ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus
Mathématique

Federico Accossato and Carlo Sanna

On the number of residues of certain second-order linear recurrences

Volume 362 (2024), p. 1365-1377

Online since: 14 November 2024

https://doi.org/10.5802/crmath.647

CENTRE
MERSENNE

The Comptes Rendus. Mathématique *are a member of the*
Mersenne Center for open scientific publishing
www.centre-mersenne.org — e-ISSN : 1778-3569

ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus. Mathématique
2024, Vol. 362, p. 1365-1377
https://doi.org/10.5802/crmath.647

Research article / *Article de recherche*
Number theory / *Théorie des nombres*

On the number of residues of certain second-order linear recurrences

Sur le nombre de résidus de certaines récurrences linéaires du second ordre

Federico Accossato[a] **and Carlo Sanna**[*, a]

E-mails: federico.accossato@polito.it, carlo.sanna@polito.it

Abstract. For every monic polynomial $f \in \mathbb{Z}[X]$ with $\deg(f) \geq 1$, let $\mathscr{L}(f)$ be the set of all linear recurrences with values in $\mathbb{Z}$ and characteristic polynomial f, and let

$$\mathscr{R}(f) := \{\rho(\boldsymbol{x}; m) : \boldsymbol{x} \in \mathscr{L}(f),\, m \in \mathbb{Z}^+\},$$

where $\rho(\boldsymbol{x}; m)$ is the number of distinct residues of $\boldsymbol{x}$ modulo m.

Dubickas and Novikas proved that $\mathscr{R}(X^2 - X - 1) = \mathbb{Z}^+$. We generalize this result by showing that $\mathscr{R}(X^2 - a_1 X - 1) = \mathbb{Z}^+$ for every nonzero integer a_1. As a corollary, we deduce that for all integers $a_1 \geq 1$ and $k \geq 2$ there exists $\xi \in \mathbb{R}$ such that the sequence of fractional parts $(\mathrm{frac}(\xi\alpha^n))_{n \geq 0}$, where $\alpha := \big(a_1 + \sqrt{a_1^2 + 4}\big)/2$, has exactly k limit points. Our proofs are constructive and employ some results on the existence of special primitive divisors of certain Lehmer sequences.

Résumé. Pour chaque polynôme monique $f \in \mathbb{Z}[X]$ avec $\deg(f) \geq 1$, soit $\mathscr{L}(f)$ l'ensemble de toutes les récurrences linéaires avec des valeurs dans $\mathbb{Z}$ et un polynôme caractéristique f, et soit

$$\mathscr{R}(f) := \{\rho(\boldsymbol{x}; m) : \boldsymbol{x} \in \mathscr{L}(f),\, m \in \mathbb{Z}^+\},$$

où $\rho(\boldsymbol{x}; m)$ est le nombre de résidus distincts de $\boldsymbol{x}$ modulo m.

Dubickas et Novikas ont prouvé que $\mathscr{R}(X^2 - X - 1) = \mathbb{Z}^+$. Nous généralisons ce résultat en montrant que $\mathscr{R}(X^2 - a_1 X - 1) = \mathbb{Z}^+$ pour tout entier non nul a_1. Comme corollaire, nous déduisons que pour tous les entiers $a_1 \geq 1$ et $k \geq 2$, il existe $\xi \in \mathbb{R}$ tel que la séquence des parties fractionnaires $(\mathrm{frac}(\xi\alpha^n))_{n \geq 0}$, où $\alpha := \big(a_1 + \sqrt{a_1^2 + 4},\big)/2$, a exactement k points de limite. Nos preuves sont constructives et utilisent certains résultats sur l'existence de diviseurs primitifs spéciaux de certaines séquences de Lehmer.

Keywords. Fractional parts of powers, Lehmer sequences, linear recurrences, Pisot numbers, primitive divisors, residues.

Mots-clés. Parties fractionnaires des puissances, suites de Lehmer, récurrences linéaires, nombres de Pisot, diviseurs primitifs, résidus.

2020 Mathematics Subject Classification. 11B37, 11B39, 11B50, 11K16.

Funding. The authors are members of GNSAGA of INdAM, and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.

Manuscript received 23 February 2024, revised 23 April 2024, accepted 3 May 2024.

[*] Corresponding author

1. Introduction

Let $a_1, \dots, a_k$ be integers. An integer sequence $\boldsymbol{x} = (x_n)_{n \geq 0}$ is a *linear recurrence* with *characteristic polynomial*

$$f = X^k - a_1 X^{k-1} - a_2 X^{k-2} - \cdots - a_k$$

if for all integers $n \geq k$ we have that

$$x_n = a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_k x_{n-k}. \tag{1}$$

The terms $x_0, \dots, x_{k-1}$, which together with f completely determine $\boldsymbol{x}$ via (1), are the *initial values* of $\boldsymbol{x}$. We let $\mathscr{L}(f)$ denote the set of all (integral) linear recurrences with characteristic polynomial f. It is easily seen that each $\boldsymbol{x} \in \mathscr{L}(f)$ is ultimately periodic modulo m, for every integer $m \geq 1$, and in fact (purely) periodic if $\gcd(m, a_k) = 1$. Indeed, properties of linear recurrences modulo m have been studied extensively, including: which residues modulo m appear in $\boldsymbol{x}$ and how frequently [3, 8, 11, 13, 16, 18], and for which values of m the linear recurrence $\boldsymbol{x}$ contains a complete system of residues modulo m [1, 4, 12, 17, 19].

We let $\tau(\boldsymbol{x}; m)$ denote the (minimal) period of $\boldsymbol{x}$ modulo m, that is, the minimal integer $t \geq 1$ such that $x_{n+t} \equiv x_n \pmod{m}$ for all sufficiently large integers $n \geq 0$. Moreover, we let $\rho(\boldsymbol{x}; m) := \#\{x_n \bmod m : n \geq 0\}$ be the number of distinct residues of $\boldsymbol{x}$ modulo m, and we put

$$\mathscr{R}(f) := \{\rho(\boldsymbol{x}; m) : \boldsymbol{x} \in \mathscr{L}(f),\, m \in \mathbb{Z}^+\}.$$

Dubickas and Novikas [9], motivated by some problems on fractional parts of powers of Pisot numbers [24], proved that $\mathscr{R}(X^2 - X - 1) = \mathbb{Z}^+$ and stated that it "may be very difficult in general" to determine $\mathscr{R}(f)$. Sanna [15] considered the special case in which f is a quadratic polynomial with roots α, β such that $\alpha\beta = \pm 1$ and α/β is not a root of unity, and proved two results. First, that $\mathscr{R}(f)$ contains all integers $n \geq 7$ with $n \neq 10$ and $4 \nmid n$. Second, that $4D_0\mathbb{Z}^+ \subseteq \mathscr{R}(f)$ if $\alpha\beta = 1$, and $8D_0\mathbb{Z}^+ \subseteq \mathscr{R}(f)$ if $\alpha\beta = -1$; where D_0 is the squarefree part of the discriminant of f, and it is assumed that $D_0 \equiv 1 \pmod{4}$ and $D_0 \geq 5$.

Our result is the following.

Theorem 1. *Let a_1 be a nonzero integer. Then $\mathscr{R}(X^2 - a_1 X - 1) = \mathbb{Z}^+$. In other words, for every $n \in \mathbb{Z}^+$ there exist $\boldsymbol{x} \in \mathscr{L}(f)$ and $m \in \mathbb{Z}^+$ such that $\rho(\boldsymbol{x}; m) = n$. Moreover, one can choose $\boldsymbol{x}$ and m so that all the residues of $\boldsymbol{x}$ modulo m are nonzero if and only if $|a_1| = 1$ and $n \geq 4$, or $|a_1| \geq 2$.*

The assumption that a_1 is nonzero is not a restriction, since it is easy to prove that $\mathscr{R}(X^2 - 1) = \{1, 2\}$. We remark that the proof of Theorem 1 is constructive. It provides an algorithm that, given as input a nonzero integer a_1 and an integer $n \geq 1$, returns as output a modulo m and the initial values x_0, x_1 of a linear recurrence $\boldsymbol{x} \in \mathscr{L}(X^2 - a_1 X - 1)$ such that $\rho(\boldsymbol{x}; m) = n$ and, if $|a_1| \geq 2$ or $n \geq 4$, all the residues of $\boldsymbol{x}$ modulo m are nonzero.

