On the number of residues of linear recurrences

ON THE NUMBER OF RESIDUES OF LINEAR RECURRENCES

CARLO SANNA†

ABSTRACT. For every nonconstant monic polynomial $g \in \mathbb{Z}[X]$, let $\mathfrak{M}(g)$ be the set of positive integers m for which there exist an integer linear recurrence $(s_n)_{n\geq 0}$ having characteristic polynomial g and a positive integer M such that $(s_n)_{n\geq 0}$ has exactly m distinct residues modulo M. Dubickas and Novikas proved that $\mathfrak{M}(X^2 - X - 1) = \mathbb{N}$. We study $\mathfrak{M}(g)$ in the case in which g is divisible by a monic quadratic polynomial $f \in \mathbb{Z}[X]$ with roots α, β such that $\alpha\beta = \pm 1$ and α/β is not a root of unity. We show that this problem is related to the existence of special primitive divisors of certain Lehmer sequences, and we deduce some consequences on $\mathfrak{M}(g)$. In particular, for $\alpha\beta = -1$, we prove that $m \in \mathfrak{M}(g)$ for every integer $m \geq 7$ with $m \neq 10$ and $4 \nmid m$.

1. INTRODUCTION

An integer sequence $\mathbf{s} = (s_n)_{n\geq 0}$ is a *linear recurrence* if there exist $c_1, \ldots, c_r \in \mathbb{Z}$ such that

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_r s_{n-r}, \tag{1}$$

for every integer $n \geq r$. The values $s_0, \ldots, s_{r-1}$ are the *initial conditions* of $\mathbf{s}$, and

$$g(X) = X^r - c_1 X^{r-1} - c_2 X^{r-2} - \cdots - c_r$$

is the *characteristic polynomial* of $\mathbf{s}$. Together they completely determine $\mathbf{s}$ via (1). A classic example of linear recurrence is the sequence of *Fibonacci numbers*, having initial conditions $0, 1$ and characteristic polynomial $X^2 - X - 1$. It is easily seen that $\mathbf{s}$ is ultimately periodic modulo M, for every positive integer M, and purely periodic if $(c_r, M) = 1$. Indeed, properties of linear recurrences modulo M have been studied intensively, including: which residues modulo M appear in the $\mathbf{s}$ and how frequently [4, 6, 9, 12, 15, 17], and for which positive integers M the linear recurrence $\mathbf{s}$ contains a complete system of residues modulo M [2, 5, 16, 18].

Let $\mathfrak{M}(g)$ denote the set of positive integers m such that there exist initial conditions $s_0, \ldots, s_{r-1} \in \mathbb{Z}$ and a positive integer M for which the linear recurrence $\mathbf{s}$ has exactly m distinct residues modulo M. Dubickas and Novikas [7] proved that $\mathfrak{M}(X^2 - X - 1) = \mathbb{N}$ and stated that the problem of determining $\mathfrak{M}(g)$ "may be very difficult in general". The first step of their proof is a lemma regarding roots of $X^2 - X - 1$ modulo p that have a prescribed multiplicative order [7, Lemma 3]. We provide below a straighforward generalization of it. (The proof is postponed to Section 3). For every integer a and for each prime number p, we let $\mathrm{ord}_p(a)$ denote the multiplicative order of a modulo p, with the implicit condition that $p \nmid a$.

Lemma 1.1. *Let $f, g \in \mathbb{Z}[x]$ be nonconstant monic polynomials with $f \mid g$, let m be a positive integer, and let p be a prime number. Suppose that:*

(i) There exists $a \in \mathbb{Z}$ such that $p \mid f(a)$ and $\mathrm{ord}_p(a) = m$.

Then $m \in \mathfrak{M}(g)$.

For $f = g = X^2 - X - 1$ and for positive integers m belonging to certain residue classes modulo 40, Dubickas and Novikas showed how to construct a and p satisfying (i) by using primitive divisors of Lucas numbers [7, Lemma 5, Lemma 7].

2010 *Mathematics Subject Classification.* Primary: 11B37, Secondary: 11B39, 11B50.

Key words and phrases. Lehmer sequence; linear recurrence; primitive divisor; residue.

† C. Sanna is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino.

Our first contribution is the next theorem, which shows that for more general quadratic polynomials f the statement (i) is equivalent to p being a particular primitive divisor of a certain term of a Lehmer sequence.

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* $(u_n(\gamma,\delta))_{n\geq 0}$ associated to γ, δ is defined by

$$u_n(\gamma,\delta) := \begin{cases} (\gamma^n-\delta^n)/(\gamma-\delta) & \text{if } 2\nmid n, \\ (\gamma^n-\delta^n)/(\gamma^2-\delta^2) & \text{if } 2\mid n, \end{cases}$$

for all integers $n \geq 0$. The conditions on γ, δ ensure that each $u_n(\gamma,\delta)$ is an integer. A prime number p is a *primitive divisor* of $u_n(\gamma,\delta)$ if $p \mid u_n(\gamma,\delta)$ but $p \nmid (\gamma^2-\delta^2)^2 u_1(\gamma,\delta)\cdots u_{n-1}(\gamma,\delta)$.

Theorem 1.2. *Let $f \in \mathbb{Z}[X]$ be a monic quadratic polynomial with roots α, β such that $\alpha\beta = \pm 1$ and α/β is not a root of unity. Also, let m be a positive integer and let p be a prime number. If $\alpha\beta = -1$ then put $\gamma := \alpha$, $\delta := -\beta$, and $n := m/(m,2)$, while if $\alpha\beta = +1$ then put $\gamma := \alpha^{1/2}$, $\delta := \alpha^{-1/2}$, and $n := m$. Then (i) is equivalent to:*

(ii) p is a primitive divisor of $u_n(\gamma,\delta)$ and $p \equiv 1 \pmod m$.

