ON AN IRREDUCIBILITY QUESTION CONCERNING PALINDROMIC NON-CYCLOTOMIC 0, 1-POLYNOMIALS

Pradipto Banerjee[1]
Department of Mathematics, IIT Hyderabad, Sangareddy, Kandi, Telangana, India
pradipto@math.iith.ac.in

Amit Kundu
Department of Mathematics, IIT Hyderabad, Kandi, Sangareddy, Kandi, Telangana, India
ma21resch01001@iith.ac.in

Received: 9/12/23, Revised: 3/23/24, Accepted: 7/15/24, Published: 8/16/24

Abstract

It is established that if $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, has degree even, and $f(x^2)$ is reducible over $\mathbb{Q}$, then $f(x^2) \equiv f(x)f(-x) \pmod 4$. Making use of this criterion, it is shown that if $f(x) = x^{d_{Q-1}} + x^{d_{Q-2}} + \cdots + x^{d_1} + 1$, where $Q < 15$, is irreducible over $\mathbb{Q}$, then $f(x^2)$ is irreducible over $\mathbb{Q}$ unless $f(x)$ is cyclotomic. These results address, for the first time, an open question of Michael Filaseta asking whether $f(x^r)$ is irreducible over $\mathbb{Q}$ for every positive integer r where $f(x)$ is a non-cyclotomic polynomial having 0 and 1 as coefficients, and is irreducible over $\mathbb{Q}$.

1. Introduction

Let $\mathscr{N}$ denote the collection of polynomials whose coefficients are 0 and 1. We will refer to the elements of $\mathscr{N}$ as 0, 1-polynomials. They are known to exhibit elegant mathematical properties, both algebraic and analytic. For instance, if W denotes the complete set of complex zeros of polynomials in $\mathscr{N}$, then Odlyzko and Poonen [8] showed that $\gamma^{-1} < |z| < \gamma$ for all $z \in W$ where $\gamma = (1 + \sqrt{5})/2$. Among several other exciting results, they demonstrated that $\overline{W}$ is path connected where $\overline{W}$ is the closure of W in $\mathbb{C}$. As for some of the algebraic aspects, Filaseta, Finch, and Nicol [5] showed, among other things, that for positive integers a, b, and c, one among $1 + x^a + x^b$, $1 + x^b + x^c$, and $1 + x^c + x^a$ is irreducible over $\mathbb{Q}$. Filaseta and Konyagin [2] established that for a fixed positive integer n, the number of squarefree polynomials (a polynomial is squarefree if it has no multiple roots) of degree at most n in $\mathscr{N}$ is asymptotic to 2^n. This implies that about one-half of the polynomials in

DOI: 10.5281/zenodo.13331507
[1]Corresponding author

$\mathscr{N}$ are squarefree. We will also mention a few other thematically relevant results as we describe the main problem below.

The present work was strongly motivated by a question of Filaseta [3] concerning the irreducibility of $f(x^r)$ over $\mathbb{Q}$ for certain $f(x) \in \mathscr{N}$ that are irreducible over $\mathbb{Q}$. In what follows, irreducibility will always refer to the irreducibility over $\mathbb{Q}$. Since any non-constant member of $\mathscr{N}$ is monic, by Gauss's lemma, it suffices to consider the irreducibility over $\mathbb{Z}$.

To state Filaseta's question in a more persuading manner, let $\mathscr{N}_{\text{irred}}$ denote the collection of irreducible polynomials in $\mathscr{N}$. For $f(x) \in \mathscr{N}_{\text{irred}}$ and a positive integer r, we consider the polynomial $f(x^r) \in \mathscr{N}$. However, $f(x^r)$ does not necessarily belong to $\mathscr{N}_{\text{irred}}$ in general. The polynomial $f(x) = x$ is a trivial example. There are other members $f(x) \in \mathscr{N}_{\text{irred}}$ with the property that $f(x^r)$ is reducible for some $r > 1$. For instance, $f(x) = x^2 + x + 1 \in \mathscr{N}_{\text{irred}}$ but $f(x^2) = f(x)f(-x)$. More generally, if $f(x) \in \mathscr{N}_{\text{irred}}$ is cyclotomic, then $f(x^p)$ is reducible for every sufficiently large prime p. To be precise, for a positive integer ℓ, *the ℓ-th cyclotomic polynomial* $\Phi_\ell(x)$ is defined as

