NON-MONOGENIC FACTORS OF THE FIBONACCI AND LUCAS POLYNOMIALS: THE ORDER $\mathbb{Z}[\zeta_n - \zeta_n^{-1}]$ FOR ODD n

KOREA SUPERINTELLIGENCE LABS

Abstract. Let F_n and L_n be the Fibonacci and Lucas polynomials, defined by $F_0 = 0$, $F_1 = 1$, $L_0 = 2$, $L_1 = x$ and the common recurrence $P_{k+2} = xP_{k+1} + P_k$. A recent preprint of Chen, Guo and Hong proves that every irreducible factor of F_n is monogenic when n is odd and that every irreducible factor of L_n is monogenic when n is even, observes that neither parity hypothesis can be dropped, and asks, as its Problems 1–3, for necessary and sufficient conditions in the two remaining parities. We settle the negative half uniformly in n. For every odd $n > 1$, the element $\beta = \zeta_n - \zeta_n^{-1}$ generates the *whole* cyclotomic field $\mathbb{Q}(\zeta_n)$ and its minimal polynomial divides L_n, yet $\mathbb{Z}[\beta]$ is a proper subring of the ring of integers of $\mathbb{Q}(\zeta_n)$: one has $2\zeta_n \in \mathbb{Z}[\beta]$ but $\zeta_n \notin \mathbb{Z}[\beta]$. Consequently L_n has a non-monogenic irreducible factor for every odd $n > 1$, and F_m has one for every even m that is not a power of 2; in particular, for odd m every irreducible factor of L_m is monogenic if and only if $m = 1$, which answers the second of the three problems outright. The proof uses no discriminant, no Dedekind criterion and no Newton polygon. The Binet identity $L_k(u - v) = u^k + (-1)^k v^k$, valid whenever $uv = 1$, puts β on L_n; the conjugation $\zeta \mapsto \zeta^{-1}$ sends β to $-\beta$, so $\zeta_n \in \mathbb{Z}[\beta]$ would make β twice an algebraic integer, and a geometric sum then makes n twice an algebraic integer as well. Individual cases were known — $n = 3$ classically, and the degrees corresponding to $n = 5, 7, 9, 11, 15, 23$ in work of Jones, Harrington–Jones and König — but we have not found the statement uniform in n, nor this mechanism, in the literature. Combining the theorem with the two positive propositions of the source classifies the monogenic factors of F_n and L_n completely and answers all three problems; that combination, the exact index $2^{\varphi(n)/2}$ and a confirming computation are recorded as remarks, outside the formal development and labelled as such. Every lemma, proposition, theorem and corollary of Sections 2–5 is machine-checked in Lean 4 against Mathlib.

1. Introduction

The objects. The *Fibonacci polynomials* and *Lucas polynomials* are the two solutions of one recurrence with two initial conditions:

$$F_0 = 0, \quad F_1 = 1, \qquad L_0 = 2, \quad L_1 = x, \qquad P_{k+2} = x\,P_{k+1} + P_k.$$

The Lucas polynomials are the coefficient triangle A114525 of the OEIS [12]; the Fibonacci polynomials are the row polynomials of the *unsigned* version of A049310, whose own entry — the signed triangle of the Chebyshev polynomials $S(n, x) = U(n, x/2)$ — records that identification. Both families are monic, of degrees $n - 1$ and n respectively, and neither is irreducible in general, so the arithmetic questions one asks about them are questions about their irreducible factors.

Following Dedekind's classical terminology, a number field K is *monogenic* when $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$, that is, when $\mathcal{O}_K$ has a power integral basis; and a non-zero irreducible $f \in \mathbb{Z}[x]$ is *monogenic* when some root α of f satisfies $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{Q}(\alpha)}$. (The second notion is strictly stronger than the first applied to $\mathbb{Q}(\alpha)$: $K = \mathbb{Q}(\sqrt{5})$ is monogenic while $x^2 - 5$ is not.) The subject has a long history, from Dedekind, Hensel and Hasse to the present; Gaál's survey [2] is the current reference.

The source and its problems. A recent preprint [1] of Chen, Guo and Hong determines the monogenity of the irreducible factors of F_n and of L_n for one parity each. We quote its two main theorems verbatim.

Theorem 1.1 ([1, Theorem 1.1])**.** *For any odd positive integer n, all irreducible factors of $F_n(x)$ are monogenic.*

Theorem 1.2 ([1, Theorem 1.2])**.** *For any even positive integer n, all irreducible factors of $L_n(x)$ are monogenic.*

Its Remark 1.3 shows that neither parity condition can simply be dropped: the odd-indexed Lucas polynomial L_5 contains the irreducible factor $x^4 + 5x^2 + 5$, which is not monogenic, and by $F_{2k} = F_k L_k$ the same factor occurs in F_{10}. The concluding section stops there. It records that "numerical experiments for $n \leq 100$ indicate that the non-monogenic factors in remaining cases do not have a naive density, suggesting a deeper obstruction that warrants further study", and poses three problems, which we again quote verbatim.