Moreover, each of the following implies (i) and (ii):

(iii) $\alpha\beta = -1$, $4 \nmid m$, $m \notin \{3, 6\}$, and p is a primitive divisor of $u_{m/(m,2)}(\gamma,\delta)$.

(iv) $\alpha\beta = -1$, $8 \mid m$, p is a primitive divisor of $u_{m/2}(\gamma,\delta)$, and $p \equiv 1 \pmod 4$.

(v) $\alpha\beta = +1$, $4 \mid m$, p is a primitive divisor of $u_m(\gamma,\delta)$, and $p \equiv 1 \pmod 4$.

As consequences of Theorem 1.2, Lemma 1.1, and results on the existence of primitive divisors of terms of Lehmer sequences (Lemma 3.4 and 3.7 below), we obtain the following results on $\mathfrak{M}(g)$.

Theorem 1.3. *Let f, α, β be as in Theorem 1.2 with $\alpha\beta = -1$, and let $g \in \mathbb{Z}[X]$ be a monic polynomial with $f \mid g$. Then $m \in \mathfrak{M}(g)$ for every integer $m \geq 7$, with $m \neq 10$ and $4 \nmid m$.*

Theorem 1.4. *Let f, α, β be as in Theorem 1.2 and let $g \in \mathbb{Z}[X]$ be a monic polynomial with $f \mid g$. Write $(\alpha-\beta)^2 = D_0 D_1^2$, where $D_0, D_1 \in \mathbb{Z}$ and D_0 is squarefree. Suppose that $D_0 \geq 5$ and $D_0 \equiv 1 \pmod 4$. Then $m \in \mathfrak{M}(g)$ for every positive integer m with $8D_0 \mid m$ if $\alpha\beta = -1$, and $4D_0 \mid m$ if $\alpha\beta = +1$.*

Given two specific polynomials $f, g \in \mathbb{Z}[X]$ satisfying the hypothesis of Theorem 1.3 and Theorem 1.4, one can try to determine $\mathfrak{M}(g)$ by using the aforementioned theorems and by employing [7, Lemma 6]. However, this requires a meticulous inspection of the numerical values of certain linear recurrences of characteristic polynomial g, and a detailed case-by-case analysis, as the one done by Dubickas and Novikas for $\mathfrak{M}(X^2-X-1)$ [7, Sections 6–8].

Remark 1.1. It should be possible to provide an equivalent version of Theorem 1.2 in terms of primitive divisors of the *Lehmer–Pierce sequence* $(\Delta_n(\alpha,\beta))_{n\geq 0}$ [8, 11, 13], which is defined by $\Delta_n(\alpha,\beta) := (\alpha^n-1)(\beta^n-1)$ for every integer $n \geq 0$.

2. Notation

For every integer a and for each prime number p, we let $\mathrm{ord}_p(a)$ denote the multiplicative order of a modulo p, with the implicit condition that $p \nmid a$. Also, when p is odd, we write $\left(\frac{a}{p}\right)$ for the Legendre symbol. For algebraic integers ζ and η, the notation $\zeta \equiv \eta \pmod p$ means that p divides $\zeta - \eta$, that is, $(\zeta-\eta)/p$ is an algebraic integer. For every positive integer n, we let $\varphi(n)$ be the Euler totient function of n. Furthermore, we write $\Phi_n(X)$ for the nth cyclotomic polynomial, and $\Phi_n(X,Y) := \Phi_n(X/Y)Y^{\varphi(n)}$ for its homogenization. Given two monic polynomials $f, g \in \mathbb{Z}[X]$, we let $\mathrm{Res}(f,g)$ denote their resultant.

3. Preliminaries

We begin by proving Lemma 1.1.

Proof of Lemma 1.1. Put $r := \deg(g)$ and let $\mathbf{s} = (s_n)_{n\geq 0}$ be the linear recurrence with initial conditions $1, a, \dots, a^{r-1}$ and characteristic polynomial g. We shall prove that $s_n \equiv a^n \pmod p$ for every integer $n \geq 0$. In turn, since $\operatorname{ord}_p(a) = m$, this implies that $\mathbf{s}$ has exactly m distinct residues modulo p, namely $1, a, \dots, a^{m-1} \pmod p$, and consequently $m \in \mathfrak{M}(g)$. Let us proceed by induction on n. For $n = 0, \dots, r-1$ the claim is obvious because of the initial conditions of $\mathbf{s}$. Assuming that the claim is true for every nonnegative integer less than n, let us prove it for n. From (1) and the induction hypothesis, we have that

$$\begin{aligned} s_n &\equiv c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_r s_{n-r} \equiv c_1 a^{n-1} + c_2 a^{n-2} + \cdots + c_r a^{n-r} \\ &\equiv a^{n-r}(a^r - g(a)) \equiv a^n \pmod p, \end{aligned}$$

because $p \mid f(a) \mid g(a)$. □

The next result is a simple equivalence for (i).

