, the prime divisors of $a_0 \neq 0$ are all in the set $\{p_1, p_2, \dots, p_s\}$. Take any $y \in \mathbb{Z}$ for which $|f_X(a_0 p_1 \dots p_s y)| \geqslant 2|a_0|$. Since the integer $f_X(a_0 p_1 \dots p_s y)/a_0$ is coprime to the product $p_1 p_2 \dots p_s$ and is greater than or equal to 2 in absolute value, it must have a prime divisor that is not in the set $\{p_1, p_2, \dots, p_s\}$. Thus, $f_X(a_0 p_1 \dots p_s y)$ must have such a prime divisor too, a contradiction. This proves that there are infinitely many primes p that divide $f_X(x)$ for some $x \in \mathbb{Z}$. Consider any such prime p satisfying $p \nmid a_0$. Let x be an integer for which $p \mid f_X(x)$. Clearly, if $p \mid x$, then $p \mid a_0$, which is not the case. Thus, $p \nmid x$, and, consequently, the set $P(f_X)$ of primes p such that $f_X(x) \equiv 0 \pmod{p}$ has a solution in integers x satisfying $p \nmid x$ is infinite.

Take any $p \in P(f_X)$ and $m \in \mathbb{Z}$ for which $p \mid f_X(m)$ and $p \nmid m$. Put $x_j := m^{j-1}$ for each $j = 1, \dots, d$. Now, we will show (by induction) that

$$x_j \equiv m^{j-1} \pmod{p} \tag{2.1}$$

for each $j \in \mathbb{N}$. Clearly, then $p \nmid x_j$ for every $j \in \mathbb{N}$, since $p \nmid m$. This will complete the proof of the theorem.

Evidently, (2.1) holds for $j = 1, \dots, d$, by the definition of the first d terms of the sequence $X = (x_j)_{j=1}^{\infty}$. Assume that (2.1) holds for $j = 1, \dots, k$, where $k \geqslant d$. We must show that then (2.1) holds for $j = k+1$. Indeed, first, using (1.1), second, applying (2.1) to $j = k, k-1, \dots, k-d+1$, and, finally, using the equality $a_{d-1} m^{d-1} + \dots + a_1 m + a_0 = m^d - f_X(m)$ and the fact that $p \mid f_X(m)$, we obtain

$$\begin{aligned} x_{k+1} &\equiv a_{d-1} x_k + \dots + a_0 x_{k-d+1} \pmod{p} \\ &\equiv a_{d-1} m^{k-1} + \dots + a_0 m^{k-d} \pmod{p} \\ &\equiv m^{k-d}(m^d - f_X(m)) \pmod{p} \equiv m^k \pmod{p}. \end{aligned}$$

This completes the proof of (2.1). □

3. Proof of Theorem 1.3

Let $g(z) := z^D + \sum_{j=0}^{D-1} b_j z^j$ be a monic irreducible divisor of the polynomial $f_X(z^2)$ of degree D, where $1 \leqslant D \leqslant 2d = \deg f_X(z^2)$. (If $f_X(z^2)$ is irreducible then $g(z) = f_X(z^2)$.)

We claim that for some $m \in \mathbb{Z}$ the polynomial $g(z^M - m)$ is irreducible in $\mathbb{Z}[z]$. Indeed, otherwise (if there is no such m), by Hilbert's irreducibility theorem (see page 298 in [15]), the polynomial $g(z^M - y)$ is reducible in $\mathbb{Z}[z, y]$, namely,

$$g(z^M - y) = (z^M - y)^D + \ldots + b_1(z^M - y) + b_0 = g_1(z, y)g_2(z, y) \tag{3.1}$$