Problem 1 ([1, Problem 1])**.** Determine a necessary and sufficient condition on an even integer n such that every irreducible factor of the Fibonacci polynomial $F_n(x)$ is monogenic.

Problem 2 ([1, Problem 2])**.** Determine a necessary and sufficient condition on an odd integer n such that every irreducible factor of the Lucas polynomial $L_n(x)$ is monogenic.

Problem 3 ([1, Problem 3])**.** More generally, given the families $F_n(x)$ and $L_n(x)$ for $n \geq 1$, is there an algorithmic criterion to decide exactly when all of their irreducible factors are monogenic? In particular, can such a criterion be completely described solely in terms of the prime factorization and the parity of n?

What is settled here. Every problem above has a negative half — exhibit a non-monogenic factor — and a positive half. This paper proves the negative half in one stroke, uniformly in n, and identifies the single order responsible for it.

Let $n > 1$ be odd, let ζ be a primitive n-th root of unity, and put

$$\beta \;=\; \zeta - \zeta^{-1}.$$

Theorem 1.3 (Theorem 4.1 below)**.** *For every odd $n > 1$ one has $\zeta \notin \mathbb{Z}[\beta]$, while $2\zeta \in \mathbb{Z}[\beta]$ and $\mathbb{Q}(\beta) = \mathbb{Q}(\zeta)$. Hence $\mathbb{Z}[\beta]$ is a proper subring of the ring of integers of $\mathbb{Q}(\zeta)$, and the minimal polynomial of β is a non-monogenic irreducible factor of $L_n(x)$.*

The three assertions pull in different directions and that is the point. The middle one says the order $\mathbb{Z}[\beta]$ is large: it contains 2ζ, so ζ misses $\mathbb{Z}[\beta]$ by a single halving, and the index is in fact exactly $2^{\varphi(n)/2}$ (Remark 6.3). The third says the failure is not a failure of degree: β generates the full cyclotomic field, which is itself monogenic. The first says that nevertheless the obvious power basis of β is not an integral basis, and that this happens for every odd $n > 1$ without exception.

Because an even m that is not a power of 2 has an odd divisor $n > 1$, and because β is then a root of F_m as well, the same order answers the negative half of Problem 1.

Theorem 1.4 (Theorem 4.3 below)**.** *For every even m that is not a power of 2, the Fibonacci polynomial $F_m(x)$ has an irreducible factor over $\mathbb{Q}$ that is not monogenic.*

Problem 2 is settled outright, since its positive side is the trivial case $L_1 = x$: for odd m, every irreducible factor of L_m is monogenic if and only if $m = 1$ (Corollary 4.2). Problems 1 and 3 need in addition the two positive propositions of [1], which we cite rather than reprove; the resulting complete classification, and the exact index $2^{\varphi(n)/2}$, are collected in Section 6 as remarks lying outside the formal development.

Individual cases already in the literature. The statement of Theorem 1.3 for one fixed n is a finite check, and several values of n have been recorded, always as isolated computations. For $n = 3$ the minimal polynomial of β is $x^2 + 3$ and $\mathbb{Z}[\beta] = \mathbb{Z}[\sqrt{-3}]$ is the textbook non-maximal order inside $\mathbb{Z}[\zeta_3]$. For $n = 5$ it is $x^4 + 5x^2 + 5$: this is the example of [1, Remark 1.3], and Jones [5] writes that "it is straightforward to verify that $x^4 + 5x^2 + 5$ is not monogenic" (the condition he checks is item (4) of

the Jakhar–Khanduja–Sangwan index criterion for quartic trinomials, quoted as Theorem 2.2 of his e-print). The discriminant data $\Delta(f) = 2^4 \cdot 5^3$ against $\Delta(K) = 5^3$ appear in [6, Table 1] — we cite those two entries only, the same row of that table also recording K itself as non-monogenic, whereas here $K = \mathbb{Q}(\zeta_5)$, which is. For $n = 7$ and $n = 15$, Harrington and Jones [3] state, as motivating examples and without proof, that "the irreducible factor $x^6+7x^4+14x^2+7$ of $F_{14}(x)$ is cyclic but not monogenic" and that "the irreducible factor $x^8+7x^6+14x^4+8x^2+1$ of $L_{15}(x)$ is neither monogenic nor cyclic". König's Theorem 1.1 [4] classifies the monogenic $f(x) = x^6 + ax^4 + bx^2 + c$ with cyclic Galois group by six triples (a, b, c), and his Lemma 1.2 lists the monogenic even polynomials of degree $2q$ with Galois group C_{2q} for the primes $5 \le q \le 19$; the minimal polynomials of $\zeta_7 - \zeta_7^{-1}$ and $\zeta_9 - \zeta_9^{-1}$ — the triples $(7, 14, 7)$ and $(6, 9, 3)$ — are absent from the first list, and those of $\zeta_{11} - \zeta_{11}^{-1}$ and $\zeta_{23} - \zeta_{23}^{-1}$, of degrees 10 and 22, from the second, so those four cases follow from his results.