For every $t \in \mathbb{R}$, let $\operatorname{floor}(t)$ be the *floor function* of t, that is, the greatest integer not exceeding t, and let $\operatorname{frac}(t) := t - \operatorname{floor}(t)$ be the *fractional part* of t. As a corollary of their aforementioned result, Dubickas and Novikas [9] proved that for every integer $k \geq 2$ there exists $\xi \in \mathbb{R}$ such that the sequence $\big(\operatorname{frac}\big(\xi((1+\sqrt{5})/2)^n\big)\big)_{n \geq 0}$ has exactly k limit points.

From Theorem 1, we deduce the following corollary.

Corollary 2. *Let $a_1 \geq 1$ be an integer, and let $\alpha := \big(a_1 + \sqrt{a_1^2 + 4}\big)/2$. Then, for every integer $k \geq 2$, and for every integer $k \geq 1$ if $a_2 \geq 2$, there exists $\xi \in \mathbb{Q}(\alpha)$ such that the sequence $\big(\operatorname{frac}(\xi\alpha^n)\big)_{n \geq 0}$ has exactly k limit points.*

We remark that sequence of fractional parts $\big(\operatorname{frac}(\xi\alpha^n)\big)_{n \geq 0}$, where $\alpha > 1$ is a real algebraic number and $\xi \in \mathbb{R}$, has been studied by several authors [5–7, 14, 21, 23, 24].

The paper is structured as follows. Section 2 contains several preliminary lemmas. More precisely, Section 2.1 is devoted to prove the existence of some special primitive divisors of specific Lehmer sequences, Section 2.2 contains some elementary but useful results on certain multiplicative orders, and Section 2.3 provides the main lemmas for the construction of the desired sequences in $\mathscr{L}(f)$. Then, Sections 3 and 4 are devoted to the proofs of Theorem 1 and Corollary 2, respectively.

2. Preliminaries

Hereafter, let a_1 be a nonzero integer, let $f := X^2 - a_1 X - 1$, let $D := a_1^2 + 4$ be the discriminant of f, let $K := \mathbb{Q}(\sqrt{D})$ be the splitting field of f, and let $\alpha, \beta \in K$ be the roots of f. Note that D is not a square in $\mathbb{Q}$, so that K is a quadratic number field. Moreover, note that α and β are distinct real numbers, $\alpha\beta = -1$, $\alpha + \beta = a_1$, $(\alpha - \beta)^2 = D$, and α/β is not a root of unity.

We begin with the following lemma.

Lemma 3. *Let $\boldsymbol{x} \in \mathscr{L}(f)$, let $m \geq 1$ be an integer, and let $t := \tau(\boldsymbol{x}; m)$. Then there exists $\boldsymbol{y} \in \mathscr{L}(X^2 + a_1 X - 1)$ such that $y_n \equiv x_{(-(n+1) \bmod t)} \pmod m$ for every integer $n \geq 0$, where $(-(n+1) \bmod t)$ is the unique integer $r \in [0, t)$ such that $r \equiv -(n+1) \pmod t$. In particular, we have that $\tau(\boldsymbol{x}; m) = \tau(\boldsymbol{y}; m)$, $\rho(\boldsymbol{x}; m) = \rho(\boldsymbol{y}; m)$, and that all residues of $\boldsymbol{x}$ modulo m are nonzero if and only if all residues of $\boldsymbol{y}$ modulo m are nonzero.*

Proof. Let us extend $\boldsymbol{x}$ to negative indices by defining $x_n := -a_1 x_{n+1} + x_{n+2}$ for every integer $n \leq -1$. Then, we have that $x_n = -a_1 x_{n+1} + x_{n+2}$ and $x_{n+t} \equiv x_n \pmod m$ for every integer n. Let $\boldsymbol{y} \in \mathscr{L}(X^2 + a_1 X - 1)$ with $y_0 = x_{t-1}$ and $y_1 = x_{t-2}$. Since $y_{n+2} = -a_1 y_{n+1} + y_n$ for every integer $n \geq 0$, it follows easily by induction that $y_n = x_{t-(n+1)}$ for every integer $n \geq 0$. Hence, by the periodicity of $\boldsymbol{x}$, we get that $y_n \equiv x_{(-(n+1) \bmod t)} \pmod m$ for every integer $n \geq 0$, as desired. □

In light of Lemma 3, hereafter we assume that $a_1 \geq 1$.

Remark 4. Since Dubickas and Novikas already proved the case $a_1 = 1$ of Theorem 1 and Corollary 2, we could assume that $a_1 \geq 2$. However, we choose to include the case $a_1 = 1$ in our proofs in order to state some of the intermediary results with greater generality.

2.1. *Lehmer sequences*

Let γ, δ be complex numbers such that $\gamma\delta$ and $(\gamma + \delta)^2$ are nonzero coprime integers and γ/δ is not a root of unity. The *Lehmer sequence* (ℓ_n) associated to γ, δ is defined by

$$\ell_n := \begin{cases} (\gamma^n - \delta^n)/(\gamma - \delta) & \text{if } n \text{ is odd;} \\ (\gamma^n - \delta^n)/(\gamma^2 - \delta^2) & \text{if } n \text{ is even;} \end{cases} \tag{2}$$

for all integers $n \geq 0$. The conditions on γ, δ ensure that each ℓ_n is an integer. A prime number p is a *primitive divisor* of ℓ_n if $p \mid \ell_n$ but $p \nmid (\gamma^2 - \delta^2)^2 \ell_1 \cdots \ell_{n-1}$ (cf. [2]). Note that $\ell_1 = \ell_2 = 1$, so that ℓ_n can have primitive divisors only if $n \geq 3$.

The sequence of *cyclotomic numbers* (ϕ_n) associated to γ, δ is defined by

$$\phi_n := \prod_{\substack{1 \leq k \leq n \\ \gcd(n,k)=1}} \left(\gamma - \mathrm{e}^{\frac{2\pi \mathrm{i} k}{n}} \delta\right), \tag{3}$$

for all integers $n \geq 1$. It can be proved that $\phi_n \in \mathbb{Z}$ for every integer $n \geq 3$ [2, p. 84].

The next lemma relates the cyclotomic numbers with the primitive divisors of the Lehmer sequence. For every prime number p, let ν_p denote the p-adic valuation. For every integer $n \geq 4$, let $P_3(n)$ denote the greatest prime factor of $n/\gcd(n, 3)$.

Lemma 5. *Let $n \geq 5$ be an integer with $n \neq 6$. Then*

$$|\phi_n| \Big/ \prod_{p \text{ prim. div. } \ell_n} p^{\nu_p(\ell_n)} \in \begin{cases} \{1, P_3(n)\} & \text{if } n \neq 12; \\ \{1,2,3,6\} & \text{if } n = 12; \end{cases}$$

where the product runs over all the primitive divisors p of ℓ_n.

Proof. From (3) it follows easily that

$$\gamma^m - \delta^m = \prod_{d \mid m} \phi_d, \tag{4}$$

for all integers $m \geq 1$. In turn, applying to (4) the Möbius inversion formula and taking into account (2), we get that

$$\phi_m = \prod_{d \mid m} \left(\gamma^d - \delta^d\right)^{\mu(m/d)} = \prod_{d \mid m} \ell_d^{\mu(m/d)}, \tag{5}$$

for all integers $m \geq 3$, where μ is the Möbius function and where we also employed the well-known fact that $\sum_{d \mid m} \mu(d) = 0$ for every integer $m \geq 2$.