$$\Phi_\ell(x) = \prod_{\substack{0<i<\ell \\ \gcd(i,\ell)=1}} (x - \omega^i), \quad \omega = e^{2\pi i/\ell}.$$

It is well-known that $\Phi_\ell(x)$ is a monic polynomial with integer coefficients and has degree $\phi(\ell)$, where ϕ is the Euler phi function. An integer polynomial is called *cyclotomic* if it is a product of the polynomials $\Phi_\ell(x)$. Otherwise, it is referred to as *non-cyclotomic*. It is an established fact that for a positive integer r, the polynomial $\Phi_\ell(x^r)$ is irreducible if and only if every prime divisor of r divides ℓ. In particular, $\Phi_\ell(x^p)$ is reducible for every $p \nmid \ell$, and factors as

$$\Phi_\ell(x^p) = \Phi_\ell(x)\Phi_{p\ell}(x).$$

There are infinitely many cyclotomic polynomials in $\mathscr{N}_{\text{irred}}$. For instance, $\Phi_3(x^{3^k}) \in \mathscr{N}_{\text{irred}}$ for every positive integer k. Accordingly, we phrase the question as follows.

Question 1. Suppose that $f(x) \in \mathscr{N}_{\text{irred}}$ is non-cyclotomic. Is it true that $f(x^r) \in \mathscr{N}_{\text{irred}}$ for every positive integer r?

Extending a method of Ljunggren [7], Filaseta [3] provided a partial answer to Question 1 in the affirmative establishing that if $f(x)$ has the additional characteristic of being *nonreciprocal*, then $f(x^r)$ is irreducible for every positive integer r. A polynomial $h(x)$ is referred to as *reciprocal* if

$$h(x) = \pm x^{\deg h} h\left(\frac{1}{x}\right),$$

with the plus sign if $h(x) \in \mathscr{N}$. Otherwise, $h(x)$ is *nonreciprocal*. In general, for a given $h(x) \in \mathbb{Z}[x]$, the polynomial $x^{\deg h} h(1/x)$ is referred to as the *reciprocal of* $h(x)$, and denoted by $\widetilde{h}(x)$. Every non-constant monomial is nonreciprocal.

Cyclotomic polynomials are prime examples of reciprocal polynomials. Given Filaseta's work, it remains to consider $f(x) \in \mathscr{N}_{\text{irred}}$ which are non-cyclotomic and reciprocal. We denote this subset of $\mathscr{N}_{\text{irred}}$ by $\mathscr{N}_{\text{irred}}^{\text{ncr}}$.

Reciprocal members of $\mathscr{N}$ are an important class of polynomials in their own right. For example, Konvalina and Matache [6] have shown that every reciprocal $0,1$-polynomial has a root on the unit circle. Filaseta and Meade [4] have established that every irreducible factor of a reciprocal $0,1$-polynomial is reciprocal. Additionally, as far as Lehmer's conjecture on the Mahler measures of monic integer polynomials is concerned, the reciprocal non-cyclotomic members of $\mathscr{N}$ remain a significant hurdle.

We now return to the topic at hand. Filaseta [3] posed the problem of proving (or disproving) that if $f(x) \in \mathscr{N}_{\text{irred}}^{\text{ncr}}$, then $f(x^r)$ is irreducible for every integer $r \geq 1$. In this regard, our initial software-based experimentations suggest the following.

Conjecture 1. Let $f(x)$ be an irreducible reciprocal non-cyclotomic $0,1$-polynomial. Then $f(x^r)$ is irreducible for every integer $r \geq 1$.