What we have not found is the statement uniform in n, or an explanation of why it should hold. König ends [4, §3], the section that proves those results, with the sentence "Whether there was any reason to expect the analogous result a priori for $\deg(g) = 3$, I do not know." The reason offered here is Theorem 1.3: for odd n the field $\mathbb{Q}(\zeta_n - \zeta_n^{-1})$ is not a proper subfield at all but the whole cyclotomic field, so the field-level results of the Hasse-problem literature — [7, 8] and their successors — are describing a different object; what fails is a property of one non-maximal *order*, and it fails uniformly. Section 7 records the searches behind that negative claim.

Method. The proof of Theorem 1.3 occupies four lines and uses only that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. The Binet identity in the shape

$$L_k(u - v) = u^k + (-1)^k v^k \qquad (uv = 1)$$

puts β on L_n for odd n, and at $k = n + 1$ gives $L_{n+1}(\beta) = \zeta + \zeta^{-1}$, hence $2\zeta = \beta + L_{n+1}(\beta) \in \mathbb{Z}[\beta]$. For the negative statement, the conjugation $\sigma\colon \zeta \mapsto \zeta^{-1}$ sends β to $-\beta$, so for any $P \in \mathbb{Z}[x]$ the difference $P(\beta) - \sigma(P(\beta)) = P(\beta) - P(-\beta)$ is twice an algebraic integer. If $\zeta = P(\beta)$ this says $\beta = 2\gamma$; multiplying by ζ turns it into $\zeta^2 - 1 = 2\delta$, and summing the resulting factorisations of $\zeta^{2k} - 1$ over $k < n$ against $\sum_{k<n} \zeta^{2k} = 0$ produces $n = 2\varepsilon$ with ε an algebraic integer — impossible for odd n.

Organisation. Section 2 fixes notation and proves the two elementary lemmas. Section 3 studies the order $\mathbb{Z}[\beta]$ from above. Section 4 contains the main theorem and its two consequences, Section 5 the concrete anchors and the controls that keep the hypotheses honest. Section 6 assembles the answers to Problems 1–3 from our theorem and the source's propositions, and is explicitly outside the formal development; so is the confirming computation reported there. Section 7 describes the verification.

2. Preliminaries

Throughout, K is a field of characteristic zero, $n \ge 1$, and $\zeta \in K$ is a primitive n-th root of unity; from Section 3 on, K is an n-th cyclotomic extension of $\mathbb{Q}$, so that $K = \mathbb{Q}(\zeta)$ and $\mathcal{O}_K = \mathbb{Z}[\zeta]$. We write φ for Euler's function and τ for the number-of-divisors function. We regard F_k, L_k as elements of $\mathbb{Z}[x]$ and evaluate them in K.

Definition 2.1. Let K be a number field and $\theta \in K$. We call θ a *monogenic generator* of K when $\mathbb{Q}(\theta) = K$ and $\mathbb{Z}[\theta] = \mathcal{O}_K$. A monic irreducible $f \in \mathbb{Z}[x]$ is monogenic exactly when one — equivalently, by conjugation, each — of its roots is a monogenic generator of the field it generates.

The two lemmas below are the whole toolkit. The first is the Binet formula for these polynomials, specialised to a pair of mutually inverse elements; this specialisation is what makes $\zeta - \zeta^{-1}$ a root of L_n. Compare [1, Lemmas 2.1, 2.2], where the same formulas appear in their analytic form over $\mathbb{C}$.

Lemma 2.2. *Let R be a commutative ring and let $u, v \in R$ satisfy $uv = 1$. Then for every $k \ge 0$,*

$$L_k(u - v) = u^k + (-1)^k v^k, \qquad F_k(u - v) \cdot (u + v) = u^k - (-1)^k v^k.$$

Proof. Two-step induction on k. Both identities hold at $k=0$ and $k=1$ by inspection ($L_0=2=1+1$, $L_1(u-v)=u-v$; $F_0=0$, $F_1(u-v)(u+v)=u+v$). For the step, apply $P_{k+2}=xP_{k+1}+P_k$ at $x=u-v$ and use $uv=1$ to rewrite $(u-v)\big(u^{k+1}+(-1)^{k+1}v^{k+1}\big)+u^k+(-1)^kv^k$ as $u^{k+2}+(-1)^{k+2}v^{k+2}$, and similarly for F. □

Lemma 2.3. *For every $P\in\mathbb{Z}[x]$ there is a $Q\in\mathbb{Z}[x]$ with $P(x)-P(-x)=2\,Q(x)$.*

Proof. Both sides are additive in P, so it suffices to treat a monomial ax^k. If k is even the left-hand side vanishes and $Q=0$ works; if k is odd it equals $2ax^k$ and $Q=ax^k$ works. □