Let p be a prime number. If p is a primitive divisor of ℓ_n, then p does not divide ℓ_k for every positive integer $k < n$. Hence, from (5) we have that $\nu_p(\phi_n) = \nu_p(\ell_n)$.

If p is not a primitive divisor of ℓ_n and $p \mid \phi_n$, then it is known that $\nu_p(\phi_n) = 1$ and that either $p = P_3(n)$, if $n \neq 12$, or $p \in \{2,3\}$, if $n = 12$; see the "only if" part of the proof of [2, Theorem 2.4], or see the paragraphs before, and the comment after, [20, Lemma 6]. □

We need a lower bound for the absolute values of cyclotomic numbers.

Lemma 6. *Suppose that γ, δ are real numbers with $\gamma\delta > 0$. Then*

$$|\phi_n| > |4(\gamma - \delta)^2 \gamma\delta|^{\varphi(n)/4}$$

for every integer $n \geq 3$, where φ is the Euler function.

Proof. This result is due to Ward [22, p. 233]. □

Hereafter, we put $\gamma := \alpha$ and $\delta := -\beta$. Note that this choice does indeed satisfy the conditions of Lehmer sequence. Moreover, we have that $\gamma\delta = 1$, $\gamma - \delta = a_1$, $(\gamma + \delta)^2 = D$, and $(\gamma^2 - \delta^2)^2 = a_1^2 D$. Furthermore, the first values of (ℓ_n) are

$$\ell_1 = 1, \quad \ell_2 = 1, \quad \ell_3 = a_1^2 + 3, \quad \ell_4 = a_1^2 + 2, \quad \ell_5 = (a_1^2 + 1)(a_1^2 + 4) + 1, \quad \ell_6 = (a_1^2 + 1)\ell_3. \tag{6}$$

In particular, note that, since ℓ_3 or ℓ_4 is even, if $n \geq 5$ then every primitive divisor of ℓ_n (if it exists) is odd.

The problem of determining which terms of a Lehmer sequence have a primitive divisor has a very long history. The first complete classification was given by Bilu, Hanrot, and Voutier [2] (see also [15, Remark 3.1] for some missing values in [2, Table 4]). We make use of the following two results.

Lemma 7. *Let $n \geq 3$ be an integer. If $a_1 = 1$ and $n \notin \{3,6,10,12\}$, or $a_1 = 3$ and $n \neq 3$, or $a_1 \notin \{1,3\}$, then ℓ_n has at least one odd primitive divisor p.*

Proof. If $n \geq 13$ then it is known that ℓ_n has at least one odd primitive divisor [20, Lemma 8]. (In fact, this is true for all Lehmer sequences with real γ, δ.) Hereafter, assume that $n \leq 12$.

If $a_1 = 1$ and $n \notin \{3,6,10,12\}$, then one can check that ℓ_n has an odd primitive divisor. If $a_1 = 3$ and $n \neq 3$, then one can check that ℓ_n has an odd primitive divisor.

Hereafter, assume that $a_1 \notin \{1,3\}$. If $n \geq 5$ and $n \neq 6$, then by Lemma 6, recalling that $\gamma - \delta = a_1$, $\gamma\delta = 1$, we get that $|\phi_n| > 2^{\varphi(n)} > n$. In turn, by Lemma 5, this implies that ℓ_n has an odd primitive divisor.

It remains to prove that if $n \in \{3,4,6\}$ then ℓ_n has an odd primitive divisor. Since $a_1 \notin \{1,3\}$, by reasoning modulo 8 and modulo 9, it follows easily that a_1^2+2 is not a power of 2, and that neither a_1^2+1 nor a_1^2+3 is equal to $2^s 3^t$ for some integers $s,t \geq 0$. Hence, there exists a prime number $p \geq 5$ dividing a_1^2+1. We claim that p is an odd primitive divisor of ℓ_6. In fact, since $p \geq 5$, by (6) and recalling that $D = a_1^2+4$, we get that $p \mid \ell_6$ and $p \nmid a_1 D \ell_1 \cdots \ell_5$. The proof that ℓ_3 and ℓ_4 have an odd primitive divisor proceeds similarly. □

Remark 8. Lemma 7 is optimal, that is, one can verify that if $a_1 = 1$ and $n \in \{3,6,10,12\}$, or if $a_1 = 3$ and $n = 3$, then ℓ_n does not have an odd primitive divisor.

For every integer $n \geq 1$, we say that a prime number p is a *high primitive divisor* of ℓ_n if p is an odd primitive divisor of ℓ_n such that $p^{\nu_p(\ell_n)} > n$.

Lemma 9. *Let $n \geq 3$ be an integer. If $a_1 = 1$ and $n \notin \{3,4,6,8,10,12,14,18,24\}$, or $a_1 = 2$ and $n \notin \{4,6,12\}$, or $a_1 = 3$ and $n \notin \{3,6\}$, or $a_1 \geq 4$, then ℓ_n has at least one high primitive divisor.*

Proof. Suppose that $n \geq 5$ and $n \neq 6$. We claim that if $(2a_1)^{\varphi(n)/2} > n^2$ then ℓ_n has a high primitive divisor. Indeed, recalling that $\gamma - \delta = a_1$ and $\gamma\delta = 1$, by Lemma 6 we have that $|\phi_n| > (2a_1)^{\varphi(n)/2}$. Hence, by Lemma 5, we get that $(2a_1)^{\varphi(n)/2} > n^2$ implies that

$$\prod_{q \text{ prim. div. } \ell_n} q^{\nu_q(\ell_n)} > n. \tag{7}$$

In particular, from (7) it follows that ℓ_n has at least one primitive divisor. Let p be the greatest primitive divisor of ℓ_n. It is known that each primitive divisor q of ℓ_n satisfies $q \equiv \pm 1 \pmod{n}$ [20, p. 427]. Hence, either $p \geq n+1$, or $p = n-1$ and p is the unique primitive divisor of ℓ_n. In both cases, taking into account (7), we get that $p^{\nu_p(\ell_n)} > n$. Hence, we have that p is a high primitive divisor of ℓ_n (note that p is odd since $n \geq 5$).

If $n \geq 2 \cdot 10^9$ then $\varphi(n) > n/\log n$ [22, Lemma 4.1]. Hence, we get that

$$(2a_1)^{\varphi(n)/2} > 2^{n/(2\log n)} > n^2,$$

which implies that ℓ_n has a high primitive divisor.

If $180 \leq n < 2 \cdot 10^9$, then $\varphi(n) > n/6$ [22, Lemma 4.2]. Hence, we get that

$$(2a_1)^{\varphi(n)/2} > 2^{n/12} > n^2,$$

which implies that ℓ_n has a high primitive divisor.

If $5 \leq n \leq 179$ with $n \neq 6$, and $|a_1| \geq 7$, then

$$(2a_1)^{\varphi(n)/2} \geq 14^{\varphi(n)/2} > n^2,$$

which implies that ℓ_n has a high primitive divisor.

If $5 \leq n \leq 179$ with $n \neq 6$, and $a_1 \leq 6$, then with the aid of a computer one can check that ℓ_n has a high primitive divisor, unless $a_1 = 1$ and $n \in \{8,10,12,14,18,24\}$, or $a_1 = 2$ and $n = 12$. Note that this verification is done more efficiently by factorizing ℓ_n only in the cases in which the inequality $(2a_1)^{\varphi(n)/2} > n^2$ does not hold.