A proof of Conjecture 1 will completely answer Question 1. However, the authors believe this is potentially a hard problem to resolve. In our modest attempt, we prove a partial result corroborating the possible validity of Conjecture 1 in the case where $r = 2$ and $f(x)$ has few terms.

Theorem 1. *Let $f(x)$ be an irreducible reciprocal non-cyclotomic $0,1$-polynomial with less than 15 terms. Then $f(x^2)$ is irreducible.*

Thus, Theorem 1, together with Filaseta's result, provides a complete answer to Question 1 for $f(x)$ having at most fourteen terms in the case $r = 2$. In the next section, we will show that it suffices to assume r is prime in Conjecture 1. We conclude this section by briefly discussing our strategy in proving Theorem 1.

Let $f(x) \in \mathscr{N}_{\text{irred}}^{\text{ncr}}$, say

$$f(x) = x^{d_{Q-1}} + x^{d_{Q-2}} + \cdots + x^{d_1} + 1.$$

We treat the exponents of $f(x)$ as unknowns. Initially, there are $Q - 1$ unknowns to begin with. To prove Theorem 1, we only need to work with $Q < 15$. By the reciprocality of $f(x)$, we have $d_{Q-1-j} = d_{Q-1} - d_j$. This reduces the number of unknowns to at most $(Q-1)/2$. In Section 3, we will further reduce this to at most $Q/3$ unknowns. This step is key in bringing the computational complexities down to a manageable state. The proof of Theorem 1 rests upon the observation (see Theorem 3, Section 2) that if $f(x) \in \mathscr{N}_{\text{irred}}$ with $f(x^2)$ reducible, then

$$f(x^2) \equiv f(x)f(-x) \pmod{4}.$$

After eliminating the common terms on the two sides of the above congruence, we obtain a congruence of the shape $H_L(x) \equiv H_R(x) \pmod{2}$ where $H_L(x)$ and $H_R(x)$

are sums of monomials whose exponents can be expressed in terms of the unknowns d_j. The idea, then, is to match the exponents on both sides depending on their sizes and parities. But at this stage, we still have around $Q/2$ unknowns involved. We will demonstrate that there is a unique odd positive integer ℓ, and unique reciprocal polynomials $f_e(x)$ and $f_o(x)$, such that

$$f(x) = f_e(x^2) + x^\ell f_o(x^2).$$

Thus, each d_j can be expressed in terms of ℓ and the exponents of the terms of $f_e(x)$ and $f_o(x)$. We introduce these unknowns and rewrite $H_L(x) \equiv H_R(x) \pmod 2$. Next, we leverage the reciprocality of $f_e(x)$ and $f_o(x)$ to reduce this to a polynomial congruence $F_L(x) \equiv F_R(x) \pmod 2$ where $F_L(x)$ and $F_R(x)$ are sums of monomials with exponents expressed in terms of the exponents of monomials in $f_e(x)$ and $f_o(x)$. We further maneuver to ensure that the total number of unknowns in the various exponents appearing in $F_L(x) \equiv F_R(x) \pmod 2$ is at most $Q/3$. We then compare the exponents as previously described, leading to several linear equations in these unknowns for which we seek positive integral solutions. We prove our result by establishing that every feasible solution produces a cyclotomic $f(x)$.

The paper is organized as follows. In Section 2, we establish the irreducibility criterion and prepare the ground for the proof of Theorem 1. In Section 3, we finish the proof of Theorem 1 with the help of several lemmas.

2. Applications of Capelli's Theorem

We begin by discussing the factorization of $f(x^r)$ for an arbitrary irreducible integer polynomial $f(x)$. Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree n. As a consequence of Capelli's main results [1] in this direction, one obtains the following neat reducibility criterion for $f(x^r)$ (see Theorems 20 and 21 in [9]).