Lemma 3.1. *Let $f \in \mathbb{Z}[X]$ be a nonconstant monic polynomial, let m be a positive integer, and let p be a prime number. Then (i) is equivalent to $p \mid \operatorname{Res}(f, \Phi_m)$ and $p \equiv 1 \pmod m$.*

Proof. On the one hand, if (i) holds then a is a primitive mth root of unity modulo p. Hence, $p \equiv 1 \pmod m$ and a is a root of Φ_m modulo p. Since $p \mid f(a)$, we have that a is a common root of f and Φ_m modulo p, and consequently $p \mid \operatorname{Res}(f, \Phi_m)$. On the other hand, if $p \mid \operatorname{Res}(f, \Phi_m)$ and $p \equiv 1 \pmod m$ then Φ_m splits completely modulo p and it has a common root with f, thus (i) follows. □

We need some results on Lehmer sequences and related values of cyclotomic polynomials. It is known that a prime number p divides some term of a Lehmer sequence $(u_n(\gamma,\delta))_{n\geq 0}$ if and only if $p \nmid \gamma\delta$. In such a case, let $r_p(\gamma,\delta)$ be the *rank of appearance* of p, that is, the smallest positive integer k such that $p \mid u_k(\gamma,\delta)$. Furthermore, it can be proved that $\Phi_n(\gamma,\delta) \in \mathbb{Z}$ for every integer $n \geq 3$ (for these facts see, e.g., [20]).

Lemma 3.2. *Let $(u_k(\gamma,\delta))_{k\geq 0}$ be a Lehmer sequence, let p be a prime number, and let $n \geq 3$ be an integer. Then we have the following:*

(p1) $p \mid u_n(\gamma,\delta)$ *if and only if* $p \nmid \gamma\delta$ *and* $r_p(\gamma,\delta) \mid n$.

(p2) If $p \nmid \gamma\delta$ *and* $p \mid (\gamma^2-\delta^2)^2$ *then* $r_p(\gamma,\delta) \in \{p, 2p\}$.

(p3) If $2 \nmid \gamma\delta(\gamma^2-\delta^2)^2$ *then* $r_2(\gamma,\delta) = 3$.

(p4) If $p \nmid 2\gamma\delta(\gamma+\delta)^2$ *then* $p \equiv \left(\frac{(\gamma^2-\delta^2)^2}{p}\right) \pmod{r_p(\gamma,\delta)}$.

(p5) If $p \mid \Phi_n(\gamma,\delta)$ *then* $p \nmid \gamma\delta$ *and* $n = r_p(\gamma,\delta)p^v$ *for some integer* $v \geq 0$.

(p6) p *is a primitive divisor of* $u_n(\gamma,\delta)$ *if and only if* $p \mid \Phi_n(\gamma,\delta)$ *and* $p \equiv \pm 1 \pmod n$.

(p7) If $n \geq 5$, $2 \nmid n$, *and* p *is a primitive divisor of* $u_n(\gamma,\delta)$ *then* $p \equiv \left(\frac{\gamma\delta(\gamma-\delta)^2}{p}\right) \pmod{2n}$.

(p8) If $4 \mid n$, $\gamma\delta = 1$, $\gamma - \delta \in \mathbb{Z}$, p *is a primitive divisor of* $u_n(\gamma,\delta)$, *and* $p \equiv 1 \pmod 4$ *then* $p \equiv 1 \pmod{2n}$.

Proof. Properties (p1), (p2), and (p3) follow from [3, Corollary 2.2], (p4) is [10, Theorem 1.9], and (p5) is [3, Proposition 2.3].

Let us prove (p6). On the one hand, if p is a primitive divisor of $u_n(\gamma,\delta)$ then $p \mid u_n(\gamma,\delta)$ but $p \nmid (\gamma^2-\delta^2)^2 u_1(\gamma,\delta)\cdots u_{n-1}(\gamma,\delta)$. Since for every positive integer k we have that

$$u_k(\gamma,\delta) = \begin{cases} \prod_{d\mid k,\, d>1} \Phi_d(\gamma,\delta) & \text{if } 2 \nmid k, \\ \prod_{d\mid k,\, d>2} \Phi_d(\gamma,\delta) & \text{if } 2 \mid k, \end{cases}$$

it follows that $p \mid \Phi_n(\gamma,\delta)$. Moreover, $n = r_p(\gamma,\delta)$ and, also by (p1), $p \nmid \gamma\delta(\gamma^2-\delta^2)^2$. Hence, from (p3) and (p4) we get that $p \equiv \pm 1 \pmod{n}$. On the other hand, if $p \mid \Phi_n(\gamma,\delta)$ and $p \equiv \pm 1 \pmod{n}$ then from (p5) we get that $p \nmid \gamma\delta$ and $n = r_p(\gamma,\delta)$. Hence, $p \mid u_n(\gamma,\delta)$ but $p \nmid u_1(\gamma,\delta)\cdots u_{n-1}(\gamma,\delta)$. Also, (p2) yields that $p \nmid (\gamma^2-\delta^2)^2$. Hence, p is a primitive divisor of $u_n(\gamma,\delta)$.

Now let us prove (p7). Since p is a primitive divisor of $u_n(\gamma,\delta)$, we have that $n = r_p(\gamma,\delta)$ and, also by (p1), $p \nmid \gamma\delta(\gamma^2-\delta^2)^2$. By $n \geq 5$ and (p3), we get that $p > 2$. Since $2 \nmid n$, we have that $v_n(\gamma,\delta) := (\gamma^n+\delta^n)/(\gamma+\delta)$ is an integer. Moreover, from $p \mid u_n(\gamma,\delta)$ and the identity

$$(\gamma+\delta)^2 v_n(\gamma,\delta)^2 - (\gamma-\delta)^2 u_n(\gamma,\delta)^2 = 4(\gamma\delta)^n,$$

it follows that $(\gamma+\delta)^2 v_n(\gamma,\delta)^2 \equiv 2^2(\gamma\delta)^n \pmod{p}$. Hence, $\left(\frac{(\gamma+\delta)^2}{p}\right) = \left(\frac{\gamma\delta}{p}\right)$ and consequently $\left(\frac{(\gamma^2-\delta^2)^2}{p}\right) = \left(\frac{\gamma\delta(\gamma-\delta)^2}{p}\right)$. Then by (p4) we obtain that $p \equiv \left(\frac{\gamma\delta(\gamma-\delta)^2}{p}\right) \pmod{n}$. Recalling that p and n are both odd, it follows that $p \equiv \left(\frac{\gamma\delta(\gamma-\delta)^2}{p}\right) \pmod{2n}$.