If $a_1 = 2$ or $a_1 = 3$, then ℓ_3 or ℓ_4 has a high primitive divisor, respectively. Hereafter, assume that $n \in \{3,4,6\}$ and $a_1 \geq 4$. It remains to prove that ℓ_n has a high primitive divisor. This is done similarly to the end of the proof of Lemma 7. Since $a_1 \geq 4$, by reasoning modulo 8 and modulo 9, it follows easily that a_1^2+2 is not equal to 2^s or $2^s 3$, for some integer $s \geq 0$, and that neither a_1^2+1 nor a_1^2+3 is equal to $2^s 3^t$ or $2^s 3^t 5$, for some integers $s,t \geq 0$. Hence, there exists a prime number $p \geq 5$ dividing a_1^2+1 and such that $p^{\nu_p(a_1^2+1)} > 6$. We claim that p is a high primitive divisor of ℓ_6. In fact, since $p \geq 5$, by (6) and recalling that $D = a_1^2+4$, we get that $p \mid \ell_6$, $p \nmid a_1 D \ell_1 \cdots \ell_5$, and $p^{\nu_p(\ell_6)} > 6$. The proof that ℓ_3 and ℓ_4 have a high primitive divisor proceeds similarly. □

Remark 10. Lemma 9 is optimal, that is, one can verify that if $a_1 = 1$ and $n \in \{3,4,6,8,10,12,14,18,24\}$, or $a_1 = 2$ and $n \in \{4,6,12\}$, or $a_1 = 3$ and $n \in \{3,6\}$, then ℓ_n has no high primitive divisor.

For every odd prime number p, let $\left(\frac{D}{p}\right)$ denote the Legendre symbol. Note that $\left(\frac{D}{p}\right) = 1$ if and only if f splits modulo p.

Lemma 11. *Let $n \geq 3$ be an odd integer and let p be an odd prime factor of ℓ_n. Then we have that* $\left(\frac{D}{p}\right) = 1$.

Proof. Since n is odd, we have that $v_n := (\gamma^n + \delta^n)/(\gamma + \delta)$ is a symmetric expression of the algebraic integers α, β (recall that $\gamma = \alpha$ and $\delta = -\beta$). Hence, we get that v_n is an integer. Furthermore, from $p \mid \ell_n$ and the identity

$$Dv_n^2 - a_1^2 \ell_n^2 = (\gamma + \delta)^2 v_n^2 - (\gamma - \delta)^2 \ell_n^2 = 4(\gamma\delta)^2 = 4,$$

we get that $Dv_n^2 \equiv 2^2 \pmod{p}$. Since p is odd, it follows that $p \nmid v_n$ and so $D \equiv (2v_n^{-1})^2 \pmod{p}$. Thus $\left(\frac{D}{p}\right) = 1$, as desired. □

2.2. *Multiplicative orders*

For every ideal $\mathfrak{i}$ of $\mathcal{O}_K$ and for every $\theta \in \mathcal{O}_K$, let $\operatorname{ord}_{\mathfrak{i}}(\theta)$ denote the multiplicative order of θ modulo $\mathfrak{i}$ (if it exists).

Lemma 12. *Let $n, v \geq 1$ be integers, let p be a prime number not dividing $a_1 D$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p. Then $p^v \mid \ell_n$ if and only if $\operatorname{ord}_{\mathfrak{p}^v}(\alpha^2) \mid n$. In particular, we have that p is a primitive divisor of ℓ_n if and only if $n = \operatorname{ord}_{\mathfrak{p}}(\alpha^2)$.*

Proof. Since $p \nmid a_1 D$, we have that $\alpha + \beta$ and $\alpha - \beta$ are invertible modulo $\mathfrak{p}^v$. Hence, using (2), we get that $p^v \mid \ell_n$ is equivalent to $\alpha^n \equiv (-\beta)^n \pmod{\mathfrak{p}^v}$, which in turn is equivalent to $(\alpha^2)^n \equiv 1 \pmod{\mathfrak{p}^v}$, since $\alpha/(-\beta) = \alpha^2$. Thus the claim follows. □

Lemma 13. *Let p be an odd prime number, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p, and let $v \geq 1$ be an integer. Then the equation $X^2 \equiv 1 \pmod{\mathfrak{p}^v}$ has exactly two solutions modulo $\mathfrak{p}^v$, namely 1 and -1.*

Proof. The equation $X^2 \equiv 1 \pmod{\mathfrak{p}^v}$ is equivalent to $\nu_{\mathfrak{p}}(X-1) + \nu_{\mathfrak{p}}(X+1) \geq v$, where $\nu_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation over $\mathcal{O}_K$. Moreover, we have that $\nu_{\mathfrak{p}}(X-1)$ and $\nu_{\mathfrak{p}}(X+1)$ cannot both be positive, since $2 \notin \mathfrak{p}$. Hence, either $X \equiv 1 \pmod{\mathfrak{p}^v}$ or $X \equiv -1 \pmod{\mathfrak{p}^v}$. □

Lemma 14. *Let p be an odd prime number, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p, and let $v \geq 1$ be an integer. Put $a := \operatorname{ord}_{\mathfrak{p}^v}(\alpha)$, $b := \operatorname{ord}_{\mathfrak{p}^v}(\beta)$, and $c := \operatorname{ord}_{\mathfrak{p}^v}(\alpha^2)$. Then the following statements hold.*

(1) *If c is odd then $a = c$ and $b = 2c$, or $a = 2c$ and $b = c$.*
(2) *If c is even then $a = b = 2c$.*
(3) $\operatorname{lcm}(a, b) = 2c$.

Proof. Hereafter, all congruences are modulo $\mathfrak{p}^v$. Since $\alpha^{2c} \equiv 1$, we have that $a \mid 2c$ and, by Lemma 13, that $\alpha^c \equiv \pm 1$. Moreover, from $\alpha^a \equiv 1$, we have that $\alpha^{2a} \equiv 1$, and so $c \mid a$. Hence, we get that $a = c$ if $\alpha^c \equiv 1$, and $a = 2c$ if $\alpha^c \equiv -1$.

Using the fact that $\beta^2 = \alpha^{-2}$, we get that $c = \operatorname{ord}_{\mathfrak{p}^v}(\beta^2)$. Hence, by a reasoning similar to before, we have that $\beta^c \equiv \pm 1$, while $b = c$ if $\beta^c \equiv 1$, and $b = 2c$ if $\beta^c \equiv -1$.

Suppose that c is odd. Since $\alpha\beta = -1$, we have that $\alpha^c \beta^c \equiv (-1)^c \equiv -1$. Hence, either $\alpha^c \equiv 1$ and $\beta^c \equiv -1$, or $\alpha^c \equiv -1$ and $\beta^c \equiv 1$. By the previous considerations, it follows that either $a = c$ and $b = 2c$, or $a = 2c$ and $b = c$. This proves (1).

Suppose that c is even. Then, by the minimality of c, we get that $\alpha^c \equiv \beta^c \equiv -1$. Hence, by the previous considerations, we have that $a = b = 2c$. This proves (2).

Finally, we obtain (3) as a direct consequence of (1) and (2). □

2.3. *Second-order linear recurrences*

In this section, we collect some results on linear recurrences in $\mathscr{L}(f)$.

Lemma 15. *Let $\boldsymbol{x} \in \mathscr{L}(f)$. Then we have that*

$$x_n = \frac{(x_1 - \beta x_0)\alpha^n - (x_1 - \alpha x_0)\beta^n}{\alpha - \beta}$$

for every integer $n \geq 0$.

Proof. This is a special case of the general expression of linear recurrences as generalized power sums [10, Section 1.1.6] and can be easily proven by induction. □

Lemma 16. *Let $\boldsymbol{x} \in \mathscr{L}(f)$, let p be a prime number not dividing $2(x_1^2 - a_1 x_1 x_0 - x_0^2)D$, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p, and let $v \geq 1$ be an integer. Then we have that $\tau(\boldsymbol{x}; p^v) = 2\operatorname{ord}_{\mathfrak{p}^v}(\alpha^2)$.*

Proof. The claim can be derived from more general results on the period of linear recurrences modulo integers [10, Section 3.1], but we provide a short proof for completeness.