Theorem 2 ([9])**.** *Let $f(x) \in \mathbb{Z}[x]$ be irreducible, and suppose that $r \geq 2$ is an integer. Then $f(x^r)$ is reducible if and only if one of the following holds.*

(i) The polynomial $f(x^p)$ is reducible for some prime p dividing r. Equivalently, for every complex root α of $f(x)$, there is some $\beta \in \mathbb{Q}(\alpha)$ such that $\alpha = \beta^p$ for some prime p dividing r.

(ii) One has $4 \mid r$, and $f(x^4)$ is reducible. Equivalently, $4 \mid r$, and for every complex root α of $f(x)$, there is some $\beta \in \mathbb{Q}(\alpha)$ such that $\alpha = -4\beta^4$.

Given Theorem 2, it suffices to assume r is either a prime or $r = 4$ in Conjecture 1. After establishing the irreducibility criterion for $f(x^2)$ below, we will demonstrate that the condition $r = 4$ can be dropped.

We will now specialize in the case where $f(x) \in \mathscr{N}_{\text{irred}}^{\text{ncr}}$, although the proof is valid for any monic irreducible polynomial of even degree with integer coefficients. It is not hard to see that if $f(x) \in \mathscr{N}_{\text{irred}}^{\text{ncr}}$, and $\deg f$ is odd, then $f(-1) = 0$. Thus, $\deg f$ is even for every $f(x) \in \mathscr{N}_{\text{irred}}^{\text{ncr}}$. Henceforth, we will assume that $\deg f$ is even.

Theorem 3. *Let $f(x) \in \mathscr{N}_{\text{irred}}$. If $f(x^2)$ is reducible, then*

$$f(x^2) \equiv f(x)f(-x) \pmod 4. \tag{1}$$

Proof. Let $f(x)$ be as stated in the theorem. Further, suppose that $f(x^2)$ is reducible. By [10, Lemma 24, pg. 152], there exists a monic polynomial $g(x) \in \mathbb{Z}[x]$ such that

$$f(x^2) = g(x)g(-x). \tag{2}$$

We claim that $g(x) \equiv f(x) \pmod 2$. But this is clear after considering Equation (2) modulo 2. Namely, we have

$$f(x^2) \equiv g(x)^2 \equiv g(x^2) \pmod 2.$$

The assertion follows. Thus, $g(x) = f(x)+2h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Eliminating $g(x)$ from Equation (2), we obtain

$$\begin{aligned} f(x^2) &= (f(x) + 2h(x))(f(-x) + 2h(-x)) \\ &\equiv f(x)f(-x) + 2(f(x)h(-x) + f(-x)h(x)) \pmod 4. \end{aligned}$$

Since $f(x)$ and $h(x)$ have integer coefficients, the conclusion of the theorem follows by observing that $f(x)h(-x) + f(-x)h(x) \equiv 0 \pmod 2$. □

Let $f(x) \in \mathscr{N}_{\text{irred}}$. Recall that in resolving Conjecture 1, one may assume that $r = 4$ if r is not a prime. We shall next establish below that $f(x^4)$ is reducible if and only if $f(x^2)$ is reducible. Consequently, it would suffice to assume that r is prime in Conjecture 1, as asserted earlier.

Theorem 4. *Let $f(x) \in \mathscr{N}_{\text{irred}}$ of degree $n > 0$. Then $f(x^4)$ is reducible if and only if $f(x^2)$ is reducible.*

Proof. Let $f(x)$ be as stated in the theorem. It is easy to see that $f(x^4)$ is reducible if $f(x^2)$ is reducible. Conversely, suppose that $f(x^4)$ is reducible and $f(x^2)$ is irreducible. Thus, $f(x^2) \in \mathscr{N}_{\text{irred}}$. We proceed as in the proof of Theorem 3 to first deduce that there is an irreducible monic polynomial $u(x) \in \mathbb{Z}[x]$ satisfying $u(x) \equiv f(x^2) \pmod 2$ such that

$$f(x^4) = u(x)u(-x). \tag{3}$$

Let $u(x) = f(x^2) + 2r(x)$ where $r(x) \in \mathbb{Z}[x]$. Substituting $u(x)$ in Equation (3) with this expression, one obtains

$$\begin{aligned} f(x^4) &= (f(x^2) + 2r(x))(f(x^2) + 2r(-x)) \\ &= f(x^2)^2 + 2f(x^2)(r(x) + r(-x)) + 4r(x)r(-x). \end{aligned}$$