It remains to prove (p8). Since p is a primitive divisor of $u_n(\gamma,\delta)$, we have that $n = r_p(\gamma,\delta)$ and, also by (p1), $p \nmid \gamma\delta(\gamma^2-\delta^2)^2$. From $4 \mid n$, $p \equiv 1 \pmod 4$, and (p4), it follows that $\left(\frac{(\gamma^2-\delta^2)^2}{p}\right) = 1$. Also, $(\gamma^2-\delta^2)^2 = (\gamma-\delta)^2(\gamma+\delta)^2$ and $\gamma-\delta$ is an integer. Hence, $\left(\frac{(\gamma+\delta)^2}{p}\right) = 1$. Noting that $(\gamma+\delta)^2$ is the discriminant of $(X-\gamma)(X+\delta) = X^2-(\gamma-\delta)X-\gamma\delta \in \mathbb{Z}[X]$, one gets that $\gamma^{p-1} \equiv 1 \pmod{p}$. Multiplying both sides by $\delta^{(p-1)/2}$, and recalling that $\gamma\delta = 1$, it follows that $\gamma^{(p-1)/2} \equiv \delta^{(p-1)/2} \pmod{p}$, and so $p \mid u_{(p-1)/2}(\gamma,\delta)$. Consequently, by (p1), we have that $n \mid (p-1)/2$, that is, $p \equiv 1 \pmod{2n}$. □

We also need the following identity for a product of cyclotomic polynomials.

Lemma 3.3. *For every positive integer m, we have*

$$\Phi_m(X)\Phi_m(-X) = (-1)^{\varphi(m)}\Phi_{m/(m,2)}\big(X^2\big)^e,$$

where $e := 1$ if $4 \nmid m$, and $e := 2$ if $4 \mid m$.

Proof. For every positive integer n, let $\zeta_n := \mathrm{e}^{2\pi\mathrm{i}/n}$ be a primitive nth root of unity. We have

$$\Phi_m(X)\Phi_m(-X) = \prod_{\substack{1\leq k\leq m\\(k,m)=1}} (X-\zeta_m^k)(-X-\zeta_m^k) = (-1)^{\varphi(m)} \prod_{\substack{1\leq k\leq m\\(k,m)=1}} (X^2-\zeta_m^{2k}). \tag{2}$$

If $2 \nmid m$ then ζ_m^2 is a primitive mth root of unity and the last product of (2) is equal to $\Phi_m\big(X^2\big)$. If $2 \mid m$ then $\zeta_m^2 = \zeta_{m/2}$ is a primitive $(m/2)$th root of unity. Also, if $2 \,||\, m$ then $\zeta_{m/2}^2$ is a primitive $(m/2)$th root of unity, and the last product of (2) is equal to

$$\begin{aligned}\prod_{\substack{1\leq k\leq m\\(k,m)=1}} (X^2-\zeta_{m/2}^k) &= \prod_{\substack{1\leq k\leq m\\(k,m/2)=1}} (X^2-\zeta_{m/2}^k) \prod_{\substack{1\leq h\leq m/2\\(h,m/2)=1}} (X^2-\zeta_{m/2}^{2h})^{-1}\\ &= \Phi_{m/2}\big(X^2\big)^2/\Phi_{m/2}\big(X^2\big) = \Phi_{m/2}\big(X^2\big).\end{aligned}$$

If $4 \mid m$ then the last product of (2) is equal to

$$\prod_{\substack{1\leq k\leq m\\(k,m)=1}} (X^2-\zeta_{m/2}^k) = \prod_{\substack{1\leq k\leq m\\(k,m/2)=1}} (X^2-\zeta_{m/2}^k) = \Phi_{m/2}\big(X^2\big)^2,$$

and the proof is complete. □

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 [3] (see also [1]). We make use of the following particular case.

Lemma 3.4. *Let $(u_k(\gamma,\delta))_{k\geq 0}$ be a Lehmer sequence with $\gamma\delta = 1$. Then $u_n(\gamma,\delta)$ has a primitive divisor for every positive integer $n \notin \{1,2,3,4,5,6,10,12\}$.*

Proof. Following [3], we can write $\gamma = \zeta\big(\sqrt{a} - \sqrt{b}\big)/2$ and $\delta = \zeta\big(\sqrt{a} + \sqrt{b}\big)/2$, where a, b are integers and ζ is a fourth root of unity. In particular, $\gamma\delta = 1$ implies that $a - b = \pm 4$. Let $n \geq 3$ be an integer and suppose that $u_n(\gamma, \delta)$ has no primitive divisor. By [3, Theorem 1.4], we have that $n \leq 30$. If $7 \leq n \leq 30$ and $n \notin \{8, 10, 12\}$, then by [3, Theorem C] we have that (a, b) belongs to [3, Table 2], but none of the pairs in such table satisfies $a - b = \pm 4$. If $n \in \{3, 4, 5, 6, 8, 10, 12\}$ then by [3, Theorem 1.3] we have that (a, b) belongs to [3, Table 4] and, checking again the condition $a - b = \pm 4$, we get that $n \in \{3, 4, 5, 6, 10, 12\}$ (see Remark 3.1). □