for some nonconstant polynomials g_1 and g_2 in $\mathbb{Z}[z, y]$. Assume that the degree of $g_1(z, y)$ in the variable y is d_1 and the degree of $g_2(z, y)$ in the variable y is d_2. Then $d_1 + d_2 = D$ and the coefficients for y^{d_1} in $g_1(z, y)$ and y^{d_2} in $g_2(z, y)$ are ± 1. Also, without restriction of generality we may assume that $d_1, d_2 \geqslant 1$, since $g(z^M - y)$ is not divisible by a nonconstant polynomial in the variable z only (the leading coefficient of the polynomial $g(z^M - y)$ in the variable y over the ring $\mathbb{Z}[z]$ is ± 1). Now, inserting $z = 0$ into (3.1) we obtain $g(-y) = g_1(0, y)g_2(0, y)$, where $\deg g_1(0, y) = d_1 \geqslant 1$ and $\deg g_2(0, y) = d_2 \geqslant 1$, which is impossible, because $g(-y)$ is irreducible in $\mathbb{Z}[y]$. This proves the claim.

Fix $m \in \mathbb{Z}$ for which the polynomial $g(z^M - m)$ is irreducible in $\mathbb{Z}[z]$. By the theorem of Frobenius (a weaker version of the Chebotarev theorem), the polynomial $g(z^M - m)$ modulo p splits into linear factors for infinitely many primes p (see, e.g., [19]; in fact, the density of such primes p is equal to $1/|G|$, where G is the Galois group of the polynomial $g(z^M - m)$). Let $p \geqslant 3$ be one of those primes which is coprime to $Mg(-m)g(0)$. Here, $g(-m) \neq 0$, since $g(z^M - m)$ is irreducible in $\mathbb{Z}[z]$, and $g(0) \neq 0$, since $g(0)$ divides $f_X(0) = -a_0 \neq 0$. Note that, as $g(z^M - m)$ splits into linear factors in $\mathbb{F}_p[z]$, so does $g(z)$. Indeed, factorize $g(z) = \prod_{j=1}^{D} (z - \alpha_j)$ in $L[z]$, where L is some finite extention of $\mathbb{F}_p$. The polynomial $g(z^M - m) = \prod_{j=1}^{D} (z^M - m - \alpha_j)$ in $L[z]$ is equal to $\prod_{i=1}^{MD} (z - r_i)$ with $r_i \in \mathbb{F}_p$. Hence, each factor $z^M - m - \alpha_j$ is the product of some M linear factors $z - r_i$ with $r_i \in \mathbb{F}_p$. It follows that $\alpha_j \in \mathbb{F}_p$, and so we can take $L = \mathbb{F}_p$.

Fix $j \in \{1, \ldots, D\}$ and write the element $m + \alpha_j$ of $\mathbb{F}_p$ as b^M with some $b \in \mathbb{F}_p$. This is possible, since the polynomial $z^M - m - \alpha_j$ has a root $b = r_i \in \mathbb{F}_p$ for some $i \in \{1, \ldots, MD\}$. Note that $b \neq 0$, since otherwise one of the factors of $g(z^M - m)$

modulo p wold be z^M, which is not the case in view of $\gcd(p, g(-m)) = 1$. Then, as

$$z^M - m - \alpha_j = z^M - b^M = b^M((zb^{-1})^M - 1) \in \mathbb{F}_p[z]$$

splits into linear factors in $\mathbb{F}_p[z]$, so does the polynomial $z^M - 1$. It follows that its divisor $\Phi_M(z)$ also splits into linear factors in $\mathbb{F}_p[z]$. Since p and M are coprime, by Lemma 1.4 we must have $t = 1$ and $M \mid (p-1)$. Fix any $c \in \mathbb{N}$ coprime to p for which $p \mid g(c)$. Such c exists, since $g(z)$ has a root α_1 in $\mathbb{F}_p$ and $\alpha_1 \neq 0$. The last inequality follows from $g(0) \not\equiv 0 \pmod{p}$. As $g(z)$ divides $f_X(z^2)$ in $\mathbb{Z}[z]$, the prime p divides $f_X(c^2)$. Let $t \in \{1, \dots, p-1\}$ be any quadratic nonresidue modulo p. (Note that $p \geqslant 3$, so such t exists.) This time, we select $x_j := tc^{2(j-1)}$ for $j = 1, \dots, d$.