Define the matrix

$$M := \begin{pmatrix} (x_1 - \beta x_0) & -(x_1 - \alpha x_0) \\ (x_1 - \beta x_0)\alpha & -(x_1 - \alpha x_0)\beta \end{pmatrix}$$

and note that

$$\det(M) = (x_1^2 - a_1 x_1 x_0 - x_0^2)(\alpha - \beta).$$

Since $p \nmid (x_1^2 - a_1 x_1 x_0 - x_0^2)D$, we get that $\alpha - \beta$ and M are invertible modulo $\mathfrak{p}^v$. Hence, by Lemma 15, for every integer $n \geq 1$, we have that

$$\begin{aligned} \begin{cases} x_n \equiv x_0 \\ x_{n+1} \equiv x_1 \end{cases} \pmod{p^v} \quad &\iff \quad M\begin{pmatrix} \alpha^n \\ \beta^n \end{pmatrix} \equiv (\alpha - \beta)\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \pmod{\mathfrak{p}^v} \\ &\iff \quad \begin{pmatrix} \alpha^n \\ \beta^n \end{pmatrix} \equiv M^{-1}(\alpha - \beta)\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \pmod{\mathfrak{p}^v} \\ &\iff \quad \begin{pmatrix} \alpha^n \\ \beta^n \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{\mathfrak{p}^v}. \end{aligned}$$

Therefore, we get that $\tau(\boldsymbol{x}; p^v) = \operatorname{lcm}\big(\operatorname{ord}_{\mathfrak{p}^v}(\alpha), \operatorname{ord}_{\mathfrak{p}^v}(\beta)\big)$. Then, since p is odd, the claim follows from Lemma 14(3). □

Lemma 17. *Let $n \geq 3$ be integer. Suppose that p is an odd primitive divisor of ℓ_n such that $\big(\frac{D}{p}\big) = 1$. Then there exists $\boldsymbol{x} \in \mathscr{L}(f)$ such that $\tau(\boldsymbol{x}; p) = \rho(\boldsymbol{x}; p) = 2n$ and all the residues of $\boldsymbol{x}$ modulo p are nonzero. Moreover, if n is odd, then there exists $\boldsymbol{y} \in \mathscr{L}(f)$ such that $\tau(\boldsymbol{y}; p) = \rho(\boldsymbol{y}; p) = n$ and all the residues of $\boldsymbol{y}$ modulo p are nonzero.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p. Since p is a primitive divisor of ℓ_n, by Lemma 12 we have that $\operatorname{ord}_{\mathfrak{p}}(\alpha^2) = n$. Since p is odd and $\big(\frac{D}{p}\big) = 1$, we have that f splits modulo p, that is, there exist integers a, b such that $a \equiv \alpha \pmod{\mathfrak{p}}$ and $b \equiv \beta \pmod{\mathfrak{p}}$. In particular, we have that $\operatorname{ord}_p(a) = \operatorname{ord}_{\mathfrak{p}}(\alpha)$ and $\operatorname{ord}_p(b) = \operatorname{ord}_{\mathfrak{p}}(\beta)$, where ord_p denotes the multiplicative order modulo p. By Lemma 14(1)–(2), we get that $\operatorname{ord}_p(a) = 2n$ or $\operatorname{ord}_p(b) = 2n$. By swapping a and b, we can assume that $\operatorname{ord}_p(a) = 2n$. Let $\boldsymbol{x} \in \mathscr{L}(f)$ such that $x_0 = 1$ and $x_1 = a$. Since $f(a) \equiv 0 \pmod{p}$, it follows easily by induction that $x_n \equiv a^n \pmod{p}$ for every integer $n \geq 0$. Hence, we get that $\tau(\boldsymbol{x}; p) = \rho(\boldsymbol{x}; p) = 2n$ and all the residues of $\boldsymbol{x}$ modulo p are nonzero, as desired.

If n is odd, then by Lemma 14(1), we have that $\operatorname{ord}_p(b) = n$. Let $\boldsymbol{y} \in \mathscr{L}(f)$ such that $y_0 = 1$ and $y_1 = b$. Then, reasoning as for $\boldsymbol{x}$, we get that $\tau(\boldsymbol{y}; p) = \rho(\boldsymbol{y}; p) = n$ and all the residues of $\boldsymbol{y}$ modulo p are nonzero, as desired. □

Lemma 18. *Let $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 = 1$, let p be a prime number not dividing D, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p, let $v \geq 1$ be an integer, let $n := \operatorname{ord}_{\mathfrak{p}}(\alpha^2)$, and let $s \geq 0$ be an integer. Then we have that $x_s \equiv 0 \pmod{p^v}$ if and only if*

$$x_1 \equiv \frac{\beta - \alpha y_s}{1 - y_s} \pmod{\mathfrak{p}^v} \tag{8}$$

and $1 - y_s$ is invertible modulo $\mathfrak{p}^v$, where $y_s := (-\alpha^2)^{-s}$.

Proof. Since $p \nmid D$, we get that $\alpha - \beta$ is invertible modulo $\mathfrak{p}^v$. Hence, employing Lemma 15 and the fact that $\beta = -\alpha^{-1}$, it follows easily that $x_s \equiv 0 \pmod{p^v}$ is equivalent to

$$x_1(1 - y_s) \equiv \beta - \alpha y_s \pmod{\mathfrak{p}^v}. \tag{9}$$

We claim that if (9) holds then $1 - y_s$ is invertible modulo $\mathfrak{p}^v$. Indeed, if $1 - y_s$ is not invertible modulo $\mathfrak{p}^v$, then $y_s \equiv 1 \pmod{\mathfrak{p}}$, and so (9) implies that $\alpha - \beta \equiv 0 \pmod{\mathfrak{p}}$, which is a contradiction, since $p \nmid D$. Hence, we have that $1 - y_s$ is invertible modulo $\mathfrak{p}^v$. Consequently, we get that (9) is equivalent to (8) and $1 - y_s$ being invertible modulo $\mathfrak{p}^v$, as desired. □

Lemma 19. *Let $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 = 1$, let p be a prime number not dividing D, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p, let $v \geq 1$ be an integer, let $n := \operatorname{ord}_{\mathfrak{p}}(\alpha^2)$, and let s, t be integers such that $0 \leq s < t < 2n$ and $s \equiv t \pmod 2$. Then we have that $x_s \equiv x_t \pmod{p^v}$ if and only if*

$$x_1 \equiv \frac{\beta - \alpha z_{s,t}}{1 - z_{s,t}} \pmod{\mathfrak{p}^v} \tag{10}$$

and $1 - z_{s,t}$ is invertible modulo $\mathfrak{p}^v$, where $z_{s,t} := (-1)^{t+1}\alpha^{-(s+t)}$.