Remark 3.1. In line $n = 5$ of [3, Table 4], one has to include also the pair $(-1, -5)$, which is $(\psi_{k-2\varepsilon}, \psi_{k-2\varepsilon} - 4\psi_k)$ for $k = 1$ and $\varepsilon = 1$ (note that $\psi_{-1} = -1$). This is lost when in [3, p. 89] it is claimed that "By (28), we have [...] $k \neq 1$ in the case (35)" but $k = 1$ (and $\varepsilon = 1$) does not contradict [3, Eq. (28)]. Similarly, in line $n = 10$ of [3, Table 4], one has to include also the pair $(-5, -1)$, which is $(\psi_{k-2\varepsilon} - 4\psi_k, \psi_{k-2\varepsilon})$ for $k = 1$ and $\varepsilon = 1$.

Remark 3.2. Lemma 3.4 cannot be improved without further information on γ, δ. Indeed, it can be checked that $u_n\Big(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\Big)$ for $n \in \{1, 2, 6, 10, 12\}$, $u_n\Big(\frac{\sqrt{-2}-\sqrt{-6}}{2}, \frac{\sqrt{-2}+\sqrt{-6}}{2}\Big)$ for $n \in \{3, 4\}$, and $u_5\Big(\frac{\sqrt{-1}-\sqrt{-5}}{2}, \frac{\sqrt{-1}+\sqrt{-5}}{2}\Big)$ have no primitive divisor.

We need the identities for the *Aurifeuillian factorizations* of the cyclotomic polynomials [19]. However, instead of using them how it is commonly done, that is, to write values of the cyclotomic polynomials as differences of two squares and thus factorize them; we use them to write values of the cyclotomic polynomials as sums of two squares (proof of Lemma 3.7 below).

A polynomial $F \in \mathbb{Z}[X, Y]$ is *symmetric*, respectively *antisymmetric*, if $F(Y, X) = F(X, Y)$, respectively $F(Y, X) = -F(X, Y)$. The *symmetry type* of F is $\mathrm{s}(F) = +1$ if F is symmetric, and $\mathrm{s}(F) = -1$ if F is antisymmetric.

Lemma 3.5. *Let k be a squarefree integer and let $n \geq 3$ be an integer. Suppose that one of the following conditions holds:*

(c1) $k \equiv 1 \pmod 4$, $k \mid n$, *and* $2k \nmid n$.

(c2) $k \not\equiv 1 \pmod 4$, $2k \mid n$, *and* $4k \nmid n$.

Then there exist homogeneous polynomials $F_{n,k}, G_{n,k} \in \mathbb{Z}[X, Y]$ such that

$$\Phi_n(X, Y) = F_{n,k}(X, Y)^2 - k(XY)^{q_n} G_{n,k}(X, Y)^2,$$

where $q_n := \prod_{p>2,\, p^v \,||\, n} p^{v-1}$. Furthermore, we have

$$\deg(F_{n,k}) = \frac{\varphi(n)}{2}, \quad \deg(G_{n,k}) = \frac{\varphi(n)}{2} - q_n,$$

while

$$\mathrm{s}(F_{n,k}) = \begin{cases} 1 & \text{if } k = 1, \text{ or } k > 1 \text{ and } 2 \mid n, \\ (-1)^{\varphi(n)/2} & \text{otherwise,} \end{cases}$$

and $\mathrm{s}(G_{n,k}) = \mathrm{sign}(k)\, \mathrm{s}(F_{n,k})$.

Proof. The claim is the homogeneous version of [19, Theorem 2.1]. □

Lemma 3.6. *Let n and k be as in Lemma 3.5, and let ζ, η be algebraic integers. If a prime number p divides both $F_{n,k}(\zeta, \eta)$ and $G_{n,k}(\zeta, \eta)$ then p divides $2n(\zeta\eta)^j$ for some integer $j \geq 0$. (Recall that we say that p divides an algebraic integer ξ if ξ/p is an algebraic integer.)*

Proof. With the notation of Lemma 3.5, we can write $n = q_n m$ for an integer $m \geq 3$ with $q_m = 1$ and such that the hypothesis of Lemma 3.5 holds with m in place of n. Moreover, by [19, Eqs. (2)] we have that $F_{n,k}(X, Y) = F_{m,k}(X^{q_n}, Y^{q_n})$ and $G_{n,k}(X, Y) = G_{m,k}(X^{q_n}, Y^{q_n})$. Therefore, without loss of generality, we can assume that $q_n = 1$.

Let $i_{n,k}$ be the order of $\mathbb{Z}[X, \sqrt{kX}]/I$, where I is the ideal generated by

$$F_{n,k}(X, 1) - G_{n,k}(X, 1)\sqrt{kX} \quad \text{and} \quad F_{n,k}(X, 1) + G_{n,k}(X, 1)\sqrt{kX} \tag{3}$$

in $\mathbb{Z}[X,\sqrt{kX}]$. Then $i_{n,k}$ is a linear combination of (3) in $\mathbb{Z}[X,\sqrt{kX}]$, and by homogeneization $i_{n,k}Y^j$ is a linear combination of

$$F_{n,k}(X)-G_{n,k}(X)\sqrt{kXY} \quad \text{and} \quad F_{n,k}(X,Y)+G_{n,k}(X,Y)\sqrt{kXY},$$

in $\mathbb{Z}[X,Y,\sqrt{kXY}]$, for some integer $j\geq 0$. Substituting $X=\zeta$ and $Y=\eta$, we get that if p divides both $F_{n,k}(\zeta,\eta)$ and $G_{n,k}(\zeta,\eta)$ then it divides $i_{n,k}\eta^j$, and so it divides $i_{n,k}(\zeta\eta)^j$. From [19, Lemma 2.6] (which requires $q_n=1$) we have that $i_{n,k}$ divides $(8n)^{\varphi(n)}$, and thus the claim follows. □

Now we can prove a result on primitive divisors of Lehmer sequences.