In order to complete the proof of the theorem, it remains to show that

$$x_j \equiv tc^{2(j-1)} \pmod{p} \tag{3.2}$$

for each $j \in \mathbb{N}$. Indeed, as the Legendre symbol $\left(\frac{t}{p}\right)$ is equal to -1, we find that

$$\left(\frac{tc^{2(j-1)}}{p}\right) = \left(\frac{t}{p}\right)\left(\frac{c^{2(j-1)}}{p}\right) = (-1) \cdot 1 = -1$$

for each $j \in \mathbb{N}$, so $t, tc^2, tc^4, tc^6, \dots$ all are nonresidues modulo p.

Evidently, (3.2) holds for $j = 1, \dots, d$, by the definition of the first d terms of the sequence $X = (x_j)_{j=1}^{\infty}$. Assume that (3.2) holds for $j = 1, \dots, k$, where $k \geqslant d$. Now, in the same fashion as in Theorem 1.1 it follows that (3.2) holds for $j = k+1$. Indeed, first, using (1.1), second, applying (3.2) to $j = k, k-1, \dots, k-d+1$ and, finally, using the equality $a_{d-1}c^{2(d-1)} + \dots + a_1c^2 + a_0 = c^{2d} - f_X(c^2)$ (see (1.2)) combined with the fact that $p \mid f_X(c^2)$, we deduce that

$$\begin{aligned} x_{k+1} &\equiv a_{d-1}x_k + \dots + a_0x_{k-d+1} \pmod{p} \\ &\equiv t(a_{d-1}c^{2(k-1)} + \dots + a_0c^{2(k-d)}) \pmod{p} \\ &\equiv tc^{2(k-d)}(c^{2d} - f_X(c^2)) \pmod{p} \equiv tc^{2k} \pmod{p}. \end{aligned}$$

This completes the proof of (3.2). □

4. Proof of Theorem 1.2

Observe that without restriction of generality we may assume that $s \geqslant 2$. Fix an integer $s \geqslant 2$ and put

$$M := 4 \prod_{q \leqslant s} q, \tag{4.1}$$

where the product is taken over the prime numbers q. By Theorem 1.3 applied to the integer M, there is a prime number $p = Mk + 1$, where $k \in \mathbb{N}$, and d integers $x_1, \dots, x_d$ such that every element of the sequence $X = (x_n)_{n=1}^{\infty}$ defined by (1.1) modulo p is a quadratic nonresidue modulo p. We claim that for such p and M, as defined in (4.1), $0, 1, \dots, s$ and $p-1, \dots, p-s$ are quadratic residues modulo p.

Indeed, $0, 1$ and -1 are quadratic residues modulo p, since $4 \mid (p-1)$. In order to prove that all elements of the set

$$R := \{0, 1, \dots, s\} \cup \{p-s, \dots, p-1\}$$

are quadratic residues, it suffices to show that every prime number q lying in the set $\{2, 3, \dots, s\}$ is a quadratic residue modulo p. To prove this, let us calculate the Legendre symbol for $q = 2$ and for every prime number q in the range $2 < q \leqslant s$. Since $8 \mid M$ and $p = Mk + 1$, we have $p \equiv 1 \pmod 8$. Hence,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = 1.$$

Similarly, using the fact that $q \mid (p-1)$ for each prime q in the range $2 < q \leqslant s$ we find that

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1,$$

since $(p-1)(q-1)/4$ is even. Thus, every prime number q in the range $2 \leqslant q \leqslant s$ is a quadratic residue modulo p. Therefore, each x_j modulo p belongs to the set

$$\{s+1, s+2, \dots, p-s-1\} = \{0, 1, \dots, p-1\} \setminus R$$

containing all nonresidues modulo p. This completes the proof of Theorem 1.2. $\square$

Note that in a similar fashion one can eliminate not only the set of residues close to 0 and p, but also a set of any fixed size composed of residues modulo p close to, say, $(p-1)/2$, where p is a large enough prime number.

Acknowledgement. We thank the referee for careful reading and some useful remarks.

References

[1] *L. M. Adleman, A. M. Odlyzko*: Irreducibility testing and factorization of polynomials. Math. Comput. *41* (1983), 699–709.