Proof. Since $p \nmid D$, we get that $\alpha - \beta$ is invertible modulo $\mathfrak{p}^v$. Hence, employing Lemma 15, we have that $x_s \equiv x_t \pmod{p^v}$ is equivalent to

$$(x_1 - \beta)\alpha^s - (x_1 - \alpha)\beta^s \equiv (x_1 - \beta)\alpha^t - (x_1 - \alpha)\beta^t \pmod{\mathfrak{p}^v}. \tag{11}$$

Since $0 \leq s < t < 2n$, $s \equiv t \pmod 2$, and $n := \operatorname{ord}_{\mathfrak{p}}(\alpha^2)$, we have that $1 - \alpha^{t-s}$ is invertible modulo $\mathfrak{p}^v$. Hence, it follows that (11) is equivalent to

$$x_1 - \beta \equiv \frac{\beta^t(\beta^{s-t} - 1)}{\alpha^s(1 - \alpha^{t-s})}(x_1 - \alpha) \pmod{\mathfrak{p}^v}. \tag{12}$$

Since $\beta = -\alpha^{-1}$ and $s \equiv t \pmod 2$, we get that

$$\frac{\beta^t(\beta^{s-t} - 1)}{\alpha^s(1 - \alpha^{t-s})} = (-1)^{t+1}\alpha^{-(s+t)} = z_{s,t}.$$

Therefore, we have that (12) is equivalent to

$$x_1(1 - z_{s,t}) \equiv \beta - \alpha z_{s,t} \pmod{\mathfrak{p}^v}. \tag{13}$$

We claim that if (13) holds then $1 - z_{s,t}$ is invertible modulo $\mathfrak{p}^v$. Indeed, if $1 - z_{s,t}$ is not invertible modulo $\mathfrak{p}^v$, then $z_{s,t} \equiv 1 \pmod{\mathfrak{p}}$, and so (13) implies that $\alpha - \beta \equiv 0 \pmod{\mathfrak{p}}$, which is a contradiction, since $p \nmid D$. Hence, we have that $1 - z_{s,t}$ is invertible modulo $\mathfrak{p}^v$. Consequently, we get that (13) is equivalent to (10) and $1 - z_{s,t}$ being invertible modulo $\mathfrak{p}^v$, as desired. □

Lemma 20. *Let $n \geq 4$ be an even integer. Suppose that p is a high primitive divisor of ℓ_n such that $\left(\frac{D}{p}\right) = -1$, and put $v := \nu_p(\ell_n)$. Then there exists $\boldsymbol{x} \in \mathscr{L}(f)$ such that $\tau(\boldsymbol{x}; p^v) = 2n$, $x_s \not\equiv x_t \pmod{p^v}$ for all integers s, t with $0 \leq s < t < 2n$ and $s \equiv t \pmod 2$, and all the residues of $\boldsymbol{x}$ modulo p^v are nonzero.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p. Since p is a primitive divisor of ℓ_n and $p^\nu \mid \ell_n$, from Lemma 12 we have that $n = \operatorname{ord}_{\mathfrak{p}}(\alpha^2) = \operatorname{ord}_{\mathfrak{p}^\nu}(\alpha^2)$.

We claim that there exists an integer c that satisfies

$$c \not\equiv \frac{\beta - \alpha^{2k+1}}{1-\alpha^{2k}} \pmod{\mathfrak{p}^\nu} \tag{14}$$

for every integer $k \geq 0$ such that $1-\alpha^{2k}$ is invertible modulo $\mathfrak{p}^\nu$. Indeed, we have p^ν choices for c modulo $\mathfrak{p}^\nu$, while the right-hand side of (14) takes at most $n = \operatorname{ord}_{\mathfrak{p}^\nu}(\alpha^2)$ values modulo $\mathfrak{p}^\nu$. Since p is a high primitive divisor of ℓ_n, we have that $p^\nu > n$ and so it is possible to choose a value of c with the desired property.

Let $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 = 1$ and $x_1 = c$. Since $\left(\frac{D}{p}\right) = -1$, we have that $p \nmid D$ and that f has no roots modulo p. Hence, also since p is odd, we get that $p \nmid 2(x_1^2 - a_1 x_1 - 1)D$. Consequently, by Lemma 16, we get that $\tau(\boldsymbol{x}; p^\nu) = 2n$, as desired.

Since $n = \operatorname{ord}_{\mathfrak{p}^\nu}(\alpha^2)$, we have that $\alpha^{2n} \equiv 1 \pmod{\mathfrak{p}^\nu}$. Consequently, by Lemma 13, we get that $\alpha^n \equiv \pm 1 \pmod{\mathfrak{p}^\nu}$. In fact, since n is even and $n = \operatorname{ord}_{\mathfrak{p}^\nu}(\alpha^2)$, it follows that $\alpha^n \equiv -1 \pmod{\mathfrak{p}^\nu}$. Hence, we have that -1 is equal to a power of α^2 modulo $\mathfrak{p}^\nu$.

Suppose that there exist integers s, t such that $0 \leq s < t < 2n$, $s \equiv t \pmod 2$, and $x_s \equiv x_t \pmod{p^\nu}$. By Lemma 19, we get that

$$c \equiv x_1 \equiv \frac{\beta - \alpha z_{s,t}}{1 - z_{s,t}} \pmod{\mathfrak{p}^\nu}, \tag{15}$$

where $z_{s,t} := (-1)^{t+1}\alpha^{-(s+t)}$ is equal to a power of α^2 modulo $\mathfrak{p}^\nu$. But then (14) and (15) are in contradiction. Therefore, it follows that $x_s \not\equiv x_t \pmod{p^\nu}$ for all integers s, t with $0 \leq s < t < 2n$ and $s \equiv t \pmod 2$.

Suppose that $x_s \equiv 0 \pmod{p^\nu}$ for some integer $s \geq 0$. Then, by Lemma 18, we have that

$$c \equiv x_1 \equiv \frac{\beta - \alpha y_s}{1 - y_s} \pmod{\mathfrak{p}^\nu}, \tag{16}$$

where $y_s := (-\alpha^2)^{-s}$ is equal to a power of α^2 modulo $\mathfrak{p}^\nu$. But then (14) and (16) are in contradiction. Therefore, it follows that $x_s \not\equiv 0 \pmod{p^\nu}$ for all integers $s \geq 0$. □

For every $\boldsymbol{x} \in \mathscr{L}(f)$ and for all integers $m, d \geq 1$ and r, let us define

$$\rho(\boldsymbol{x}; m, r, d) := \#\{x_n \bmod m : n \geq 0,\ n \equiv r \pmod d\}.$$

We need the following lemma.

Lemma 21. *Let $m_1, m_2 \geq 1$ be coprime integers, let $\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)} \in \mathscr{L}(f)$, and put $\tau_i := \tau(\boldsymbol{x}^{(i)}; m_i)$ for each $i \in \{1,2\}$. If $\rho(\boldsymbol{x}^{(2)}; m_2) = \tau_2$ then there exists $\boldsymbol{x} \in \mathscr{L}(f)$ such that $\boldsymbol{x} \equiv \boldsymbol{x}^{(i)} \pmod{m_i}$ for each $i \in \{1,2\}$, and*

$$\rho(\boldsymbol{x}; m_1 m_2) = \frac{\tau_2}{d} \sum_{r=0}^{d-1} \rho(\boldsymbol{x}^{(1)}; m_1, r, d),$$

where $d := \gcd(\tau_1, \tau_2)$.

Proof. Since m_1, m_2 are coprime, we can pick $\boldsymbol{x} \in \mathscr{L}(f)$ such that $x_j \equiv x_j^{(i)} \pmod{m_i}$ for each $i \in \{1,2\}$ and $j \in \{0,1\}$. Then, it follows easily by induction that $x_j \equiv x_j^{(i)} \pmod{m_i}$ for each $i \in \{1,2\}$ and for every integer $j \geq 0$. At this point, the rest of the claim is a consequence of [9, Lemma 6]. □

3. Proof of Theorem 1

We collected in Table 1 some values of $\tau(\boldsymbol{x}; m)$ and $\rho(\boldsymbol{x}; m)$, for $\boldsymbol{x} \in \mathscr{L}(f)$ and $m \in \mathbb{Z}^+$, that are needed for the proof. We begin with the following lemma.

Lemma 22. *There exist $\boldsymbol{x} \in \mathscr{L}(f)$ and $m \in \mathbb{Z}^+$ such that $\rho(\boldsymbol{x}; m) = 4$ and all the residues of $\boldsymbol{x}$ modulo m are nonzero. In particular, we have that $4 \in \mathscr{R}(f)$.*

Proof. If $a_1 = 1$ or $a_1 = 2$, then the claim follows from rows 2 or 13 of Table 1, respectively.