We shall also use the factorisation of F_n recorded in [1, §5], which we quote because it converts every statement about factors of F_n or L_n into a statement about a single polynomial per divisor. The zeros of F_n are the $n-1$ distinct numbers $2i\cos(k\pi/n)$, $1\le k\le n-1$ [1, Lemma 2.1]; grouping them by $d=n/\gcd(k,n)$ and writing $\Omega_d\in\mathbb{Z}[x]$ for the minimal polynomial of $i(\zeta_{2d}+\zeta_{2d}^{-1})=2i\cos(\pi/d)$, which has degree $\varphi(d)$, one gets

$$F_n(x)=\prod_{d\mid n,\ d>1}\Omega_d(x),\qquad \sum_{d\mid n,\ d>1}\varphi(d)=n-1, \tag{1}$$

so that the irreducible factors of F_n over $\mathbb{Q}$ are exactly the Ω_d with $d\mid n$, $d>1$. ([1, §5] carries this out under the standing hypothesis that n is odd, but the construction uses only the zero set of F_n, so (1) holds for every $n\ge 1$.) Since $F_{2m}=F_mL_m$, the irreducible factors of L_m are the Ω_d with $d\mid 2m$ and $d\nmid m$. Nothing in Sections 3–5 uses (1); it enters only in Section 6.

Remark 2.4. For odd g, the polynomial Ω_{2g} is the minimal polynomial of $\zeta_g-\zeta_g^{-1}$. Indeed $\gcd(4,g)=1$ allows one to write $\zeta_{4g}=\pm i\,\zeta_g^{s}$ for a suitable s coprime to g, and then $i(\zeta_{4g}+\zeta_{4g}^{-1})=\mp(\zeta_g^{s}-\zeta_g^{-s})$, a conjugate of $\zeta_g-\zeta_g^{-1}$; the degrees agree, both being $\varphi(2g)=\varphi(g)$. So the order studied below is exactly the one attached to the divisors $d\equiv 2 \pmod 4$, $d>2$, of (1).

Remark 2.5 (on the symbol Ω_d). The source writes Ω_d for two things. In its §5 (the proof of Theorem 1.1) Ω_d is the minimal polynomial of $i(\zeta_{2d}+\zeta_{2d}^{-1})$, of degree $\varphi(d)$; in its §6 (the proof of Theorem 1.2) it is the minimal polynomial of $\zeta_{2d}-\zeta_{2d}^{-1}$, of degree $\varphi(2d)/2$, and there $d=2n/g$ with n even and g odd, so that $4\mid d$ always. We use the §5 convention throughout. The two agree wherever both are defined: for $d=4k$ one has $\zeta_{2d}-\zeta_{2d}^{-1}=2i\sin(\pi/d)=2i\cos\big((2k-1)\pi/d\big)$ with $\gcd(2k-1,2d)=1$, so the two generators are conjugate, and $\varphi(2d)/2=\varphi(d)$ because d is even.

3. The order $\mathbb{Z}[\zeta-\zeta^{-1}]$ from above

From here on K is an n-th cyclotomic extension of $\mathbb{Q}$ with primitive root ζ, and $\beta=\zeta-\zeta^{-1}$.

Proposition 3.1. *Let n be odd. Then $L_n(\beta)=0$. If moreover $n>1$ and m is even with $n\mid m$, then $F_m(\beta)=0$. In both cases the minimal polynomial of β over $\mathbb{Q}$ is irreducible and divides the polynomial in question.*

Proof. Apply Lemma 2.2 with $u=\zeta$, $v=\zeta^{-1}$, so that $u-v=\beta$ and $uv=1$. At $k=n$ we get $L_n(\beta)=\zeta^n+(-1)^n\zeta^{-n}=1-1=0$, using $\zeta^n=1$ and n odd. At $k=m$ even and divisible by n we get $F_m(\beta)(\zeta+\zeta^{-1})=\zeta^m-\zeta^{-m}=0$; and $\zeta+\zeta^{-1}\neq 0$, for otherwise $\zeta^2=-1$, forcing $n\mid 4$ and hence, n being odd and >1, a contradiction. So $F_m(\beta)=0$. Finally β is integral over $\mathbb{Z}$, being a difference of roots of unity, so it has a minimal polynomial over $\mathbb{Q}$, which is irreducible and divides every rational polynomial vanishing at β. □

Proposition 3.2. *Let n be odd. Then $L_{n+1}(\beta)=\zeta+\zeta^{-1}$; consequently*

$$2\zeta=\beta+L_{n+1}(\beta)\in\mathbb{Z}[\beta],\qquad \textit{and}\qquad \mathbb{Q}(\beta)=K.$$

Proof. Lemma 2.2 at $k=n+1$, which is even, gives $L_{n+1}(\beta)=\zeta^{n+1}+\zeta^{-(n+1)}=\zeta+\zeta^{-1}$. Adding β gives 2ζ, and L_{n+1} has integer coefficients, so $2\zeta\in\mathbb{Z}[\beta]$. Dividing by 2 inside the $\mathbb{Q}$-algebra generated by β gives $\zeta\in\mathbb{Q}(\beta)$, and $\mathbb{Q}(\zeta)=K$. □

The generation statement is [1, Lemma 3.1] in the case $4 \nmid n$, where it is obtained by computing the subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ fixing $\zeta_n - \zeta_n^{-1}$. The explicit halving $2\zeta = \beta + L_{n+1}(\beta)$ is what makes the proof above two lines long, and it is the sharp form of the failure proved in the next section.