Lemma 3.7. *Let $(u_k(\gamma,\delta))_{k\geq 0}$ be a Lehmer sequence and write $(\gamma^2-\delta^2)^2=D_0D_1^2$ where $D_0,D_1\in\mathbb{Z}$ and D_0 is squarefree. Suppose that $D_0\geq 5$ and $D_0\equiv 1 \pmod 4$. Then, for every positive integer ℓ such that $4D_0\mid\ell$, we have that each odd primitive divisor p of $u_\ell(\gamma,\delta)$ satisfies $p\equiv 1 \pmod 4$.*

Proof. Since $4D_0\mid\ell$, we can write $\ell=2^vn$ for some positive integers v and n with $2D_0\mid n$ and $4D_0\nmid n$. Put $k:=-D_0$. By the hypotheses on D_0, we have that k is negative and squarefree, $n\geq 3$, and (c2) holds. Moreover, since D_0 is squarefree and $D_0\equiv 1 \pmod 4$, it follows that $4\mid\varphi(D_0)$, and so $4\mid\varphi(n)$. Therefore, by Lemma 3.5, we get that

$$\Phi_n(X,Y)=F_{n,k}(X,Y)^2+D_0(XY)^{q_n}G_{n,k}(X,Y)^2, \tag{4}$$

for some homogeneous polynomials $F_{n,k},G_{n,k}\in\mathbb{Z}[X,Y]$, with $F_{n,k}$ symmetric and $G_{n,k}$ antisymmetric. Since $G_{n,k}$ is antisymmetric and homogeneous, we have that $G_{n,k}(X,Y)=(X-Y)H_{n,k}(X,Y)$ for some symmetric homogeneous polynomial $H_{n,k}\in\mathbb{Z}[X,Y]$. Now $F_{n,k}\big(X^{2^v},Y^{2^v}\big)$ and $H_{n,k}\big(X^{2^v},Y^{2^v}\big)$ are both symmetric homogeneous polynomials of even degree, and thus they are polynomials in XY and $(X+Y)^2$ with integer coefficients. Then, recalling that $\gamma\delta$ and $(\gamma+\delta)^2$ are integers, it follows that $F_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)$ and $H_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)$ are integers. Since $2\mid n$, by (4) we get that

$$\begin{aligned}\Phi_\ell(\gamma,\delta)&=\Phi_{2^vn}(\gamma,\delta)=\Phi_n\big(\gamma^{2^v},\delta^{2^v}\big)=F_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)^2+D_0(\gamma\delta)^{2^vq_n}G_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)^2\\&=F_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)^2+D_0(\gamma\delta)^{2^vq_n}\big(\gamma^{2^v}-\delta^{2^v}\big)^2H_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)^2\\&=F_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)^2+D_0(\gamma\delta)^{2^vq_n}(\gamma^2-\delta^2)^2u_{2^v}(\gamma,\delta)^2H_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)^2\\&=A^2+B^2,\end{aligned} \tag{5}$$

where $A:=F_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)$ and $B:=D_0D_1(\gamma\delta)^{2^{v-1}q_n}u_{2^v}(\gamma,\delta)H_{n,k}\big(\gamma^{2^v},\delta^{2^v}\big)$ are both integers. Let p be an odd primitive divisor of $u_\ell(\gamma,\delta)$. Hence, also by Lemma 3.2(p1) and (p6), we have that $p\nmid\gamma\delta(\gamma^2-\delta^2)^2n$ and $p\mid\Phi_\ell(\gamma,\delta)$. Thus, from (5) and Lemma 3.6, it follows that $p\mid A^2+B^2$ but $p\nmid A$ and $p\nmid B$. Consequently, we have that $p\equiv 1 \pmod 4$. □

4. Proof of Theorem 1.2

Let us begin by proving the equivalence of (i) and (ii). Let $D:=(\alpha-\beta)^2$ be the discriminant of f. First, assume that $\alpha\beta=-1$. Note that $\gamma\delta=1$ and $(\gamma+\delta)^2=D$ are nonzero coprime integers and $\gamma/\delta=-\alpha/\beta$ is not a root of unity, so that $(u_k(\gamma,\delta))_{k\geq 0}$ is a Lehmer sequence. Put $R_m^{(\varepsilon)}:=\mathrm{Res}(f(\varepsilon X),\Phi_m(X))$ for $\varepsilon\in\{-1,+1\}$. The roots of $f(-X)$ are $-\alpha$ and $-\beta$, while $\gamma/\delta=\alpha^2$ and $\delta/\gamma=\beta^2$. Hence, from Lemma 3.3, it follows that

$$\begin{aligned}R_m^+R_m^-&=\Phi_m(\alpha)\Phi_m(\beta)\Phi_m(-\alpha)\Phi_m(-\beta)=\Phi_m(\alpha)\Phi_m(-\alpha)\Phi_m(\beta)\Phi_m(-\beta)\\&=\big(\Phi_n\big(\alpha^2\big)\Phi_n\big(\beta^2\big)\big)^e=\big(\Phi_n(\gamma/\delta)\Phi_n(\delta/\gamma)\big)^e=\Big(\Phi_n(\gamma,\delta)\delta^{-\varphi(n)}\Phi_n(\delta,\gamma)\gamma^{-\varphi(n)}\Big)^e\\&=\big(\Phi_n(\gamma,\delta)\Phi_n(\delta,\gamma)\big)^e=\pm\Phi_n(\gamma,\delta)^{2e},\end{aligned} \tag{6}$$

where $e:=1$ if $4\nmid m$, and $e:=2$ if $4\mid m$.