If a_1 is odd and $a_1 \geq 3$, then pick $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 = 1$, $x_1 = 2$, and let $m := 2a_1$. Since $2a_1 \equiv 0 \pmod{m}$ and $a_1^2 \equiv a_1 \pmod{m}$, we get that the first terms of $\boldsymbol{x}$ are congruent to

$$1, 2, 1, a_1 + 2, a_1 + 1, a_1 + 2, 1, 2, \ldots \pmod{m}.$$

Noting that $m \geq 6$ and $a_1 \not\equiv -2, -1, 0, 1 \pmod{m}$, it follows easily that $\tau(\boldsymbol{x}; m) = 6$, $\rho(\boldsymbol{x}; m) = 4$ and that all the residues of $\boldsymbol{x}$ modulo m are nonzero.

If a_1 is even and $a_1 \geq 4$, then pick $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 = 1$, $x_1 = 3$, and let $m := 2a_1$. Since $a_1^2 \equiv 2a_1 \equiv 0 \pmod{m}$, we get that the first terms of $\boldsymbol{x}$ are congruent to

$$1, 3, a_1 + 1, a_1 + 3, 1, 3, \ldots \pmod{m}.$$

Noting that $m \geq 8$ and $a_1 \not\equiv -3, -2, -1, 0, 2 \pmod{m}$, it follows easily that $\tau(\boldsymbol{x}; m) = \rho(\boldsymbol{x}; m) = 4$ and that all the residues of $\boldsymbol{x}$ modulo m are nonzero. □

Table 1. Values of $\tau(\boldsymbol{x}; m)$ and $\rho(\boldsymbol{x}; m)$ for $\boldsymbol{x} \in \mathscr{L}(X^2 - a_1 X - 1)$ with initial values x_0, x_1. The symbol $*$ means that all the residues of $\boldsymbol{x}$ modulo m are nonzero.

row n.	a_1	x_0	x_1	m	$\tau(\boldsymbol{x}; m)$	$\rho(\boldsymbol{x}; m)$	
1	1	0	1	3	8	3	
2	1	1	3	5	4	4	*
3	1	1	3	8	12	6	*
4	1	1	3	10	12	8	*
5	1	1	3	13	28	12	*
6	1	1	3	17	36	16	*
7	1	1	3	28	48	20	*
8	1	1	3	26	84	24	*
9	1	1	3	56	48	28	*
10	1	1	3	52	84	36	*
11	1	1	3	78	168	48	*
12	2	1	1	4	4	2	*
13	2	1	1	5	12	4	*
14	2	1	1	28	12	8	*
15	2	1	1	13	28	12	*
16	2	1	1	39	56	24	*
17	3	1	1	9	6	3	*
18	3	1	1	8	12	6	*
19	3	1	1	17	16	12	*

We have to prove that $\mathscr{R}(f) = \mathbb{Z}^+$. First, we prove that $\{n, 2n\} \subseteq \mathscr{R}(f)$ for every odd integer $n \geq 1$. We have that $1 \in \mathscr{R}(f)$, since $\rho(\boldsymbol{x}; 1) = 1$ for every $\boldsymbol{x} \in \mathscr{L}(f)$; and $2 \in \mathscr{R}(f)$, since $\rho(\boldsymbol{x}; 2) = 2$ for every $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 \not\equiv x_1 \pmod{2}$. If $a_1 = 1$, or $a_1 = 3$, then $\{3, 6\} \subseteq \mathscr{R}(f)$ by rows 1 and 3, or 17 and 18, of Table 1, respectively. Hence, assume that $n \geq 3$ is an odd integer, and $a_1 \notin \{1,3\}$ or $n \neq 3$. By Lemma 7, we have that ℓ_n has an odd primitive divisor p. Moreover, since n is odd, from Lemma 11 it follows that $\left(\frac{D}{p}\right) = 1$. Therefore, from Lemma 17 we obtain that $\{n, 2n\} \subseteq \mathscr{R}(f)$.

It remains to prove that $2n \in \mathscr{R}(f)$ for every even integer $n \geq 2$. By Lemma 22, we have that $4 \in \mathscr{R}(f)$. Hence, we can assume that $n \geq 4$.

If $a_1 = 1$ and $n \in \{4,6,8,10,12,14,18,24\}$, or $a_1 = 2$ and $n \in \{4,6,12\}$, or $a_1 = 3$ and $n = 6$, then $2n \in \mathscr{R}(f)$ by rows 4–11, 14–16, or 19 of Table 1, respectively.

Hence, assume that $n \geq 4$ is an even integer, and that $a_1 = 1$ and $n \notin \{4,6,8,10,12,14,18,24\}$, or $a_1 = 2$ and $n \notin \{4,6,12\}$, or $a_1 = 3$ and $n \neq 6$, or $a_1 \geq 4$. Then, by Lemma 9, we have that ℓ_n has a high primitive divisor p.

If $\left(\frac{D}{p}\right) = 1$ then Lemma 17 yields that $2n \in \mathscr{R}(f)$, as desired. Hence, suppose that $\left(\frac{D}{p}\right) = -1$. Thanks to Lemma 20, there exists $\boldsymbol{x}^{(1)} \in \mathscr{L}(f)$ such that $\tau(\boldsymbol{x}^{(1)}; m_1) = 2n$ and $\rho(\boldsymbol{x}^{(1)}; m_1, r, 2) = n$ for each $r \in \{0,1\}$, where $m_1 := p^{\nu_p(\ell_n)}$. Note that, since n is even, we also get that $\rho(\boldsymbol{x}^{(1)}; m_1, r, 4) = n/2$ for each $r \in \{0,1,2,3\}$. We define $\boldsymbol{x}^{(2)} \in \mathscr{L}(f)$ and $m_2 \in \mathbb{Z}^+$ as follows. If $a_1 = 1$ then we pick $\boldsymbol{x}^{(2)}$ and m_2 from rows 2 of Table 1. If $a_1 \geq 2$ then we let $x_0^{(2)} := 0$, $x_1^{(2)} := 1$, and put $m_2 := a_1$. It follows easily that $\tau(\boldsymbol{x}^{(2)}; m_2) = \rho(\boldsymbol{x}^{(2)}; m_2) \in \{2,4\}$. Since p is a primitive divisor of ℓ_n, we have that $p \nmid a_1 D$. Hence, we get that m_1, m_2 are coprime integers. (Note that $m_2 = D = 5$ if $a_1 = 1$.) Put $\tau_i := \tau(\boldsymbol{x}^{(i)}; m_i)$ for each $i \in \{1,2\}$, and let $d := \gcd(\tau_1, \tau_2)$. Note that, since n is even, we have that $d = \tau_2 \in \{2,4\}$. Therefore, applying Lemma 21 we get that there exists $\boldsymbol{x} \in \mathscr{L}(f)$ such that

$$\rho(\boldsymbol{x}; m_1 m_2) = \frac{\tau_2}{d} \sum_{r=0}^{d-1} \rho(\boldsymbol{x}^{(1)}; m_1, r, d) = 1 \cdot \sum_{r=0}^{d-1} \frac{2n}{d} = 2n,$$

so that $2n \in \mathscr{R}(f)$, as desired. The proof that $\mathscr{R}(f) = \mathbb{Z}^+$ is complete.