4. The main theorem

Theorem 4.1. *Let $n > 1$ be odd, let K be an n-th cyclotomic extension of $\mathbb{Q}$ with primitive root ζ, and let $\beta = \zeta - \zeta^{-1}$. Then*

$$\zeta \notin \mathbb{Z}[\beta].$$

Consequently $\mathbb{Q}(\beta) = K$ but $\mathbb{Z}[\beta] \neq \mathcal{O}_K$: the element β generates K and is not a monogenic generator of it, and the minimal polynomial of β is a non-monogenic irreducible factor of $L_n(x)$.

Proof. Suppose $\zeta = P(\beta)$ for some $P \in \mathbb{Z}[x]$.

Step 1: the conjugation. Since ζ^{-1} is another root of the minimal polynomial of ζ over $\mathbb{Q}$, there is a $\mathbb{Q}$-algebra homomorphism $\sigma\colon K \to K$ with $\sigma(\zeta) = \zeta^{-1}$. Then $\sigma(\beta) = \zeta^{-1} - \zeta = -\beta$. Applying σ to $\zeta = P(\beta)$ and using that σ fixes the coefficients of P gives $\zeta^{-1} = P(-\beta)$. Subtracting,

$$\beta = \zeta - \zeta^{-1} = P(\beta) - P(-\beta).$$

Step 2: β is twice an algebraic integer. By Lemma 2.3, $P(x) - P(-x) = 2Q(x)$ with $Q \in \mathbb{Z}[x]$, so $\beta = 2\gamma$ with $\gamma = Q(\beta)$. As β is integral over $\mathbb{Z}$, so is γ.

Step 3: transport to ζ^2. Multiplying by ζ and using $\zeta\beta = \zeta^2 - 1$ gives $\zeta^2 - 1 = 2\delta$ with $\delta = \zeta\gamma$ again integral over $\mathbb{Z}$. Put $\eta = \zeta^2$. Since n is odd, 2 is invertible modulo n, so η is again a primitive n-th root of unity; in particular $\eta \neq 1$ and $\sum_{k=0}^{n-1} \eta^k = 0$.

Step 4: summing. For each $k \geq 0$,

$$\eta^k - 1 = \Big(\sum_{i=0}^{k-1} \eta^i\Big)(\eta - 1) = 2\,\delta \sum_{i=0}^{k-1} \eta^i.$$

Summing over $0 \leq k \leq n-1$ and using $\sum_{k=0}^{n-1} \eta^k = 0$ on the left gives

$$-n = \sum_{k=0}^{n-1} \big(\eta^k - 1\big) = 2\,\delta S, \qquad S = \sum_{k=0}^{n-1} \sum_{i=0}^{k-1} \eta^i,$$

and S, being a sum of powers of η, is integral over $\mathbb{Z}$. Hence $n = 2\varepsilon$ with $\varepsilon = -\delta S$ integral over $\mathbb{Z}$. But $\varepsilon = n/2$ lies in $\mathbb{Q}$, and $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, so $n/2 \in \mathbb{Z}$ — contradicting that n is odd.

This proves $\zeta \notin \mathbb{Z}[\beta]$. For the consequences: ζ is integral over $\mathbb{Z}$, so $\zeta \in \mathcal{O}_K$ while $\zeta \notin \mathbb{Z}[\beta]$, whence $\mathbb{Z}[\beta] \neq \mathcal{O}_K$; $\mathbb{Q}(\beta) = K$ is Proposition 3.2; and the minimal polynomial of β divides L_n by Proposition 3.1 and is irreducible, so it is an irreducible factor of L_n that is not monogenic. □

Two remarks on the shape of the proof. It never mentions a discriminant, a Dedekind criterion or a Newton polygon, and it never uses the classical description $\mathcal{O}_K = \mathbb{Z}[\zeta]$: the contradiction is reached from $\zeta \in \mathbb{Z}[\beta]$ alone, and the identification of $\mathcal{O}_K$ is needed only to phrase the conclusion as a statement about the ring of integers. And it is uniform: no case distinction on n beyond its parity, and no computation whose size grows with n.

Corollary 4.2. *Let m be odd. Every irreducible factor of $L_m(x)$ is monogenic if and only if $m = 1$. This answers Problem 2.*

Proof. If $m = 1$ then $L_1 = x$, whose unique irreducible factor is x itself, and 0 is a monogenic generator of $\mathbb{Q}$ (Proposition 5.2 (iii)). If $m > 1$, the minimal polynomial of $\zeta_m - \zeta_m^{-1}$ is a non-monogenic irreducible factor of L_m by Theorem 4.1. □

Corollary 4.2 stays inside the formal development, unlike the answers to Problems 1 and 3 in Section 6: it is the conjunction of machine-checked statements only, and uses neither (1) nor any result of [1].