Suppose that (i) holds. By Lemma 3.1, we have that $p \mid R_m^+$ and $p \equiv 1 \pmod m$. Hence, from (6) and the fact that $n \mid m$, we get that $p \mid \Phi_n(\gamma,\delta)$ and $p \equiv 1 \pmod n$. Therefore, Lemma 3.2(p6) implies that p is a primitive divisor of $u_n(\gamma,\delta)$, and (ii) follows.

Now suppose that (ii) holds. Thus, from Lemma 3.2(p6), it follows that $p \mid \Phi_n(\gamma,\delta)$. Consequently, by (6), we get that either $p \mid R_m^+$ or $p \mid R_m^-$. In the first case, (i) follows immediately from Lemma 3.1. In the second case, from Lemma 3.1 it follows that there exists $b \in \mathbb{Z}$ such that $p \mid f(-b)$ and $\mathrm{ord}_p(b) = m$. Since f is quadratic and has a root modulo p, we have that f splits completely modulo p. Let $a \in \mathbb{Z}$ be such that $f(X) \equiv (X-a)(X+b) \pmod p$. Recalling that $\alpha\beta = -1$, we get that $ab \equiv 1 \pmod p$, and consequently $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = m$. Thus (i) follows.

Now assume that $\alpha\beta = +1$. Note that $\gamma\delta = 1$ and $(\gamma+\delta)^2 = \alpha+\beta+2$ are nonzero coprime integers and $\gamma/\delta = \alpha$ is not a root of unity, so that $(u_k(\gamma,\delta))_{k\ge 0}$ is a Lehmer sequence. Since $\gamma/\delta = \alpha$ and $\delta/\gamma = \beta$, we have that

$$\begin{aligned}(7)\qquad \mathrm{Res}(f,\Phi_m) &= \Phi_m(\alpha)\Phi_m(\beta) = \Phi_m(\gamma/\delta)\Phi_m(\delta/\gamma) = \Phi_m(\gamma,\delta)\delta^{-\varphi(m)}\Phi_m(\delta,\gamma)\gamma^{-\varphi(m)}\\ &= \Phi_m(\gamma,\delta)\Phi_m(\delta,\gamma) = \pm\Phi_m(\gamma,\delta)^2 = \pm\Phi_n(\gamma,\delta)^2.\end{aligned}$$

Suppose that (i) holds. From Lemma 3.1 and (7), it follows that $p \mid \Phi_n(\gamma,\delta)$ and $p \equiv 1 \pmod m$. Hence, Lemma 3.2(p6) yields that (ii) holds.

Now suppose that (ii) holds. Then Lemma 3.2(p6) and (7) give that $p \mid \mathrm{Res}(f,\Phi_m)$. Consequently, by Lemma 3.1, we get that (i) holds.

The proof of the equivalence of (i) and (ii) is complete. Let us prove that each of (iii), (iv), and (v) implies (ii) (and consequently also (i)).

Suppose that (iii) holds. Since $4 \nmid m$, $m \notin \{3,6\}$, and $u_1(\gamma,\delta) = u_2(\gamma,\delta) = 1$, we have that $n \ge 5$ and $2 \nmid n$. Hence, by Lemma 3.2(p7) it follows that $p \equiv \left(\frac{\gamma\delta(\gamma-\delta)^2}{p}\right) \equiv 1 \pmod{2n}$, since $\gamma\delta = 1$ and $\gamma - \delta = \alpha+\beta$ is an integer. Then from $m \mid 2n$ we get that $p \equiv 1 \pmod m$, and (ii) follows.

Suppose that (iv) holds. We have that $4 \mid n$, $\gamma\delta = 1$, $\gamma - \delta = \alpha+\beta \in \mathbb{Z}$, p is a primitive divisor of $u_n(\gamma,\delta)$, and $p \equiv 1 \pmod 4$. From Lemma 3.2(p8) it follows that $p \equiv 1 \pmod{2n}$, i.e., $p \equiv 1 \pmod m$, and (ii) follows.

Suppose that (v) holds. Then by Lemma 3.2(p6), we have that either $p \equiv 1 \pmod m$ or $p \equiv -1 \pmod m$. Since $4 \mid m$ and $p \equiv 1 \pmod 4$, the second case is impossible. Therefore, $p \equiv 1 \pmod m$ and (ii) follows.

The proof is complete.

5. Proof of Theorem 1.3

Let $f, \alpha, \beta, \delta, \gamma$ be as in Theorem 1.2 with $\alpha\beta = -1$, let $g \in \mathbb{Z}[X]$ be a monic polynomial with $f \mid g$, and let $m \ge 7$ be an integer with $m \ne 10$ and $4 \nmid m$. Since $\gamma\delta = 1$ and $m/(m,2) \notin \{1,2,3,4,5,6,10,12\}$, from Lemma 3.4 we get that $u_{m/(m,2)}(\gamma,\delta)$ has a primitive divisor p. Hence, from the implication (iii)⇒(i) of Theorem 1.2 and from Lemma 1.1, it follows that $m \in \mathfrak{M}(g)$. The proof is complete.