At this point, note that for each integer $n \geq 4$, and for each integer $n \geq 3$ if $a_1 \geq 2$, the sequence $\boldsymbol{x} \in \mathscr{L}(f)$ and the modulo m that we constructed so that $\rho(\boldsymbol{x}; m) = n$ have the additional property that all the residues of $\boldsymbol{x}$ modulo m are nonzero. This follows from Table 1, Lemma 17, Lemma 22, and Lemma 20–Lemma 21 (note that $\boldsymbol{x}$ has no zero modulo $m_1 m_2$ since $\boldsymbol{x}^{(1)}$ has no zero modulo m_1). Moreover, if $a_1 \geq 2$, then picking $\boldsymbol{x} \in \mathscr{L}(f)$ with $x_0 = 1$, $x_1 = 1$, and $m := a_1$, we get that $\rho(\boldsymbol{x}; m) = 1$ and all the residues of $\boldsymbol{x}$ modulo m are nonzero. If $a_1 = 2$ or $a_1 \geq 3$, then picking $\boldsymbol{x}$ and m as in row 12 of Table 1, or taking $x_0 = 1$, $x_1 = 2$, and $m = a_1$, we get that $\rho(\boldsymbol{x}; m) = 2$ and all the residues of $\boldsymbol{x}$ modulo m are nonzero.

It remains to prove that if $a_1 = 1$ and $n \in \{1,2,3\}$ then there exist no $\boldsymbol{x} \in \mathscr{L}(f)$ and $m \in \mathbb{Z}^+$ such that $\rho(\boldsymbol{x}; m) = n$ and all the residues of $\boldsymbol{x}$ modulo m are nonzero. This is done in the last paragraph of [9, p. 122].

The proof is complete.

4. Proof of Corollary 2

If $a_1 = 1$ then the result is in fact [9, Corollary 2]. Hence, assume that $a_1 \geq 2$.

We order α and β so that $\alpha = \left(a_1 + \sqrt{D}\right)/2$ and $\beta = \left(a_1 - \sqrt{D}\right)/2$. In particular, note that $\alpha > 1$ and $-1 < \beta < 0$.

Let $k \geq 1$ be an integer. By Theorem 1, there exist $\boldsymbol{x} \in \mathscr{L}(f)$ and $m \in \mathbb{Z}^+$ such that $\rho(\boldsymbol{x}; m) = k$ and $x_n \not\equiv 0 \pmod{m}$ for every integer $n \geq 0$. Moreover, by Lemma 15, we have that $x_n = c_1\alpha^n - c_2\beta^n$ for all integers $n \geq 0$, where

$$c_1 := \frac{x_1 - \beta x_0}{\alpha - \beta} \quad \text{and} \quad c_2 := \frac{x_1 - \alpha x_0}{\alpha - \beta}.$$

By eventually replacing $\boldsymbol{x}$ with $-\boldsymbol{x} := (-x_n)_{n\geq 0}$, we can assume that $c_1 > 0$. Furthermore, note that $c_2 \neq 0$. Let $\xi := c_1/m$, so that $\xi \in \mathbb{Q}(\alpha)$. Then, we have that

$$\xi\alpha^n - \frac{x_n}{m} = \frac{c_2\beta^n}{m} \longrightarrow 0, \tag{17}$$

as $n \to +\infty$, since $|\beta| < 1$. Let $r_1, \ldots, r_k \in \mathbb{Z}$, with $0 < r_1 < \cdots < r_k < m$, be the residues of $\boldsymbol{x}$ modulo m. From (17) it follows easily that the set of limit points of $\big(\operatorname{frac}(\xi\alpha^n)\big)_{n\geq 0}$ is equal to $\{r_1/m, \ldots, r_k/m\}$. Hence, we get that $\big(\operatorname{frac}(\xi\alpha^n)\big)_{n\geq 0}$ has exactly k limit points.

The proof is complete.

Acknowledgments

The authors would like to thank the anonymous referee for carefully reading the paper and for providing valuable suggestions.

Declaration of interests

The authors do not work for, advise, own shares in, or receive funds from any organization that could benefit from this article, and have declared no affiliations other than their research organizations.

References

[1] B. Avila and Y. Chen, “On moduli for which the Lucas numbers contain a complete residue system”, *Fibonacci Q.* **51** (2013), no. 2, pp. 151–152.

[2] Y. Bilu, G. Hanrot and P. M. Voutier, “Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte”, *J. Reine Angew. Math.* **539** (2001), pp. 75–122.

[3] R. T. Bumby, “A distribution property for linear recurrence of the second order”, *Proc. Am. Math. Soc.* **50** (1975), pp. 101–106.

[4] S. A. Burr, “On moduli for which the Fibonacci sequence contains a complete system of residues”, *Fibonacci Q.* **9** (1971), no. 5, pp. 497–504.

[5] A. Dubickas, “There are infinitely many limit points of the fractional parts of powers”, *Proc. Indian Acad. Sci., Math. Sci.* **115** (2005), no. 4, pp. 391–397.

[6] A. Dubickas, “Arithmetical properties of powers of algebraic numbers”, *Bull. Lond. Math. Soc.* **38** (2006), no. 1, pp. 70–80.

[7] A. Dubickas, “On the limit points of the fractional parts of powers of Pisot numbers”, *Arch. Math., Brno* **42** (2006), no. 2, pp. 151–158.

[8] A. Dubickas and A. Novikas, “Linear recurrence sequences without zeros”, *Czech. Math. J.* **64(139)** (2014), no. 3, pp. 857–865.

[9] A. Dubickas and A. Novikas, “Recurrence with prescribed number of residues”, *J. Number Theory* **215** (2020), pp. 120–137.

[10] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence sequences*, American Mathematical Society, 2003, pp. xiv+318.

[11] T. Herendi, “Uniform distribution of linear recurring sequences modulo prime powers”, *Finite Fields Appl.* **10** (2004), no. 1, pp. 1–23.

[12] M. Javaheri and S. Cambrea, “The distribution of Fibonacci numbers modulo primes”, *Am. Math. Mon.* **129** (2022), no. 1, pp. 75–79.

[13] H. Niederreiter, A. Schinzel and L. Somer, “Maximal frequencies of elements in second-order linear recurring sequences over a finite field”, *Elem. Math.* **46** (1991), no. 5, pp. 139–143.

[14] C. Pisot, “Répartition (mod1) des puissances successives des nombres réels”, *Comment. Math. Helv.* **19** (1946), pp. 153–160.

[15] C. Sanna, “On the number of residues of linear recurrences”, *Res. Number Theory* **8** (2022), no. 1, article no. 7 (10 pages).

[16] A. Schinzel, “Special Lucas sequences, including the Fibonacci sequence, modulo a prime”, in *A tribute to Paul Erdős*, Cambridge University Press, 1990, pp. 349–357.

[17] L. Somer, “Primes having an incomplete system of residues for a class of second-order recurrences”, in *Applications of Fibonacci numbers (San Jose, CA, 1986)*, Kluwer Academic Publishers, 1988, pp. 113–141.

[18] L. Somer, “Distribution of residues of certain second-order linear recurrences modulo p. III”, in *Applications of Fibonacci numbers, Vol. 6 (Pullman, WA, 1994)*, Kluwer Academic Publishers, 1996, pp. 451–471.

[19] L. Somer and M. Křížek, “On moduli for which certain second-order linear recurrences contain a complete system of residues modulo m”, *Fibonacci Q.* **55** (2017), no. 3, pp. 209–228.

[20] C. L. Stewart, “On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers”, *Proc. Lond. Math. Soc.* **35** (1977), no. 3, pp. 425–447.

[21] T. Vijayaraghavan, “On the fractional parts of the powers of a number. I”, *J. Lond. Math. Soc.* **15** (1940), pp. 159–160.

[22] M. Ward, “The intrinsic divisors of Lehmer numbers”, *Ann. Math.* **62** (1955), pp. 230–236.

[23] T. Zaïmi, “An arithmetical property of powers of Salem numbers”, *J. Number Theory* **120** (2006), no. 1, pp. 179–191.

[24] T. Zaïmi, M. Selatnia and H. Zekraoui, “Comments on the fractional parts of Pisot numbers”, *Arch. Math., Brno* **51** (2015), no. 3, pp. 153–161.