Theorem 4.3. *Let m be even and not a power of 2. Then $F_m(x)$ has an irreducible factor over $\mathbb{Q}$ that is not monogenic. Explicitly, if $n > 1$ is any odd divisor of m, the minimal polynomial of $\zeta_n - \zeta_n^{-1}$ is such a factor. This answers the negative half of Problem 1.*

Proof. An even m that is not a power of 2 has an odd divisor $n > 1$. Take ζ a primitive n-th root of unity and $\beta = \zeta - \zeta^{-1}$. By Proposition 3.1, β is a root of F_m and its minimal polynomial over $\mathbb{Q}$ is an irreducible factor of F_m; by Theorem 4.1 that factor is not monogenic. □

5. Anchors, sharpness and controls

The smallest two cases are classical, and one of them is the source's own example; both are proved here directly, as a check that Theorem 4.1 is about the polynomials it claims to be about.

Proposition 5.1. *Let K be a field and $\zeta \in K$.*

(i) *If ζ is a primitive 3rd root of unity then $(\zeta - \zeta^{-1})^2 + 3 = 0$.*
(ii) *If ζ is a primitive 5th root of unity then $(\zeta - \zeta^{-1})^4 + 5(\zeta - \zeta^{-1})^2 + 5 = 0$.*

Proof. In each case rewrite ζ^{-1} as a power of ζ ($\zeta^{-1} = \zeta^2$, resp. $\zeta^{-1} = \zeta^4$) and reduce using $\zeta^n = 1$ and $1 + \zeta + \cdots + \zeta^{n-1} = 0$. □

Part (i) identifies $\mathbb{Z}[\beta]$ at $n = 3$ as $\mathbb{Z}[\sqrt{-3}]$, the index-2 suborder of $\mathbb{Z}[\zeta_3]$, and $x^2 + 3$ as the corresponding factor of $L_3 = x^3 + 3x$ and of $F_6 = x(x^2 + 1)(x^2 + 3)$. Part (ii) identifies the quartic of [1, Remark 1.3]: the source's single example is the case $n = 5$ of Theorem 4.1.

Both hypotheses of Theorem 4.1 are needed, and the conclusion cannot be strengthened from "some factor" to "every factor". The following four statements record this.

Proposition 5.2. (i) *If ζ is a primitive 1st root of unity then $\zeta \in \mathbb{Z}[\zeta - \zeta^{-1}]$; likewise if ζ is a primitive 2nd root of unity, in which case $\zeta = -1$ and $\zeta - \zeta^{-1} = 0$. So neither $n > 1$ nor the parity hypothesis of Theorem 4.1 is decorative.*
(ii) *For odd k, x divides $L_k(x)$.*
(iii) *0 is a monogenic generator of $\mathbb{Q}$.*
(iv) *For every $n > 0$ a primitive n-th root of unity exists in $\mathbb{C}$, so the hypotheses of Theorem 4.1 are not vacuous.*

In particular, by (ii) and (iii), it is false that every irreducible factor of L_n with n odd is non-monogenic.

Proof. (i) At $n = 1$, $\zeta = 1$; at $n = 2$, $\zeta^2 = 1$ and $\zeta \neq 1$ give $\zeta = -1$; in both cases $\zeta \in \mathbb{Z} \subseteq \mathbb{Z}[\zeta - \zeta^{-1}]$. (ii) The constant term of L_k vanishes for odd k, by the same two-step induction as in Lemma 2.2. (iii) $\mathbb{Q}(0) = \mathbb{Q}$ and $\mathbb{Z}[0] = \mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$. (iv) Take $\exp(2\pi i/n)$. □

Finally, Proposition 3.2 is the sharpness statement: the failure recorded by Theorem 4.1 is by a single factor of 2, not by a large or unspecified amount.

6. Consequences for Problems 1–3, and a confirming computation

This section is outside the formal development. Every lemma, proposition, theorem and corollary of Sections 2–5 is machine-checked; the statements below combine Theorem 4.1 with results of [1] that we cite rather than reprove, and with a computation carried out in PARI/GP [11]. They are stated as remarks for that reason.

Remark 6.1 (Classification of the Ω_d). For $d > 1$, the polynomial Ω_d of (1) is monogenic if and only if $d \not\equiv 2 \pmod 4$ or $d = 2$. Indeed: for odd d, Ω_d is the minimal polynomial of $i(\zeta_{2d} + \zeta_{2d}^{-1})$ and [1, Proposition 4.1] shows $\mathbb{Z}[i(\zeta_{2d} + \zeta_{2d}^{-1})]$ is the full ring of integers; for $4 \mid d$, Ω_d is also the minimal polynomial of $\zeta_{2d} - \zeta_{2d}^{-1}$ and [1, Proposition 3.2] applies with $m = 2d$, since $4 \mid 2d$ and $2d > 4$; $\Omega_2 = x$ is monogenic; and for $d = 2g$ with $g > 1$ odd, Ω_d is the minimal polynomial of $\zeta_g - \zeta_g^{-1}$ (Remark 2.4) and Theorem 4.1 applies. The two propositions cited here are the source's. By [1, Remark 3.3], [1,

Proposition 3.2] extends Shah and Nakahara [7], who treated $m = 2^k \geq 8$ and $m = 4p^k$ with p an odd prime; by [1, Remark 4.2], [1, Proposition 4.1] reproves a result of Motoda, Nakahara and Shah [8]. Only [1, Proposition 4.1] is used above, so the classification does not depend on [8], which we have not read (see Section 7).