[2] *D. Carroll, E. Jacobson, L. Somer*: Distribution of two-term recurrence sequences mod p^e. Fibonacci Q. *32* (1994), 260–265.

[3] *A. Dubickas*: Distribution of some quadratic linear recurrence sequences modulo 1. Carpathian J. Math. *30* (2014), 79–86.

[4] *A. Dubickas*: Arithmetical properties of powers of algebraic numbers. Bull. Lond. Math. Soc. *38* (2006), 70–80.

[5] *A. Dubickas*: On the distance from a rational power to the nearest integer. J. Number Theory *117* (2006), 222–239.

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

[7] *H. Kaneko*: Limit points of fractional parts of geometric sequences. Unif. Distrib. Theory *4* (2009), 1–37.

[8] *H. Kaneko*: Distribution of geometric sequences modulo 1. Result. Math. *52* (2008), 91–109.

[9] *J. C. Lagarias, A. M. Odlyzko*: Effective versions of the Chebotarev density theorem. Algebraic Number Fields: L-Functions and Galois Properties (A. Fröhlich, ed.). Proc. Symp., Durham, 1975, Academic Press, London, 1977, pp. 409–464.

[10] *D. Laksov*: Linear recurring sequences over finite fields. Math. Scand. *16* (1965), 181–196.

[11] *R. Lidl, H. Niederreiter*: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge, 1994.

[12] *J. Neukirch*: Algebraic Number Theory. Grundlehren der Mathematischen Wissenschaften 322, Springer, Berlin, 1999.

[13] *H. Niederreiter, A. Schinzel, L. Somer*: Maximal frequencies of elements in second-order linear recurring sequences over a finite field. Elem. Math. *46* (1991), 139–143.

[14] *P. Ribenboim, G. Walsh*: The ABC conjecture and the powerful part of terms in binary recurring sequences. J. Number Theory *74* (1999), 134–147.

[15] *A. Schinzel*: Polynomials with special regard to reducibility. Encyclopedia of Mathematics and Its Applications 77, Cambridge University Press, Cambridge, 2000.

[16] *A. Schinzel*: Special Lucas sequences, including the Fibonacci sequence, modulo a prime. A Tribute to Paul Erdős (A. Baker, et al., eds.). Cambridge University Press, Cambridge, 1990, pp. 349–357.

[17] *L. Somer*: Distribution of residues of certain second-order linear recurrences modulo p. Applications of Fibonacci Numbers, Vol. 3 (G. E. Bergum, et al., eds.). Proc. 3rd Int. Conf., Pisa, 1988, Kluwer Academic Publishers Group, Dordrecht, 1990, pp. 311–324.

[18] *L. Somer*: Primes having an incomplete system of residues for a class of second-order recurrences. Applications of Fibonacci Numbers, Proc. 2nd Int. Conf. (A. N. Philippou, et al., eds.). Dordrecht, 1988, pp. 113–141.

[19] *P. Stevenhagen, H. W. Lenstra,* Jr.: Chebotarëv and his density theorem. Math. Intell. *18* (1996), 26–37.

[20] *J. F. Voloch*: Chebyshev's method for number fields. J. Théor. Nombres Bordx. *12* (2000), 81–85.

[21] *T. Zaïmi*: An arithmetical property of powers of Salem numbers. J. Number Theory *120* (2006), 179–191.

[22] *Q.-X. Zheng, W.-F. Qi, T. Tian*: On the distinctness of modular reductions of primitive sequences over $\mathbb{Z}/(2^{32}-1)$. Des. Codes Cryptography *70* (2014), 359–368.

[23] *V. Zhuravleva*: Diophantine approximations with Fibonacci numbers. J. Théor. Nombres Bordx. *25* (2013), 499–520.
[24] *V. Zhuravleva*: On the two smallest Pisot numbers. Math. Notes *94* (2013), 820–823; translation from Mat. Zametki *94* (2013), 784–787.

Authors' address: Artūras Dubickas, Aivaras Novikas, Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania, e-mail: arturas.dubickas@mif.vu.lt, aivaras.novikas@mif.vu.lt.