6. Proof of Theorem 1.4

Let $f, \alpha, \beta, \delta, \gamma$ be as in Theorem 1.2 and let $g \in \mathbb{Z}[X]$ be a monic polynomial with $f \mid g$. Also, write $(\alpha-\beta)^2 = D_0 D_1^2$, where $D_0, D_1 \in \mathbb{Z}$ and D_0 is squarefree, and suppose that $D_0 \ge 5$ and $D_0 \equiv 1 \pmod 4$.

First, assume that $\alpha\beta = -1$. Hence, we have that $(\gamma^2-\delta^2)^2 = (\alpha^2-\beta^2)^2 = D_0(D_1(\alpha+\beta))^2$, where $D_1(\alpha+\beta)$ is an integer. Let m be a positive integer with $8D_0 \mid m$. Since $m/2 \ge 20$, from Lemma 3.4 and Lemma 3.2(p2) and (p3), it follows that $u_{m/2}(\gamma,\delta)$ has an odd primitive divisor p. Furthermore, Lemma 3.7 yields that $p \equiv 1 \pmod 4$. Hence, (iv) holds and, by Theorem 1.2 and Lemma 1.1, we get that $m \in \mathfrak{M}(g)$.

Now assume that $\alpha\beta = +1$. Hence, we have that $(\gamma^2-\delta^2)^2 = (\alpha-\beta)^2 = D_0 D_1^2$. Let m be a positive integer with $4D_0 \mid m$. Since $m \ge 20$, from Lemma 3.4 and Lemma 3.2(p2) and (p3),

it follows that $u_m(\gamma,\delta)$ has an odd primitive divisor p. Furthermore, Lemma 3.7 yields that $p \equiv 1 \pmod 4$. Hence, (v) holds and, by Theorem 1.2 and Lemma 1.1, we get that $m \in \mathfrak{M}(g)$.

The proof is complete.

7. Further remarks

For the sake of completeness, we also include the case in which g has a linear factor.

Proposition 7.1. *Let $g \in \mathbb{Z}[X]$ be a nonconstant monic polynomial with an integer root $a \notin \{-1,0,+1\}$. Then every positive integer m belongs to $\mathfrak{M}(g)$, with the possible exception of $m = 2$ if $a = \pm 2^v - 1$ for some positive integer v, $m = 3$ if $a = -2$, and $m = 6$ if $a = 2$.*

Proof. It is clear that $1 \in \mathfrak{M}(g)$. By Zsigmondy's theorem [14, p. 1], for every integer $a \notin \{-1,0,+1\}$ and for every positive integer m with $(a,m) \notin \{(\pm 2^v - 1, 2) : v \geq 1\} \cup \{(-2,3),(2,6)\}$, there exists a prime number p such that $\mathrm{ord}_p(a) = m$. Hence, by Lemma 1.1 with $f(X) = X - a$, we get that $m \in \mathfrak{M}(g)$. □

8. Acknowledgements

The authors thanks the anonymous referee for carefully reading the paper.

References

1. M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Théor. Nombres Bordeaux **18** (2006), no. 2, 299–313.
2. B. Avila and Y. Chen, *On moduli for which the Lucas numbers contain a complete residue system*, Fibonacci Quart. **51** (2013), no. 2, 151–152.
3. Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122, With an appendix by M. Mignotte.
4. R. T. Bumby, *A distribution property for linear recurrence of the second order*, Proc. Amer. Math. Soc. **50** (1975), 101–106.
5. S. A. Burr, *On moduli for which the Fibonacci sequence contains a complete system of residues*, Fibonacci Quart. **9** (1971), no. 5, 497–504, 526.
6. A. Dubickas and A. Novikas, *Linear recurrence sequences without zeros*, Czechoslovak Math. J. **64(139)** (2014), no. 3, 857–865.
7. A. Dubickas and A. Novikas, *Recurrence with prescribed number of residues*, J. Number Theory **215** (2020), 120–137.
8. A. Flatters, *Primitive divisors of some Lehmer-Pierce sequences*, J. Number Theory **129** (2009), no. 1, 209–219.
9. T. Herendi, *Uniform distribution of linear recurring sequences modulo prime powers*, Finite Fields Appl. **10** (2004), no. 1, 1–23.
10. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448.
11. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479.
12. 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, 139–143.
13. T. A. Pierce, *The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$*, Ann. of Math. (2) **18** (1916), no. 2, 53–64.
14. A. Schinzel, *On primitive prime factors of $a^n - b^n$*, Proc. Cambridge Philos. Soc. **58** (1962), 555–562.
15. A. Schinzel, *Special Lucas sequences, including the Fibonacci sequence, modulo a prime*, A tribute to Paul Erdős, Cambridge Univ. Press, Cambridge, 1990, pp. 349–357.
16. L. Somer, *Primes having an incomplete system of residues for a class of second-order recurrences*, Applications of Fibonacci numbers (San Jose, CA, 1986), Kluwer Acad. Publ., Dordrecht, 1988, pp. 113–141.
17. L. Somer, *Distribution of residues of certain second-order linear recurrences modulo p. III*, Applications of Fibonacci numbers, Vol. 6 (Pullman, WA, 1994), Kluwer Acad. Publ., Dordrecht, 1996, pp. 451–471.
18. L. Somer and M. Křížek, *On moduli for which certain second-order linear recurrences contain a complete system of residues modulo m*, Fibonacci Quart. **55** (2017), no. 3, 209–228.
19. P. Stevenhagen, *On Aurifeuillian factorizations*, Nederl. Akad. Wetensch. Indag. Math. **49** (1987), no. 4, 451–468.
20. C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), no. 3, 425–447.

Politecnico di Torino, Department of Mathematical Sciences
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
Email address: carlo.sanna.dev@gmail.com