Remark 6.2 (Answers to the three problems). Granting Remark 6.1, (1) turns each problem into a divisor count. Write $n = 2^a m$ with m odd.

(1) For even n, every irreducible factor of F_n is monogenic if and only if n is a power of 2. The divisors d of n with $d \equiv 2 \pmod 4$ and $d > 2$ are exactly the $2e$ with $e \mid m$, $e > 1$; there are none precisely when $m = 1$.
(2) For odd m, every irreducible factor of L_m is monogenic if and only if $m = 1$. (This is Corollary 4.2, and does not need Remark 6.1.)
(3) Yes, and the criterion is read off the factorisation alone. For even n,

$$\#\{\text{non-monogenic irreducible factors of } F_n\} = \tau(m) - 1 = \tau(\text{odd part of } n) - 1,$$

and for odd m the same count holds for L_m. Together with Theorems 1.1 and 1.2, this decides monogenity of the whole factorisation from the prime factorisation and parity of n, as Problem 3 asks.

The arithmetic function $\tau(\text{odd part of } n)-1$ is entry A069283 of the OEIS [12], named there "$a(n) = -1+$ number of odd divisors of n" and running from offset 0 with the convention $a(0) = 0$; only the values $n \geq 1$ are in play here. The match is with the arithmetic function only, and carries no monogenity content. It also explains the source's observation quoted in Section 1: the non-monogenic factors have no naive density because their number is a divisor count, not a density.

Remark 6.3 (The index). For odd $n > 1$ one has, inside $\mathcal{O}_K = \mathcal{O}_{K^+} \oplus \zeta\,\mathcal{O}_{K^+}$ where $K^+ = \mathbb{Q}(\zeta+\zeta^{-1})$,

$$\mathbb{Z}[\beta] = \mathcal{O}_{K^+} \oplus 2\zeta\,\mathcal{O}_{K^+}, \qquad \text{so} \qquad [\mathcal{O}_K : \mathbb{Z}[\beta]] = 2^{\varphi(n)/2}, \qquad \operatorname{disc}(\Omega_{2n}) = 2^{\varphi(n)}\, d_{\mathbb{Q}(\zeta_n)}.$$

The reason is that $\beta^2 = (\zeta^2 + \zeta^{-2}) - 2$ and ζ^2 is again a primitive n-th root of unity, so $\mathbb{Z}[\beta^2] = \mathbb{Z}[\zeta^2 + \zeta^{-2}] = \mathbb{Z}[\zeta + \zeta^{-1}] = \mathcal{O}_{K^+}$, while $\mathbb{Z}[\beta] = \mathbb{Z}[\beta^2] + \beta\,\mathbb{Z}[\beta^2]$ and $\beta = 2\zeta - (\zeta + \zeta^{-1})$. At $n = 5$ this gives index 4 and $\operatorname{disc}(x^4 + 5x^2 + 5) = 2000 = 2^4 \cdot 125$, the two entries recorded in [6, Table 1]; [1] gives no discriminants. This argument is not part of the formal development.

Remark 6.4 (Confirming computation). The classification of Remark 6.1 and both count laws of Remark 6.2 were checked in PARI/GP [11] over the source's own experimental range. Extracting Ω_d from F_d by dividing out the F_e with $e \mid d$, $e < d$, one finds $\deg \Omega_d = \varphi(d)$ and $\operatorname{disc}(\Omega_d) = d_{\mathbb{Q}(\Omega_d)}$ exactly when $d \not\equiv 2 \pmod 4$ or $d = 2$, for all 99 values $2 \leq d \leq 100$, with no exception; the non-monogenic $d \leq 100$ are precisely $6, 10, 14, \ldots, 98$. The count law was verified for every even $n \leq 100$ and every odd $m \leq 49$, with no mismatch. Separately, for each of the 20 odd values $3 \leq n \leq 41$, the four assertions $\zeta \notin \mathbb{Z}[\beta]$, $2\zeta \in \mathbb{Z}[\beta]$, $L_{n+1}(\beta) = \zeta + \zeta^{-1}$ and $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 2^{\varphi(n)/2}$ were confirmed by computing the coordinate vectors in the $\mathbb{Z}$-basis $1, \beta, \ldots, \beta^{\varphi(n)-1}$ and comparing disc with the field discriminant. The whole computation costs under two CPU-seconds and 27 megabytes. None of the theorems of this paper rests on it: it is a check on the statements, and the only exhaustive search anywhere in this work.

7. Verification

Every lemma, proposition, theorem and corollary of Sections 2–5 — the two lemmas, the two propositions on the order, the main theorem and its two consequences, the anchors and the four controls — has been formally verified in Lean 4 [9] against *Mathlib* [10], in a single module of about five hundred lines carrying nineteen theorems. A numbered statement here is in general the conjunction of several of those theorems, which are stated one clause at a time: Theorem 4.1, for instance, is assembled from the non-membership $\zeta \notin \mathbb{Z}[\beta]$, the failure of monogenity, and the irreducibility and divisibility of the minimal polynomial, and Corollary 4.2 from Theorem 4.1 together with Proposition 5.2 (ii),(iii). The module contains no `sorry`, no hand-written `axiom`, and

no appeal to compiled evaluation: `#print axioms` on each of the nineteen returns exactly `propext`, `Classical.choice` and `Quot.sound`, the three standard axioms of Mathlib's foundation. In particular nothing here is a certificate check, and no statement is established only on a finite range: the arguments are uniform in n, and the computation of Remark 6.4 lies outside the development, as does everything else in Section 6. The predicate of Definition 2.1 is defined in the module as the conjunction $\mathbb{Q}[\theta] = \top$ and $\mathbb{Z}[\theta] = \mathrm{integralClosure}(\mathbb{Z}, K)$; Mathlib has no monogenicity predicate for number fields, no Dedekind criterion and no order-index API, and the proof needs none of them. The classical identification $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, valid for every n, is available in Mathlib as `IsCyclotomicExtension.Rat.adjoin_singleton_eq_top`.

The negative claim of Section 1 — that the statement uniform in n is not in the literature — rests on the following searches, carried out on 3 September 2026 and reported so that they can be judged rather than repeated. A full-text corpus of arXiv mathematics was searched for the token `monogen`, giving 1998 distinct papers; intersecting with the papers mentioning $\zeta - \zeta^{-1}$, Fibonacci polynomials or Lucas polynomials left 22, all of which were read, and none states the uniform result. Gaál's survey [2] was read in full and contains no statement about $\mathbb{Z}[\zeta_n - \zeta_n^{-1}]$ for odd n. The OEIS was searched for the index sequence $2, 4, 8, 8, 32, 64, 16, 256, 512$ and for two phrase searches, with no result. Eight live web query shapes, combining monogenity with $\zeta - \zeta^{-1}$, with the Fibonacci and Lucas polynomials and with index forms, returned only [1]. Two limitations are recorded: one bibliographic database (Semantic Scholar) was rate-limited throughout and contributed no signal, and [8] is behind a paywall and was not consulted directly — it is used only for the attribution in Remark 6.1, which is not part of the formal development, and that attribution agrees with the review of [8] in zbMATH (Zbl 1032.11043), which states that the compositum of $\mathbb{Q}(i)$ with the maximal real subfield of a cyclotomic field of odd conductor $f > 1$ is monogenic.

References

[1] H. Chen, W. Guo and H. Hong, *Monogenity of Fibonacci polynomials and Lucas polynomials*, arXiv:2606.08024v1 (6 June 2026). Live at v1, with no journal reference, when checked on 3 September 2026.

[2] I. Gaál, *Monogenity and Power Integral Bases: Recent Developments*, Axioms **13** (2024), no. 7, article 429, doi:10.3390/axioms13070429.

[3] J. Harrington and L. Jones, *Monogenic cyclic polynomials in recurrence sequences*, arXiv:2505.09481v2; Colloq. Math. **180** (2026), 21–30, doi:10.4064/cm9671-10-2025. The quotations here are from the e-print, whose §1 carries them verbatim in both v1 and v2.

[4] J. König, *A note on monogenic even polynomials*, arXiv:2505.10119v1 (15 May 2025). Live at v1, with no journal reference, when checked on 3 September 2026.

[5] L. Jones, *Monogenic cyclic quartic trinomials*, arXiv:2404.17869v1 (27 April 2024); the e-print carries no journal reference. A paper with the same abstract and the same main theorem appeared as *Monogenic even quartic trinomials*, Bull. Austral. Math. Soc. **111** (2025), no. 2, 238–243, doi:10.1017/S0004972724000510. The quotation and the numbering used above are those of the e-print.

[6] L. Jones and D. White, *Monogenic trinomials with non-squarefree discriminant*, arXiv:1908.07947v2; Internat. J. Math. **32** (2021), no. 13, article 2150089, doi:10.1142/S0129167X21500890. Table 1 is the item cited, in the numbering of the e-print.

[7] S. I. A. Shah and T. Nakahara, *Monogenesis of the rings of integers in certain imaginary abelian fields*, Nagoya Math. J. **168** (2002), 85–92, doi:10.1017/S0027763000008369.

[8] Y. Motoda, T. Nakahara and S. I. A. Shah, *On a problem of Hasse for certain imaginary abelian fields*, J. Number Theory **96** (2002), no. 2, 326–334, doi:10.1016/S0022-314X(02)92805-2. Not consulted directly; see Section 7.

[9] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28 (A. Platzer and G. Sutcliffe, eds.), Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635.

[10] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381.

[11] The PARI Group, *PARI/GP*, version 2.13.3, Univ. Bordeaux, `https://pari.math.u-bordeaux.fr`.

[12] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`. Entries A049310, A114525 and A069283; searches of 3 September 2026, no match for the index sequence.