Since $r(x) + r(-x) \equiv 0 \pmod 2$, it follows that $f(x^4) \equiv f(x^2)^2 \pmod 4$. Consequently,

$$f(x^2) \equiv f(x)^2 \pmod 4. \tag{4}$$

Now, suppose $f(x)$ is not a constant. Then there is an integer $t \in \{1, 2, \ldots, n\}$ such that $f(x) = 1 + x^t + x^{t+1}v(x)$ for some $v(x) \in \mathbb{Z}[x]$. Then, Equation (4) implies

$$1 + x^{2t} + x^{2t+2}v(x^2) \equiv 1 + 2x^t + x^{t+1}v_1(x) \pmod 4,$$

for some $v_1(x) \in \mathbb{Z}[x]$. We obtain a contradiction by comparing the coefficients of x^t on both sides above. This concludes the proof. □

3. A Proof of Theorem 1

We now turn to the proof of Theorem 1. In what follows, we assume that $f(x)$ is as stated in Theorem 1. We further assume throughout that $\deg f = n = 2m$ where $m > 0$ is an integer. Moreover, since every irreducible $0,1$-polynomial of degree 2 is cyclotomic, we constrain ourselves to the case that $m > 1$. As before, $Q = f(1)$ will denote the number of terms of $f(x)$, and we restrict to $Q < 15$ for our purposes.

We will prove Theorem 1 by contradiction. Accordingly, we suppose that $f(x^2)$ is reducible. Then Theorem 3 implies that Equation (1) holds. We will next establish several lemmas to prove Theorem 1.

Lemma 1. *Let $h(x) \in \mathbb{Z}[x]$ be an irreducible reciprocal polynomial of degree $2k$ such that $h(x) \notin \mathbb{Z}[x^2]$. Then, there are unique reciprocal integer polynomials $h_e(x)$ and $h_o(x)$ and a unique odd positive integer ℓ_h, satisfying*

$$\deg h_e = k \quad \textit{and} \quad \deg h_o = k - \ell_h, \tag{5}$$

such that

$$h(x) = h_e(x^2) + x^{\ell_h} h_o(x^2) \quad \textit{with} \quad h_e(0)h_o(0) \neq 0. \tag{6}$$

Proof. Observe that $h(x) \notin \mathbb{Z}[x^2]$ implies there are unique $h_e(x), h_o(x) \in \mathbb{Z}[x]$, and a unique odd positive integer ℓ_h, such that Equation (6) holds with $h_o(0) \neq 0$. Since $h(x)$ is irreducible of degree $2k$, we deduce that $h(x) \not\equiv x$ so that $h(0) \neq 0$. It follows that $h_e(0) = h(0) \neq 0$. Furthermore, it can be easily seen that both $h_e(x^2)$ and $h_o(x^2)$ are reciprocal since $h(x)$ is the reciprocal of an even degree. Thus, $h_e(x)$ and $h_o(x)$ are reciprocal.

It remains to establish Equation (5). It is clear from $\deg h = 2k$ that $\deg h_e = k$. Taking the reciprocal of the polynomials appearing on both sides of Equation (6), we obtain

$$h(x) = \widetilde{h}(x) = h_e(x^2) + x^{2k-\ell_h-2\deg h_o} h_o(x^2).$$

Comparing the above with Equation (6), we deduce that

$$\ell_h = 2k - \ell_h - 2\deg h_o,$$

establishing Equation (5). The lemma follows. □

Lemma 2. *Suppose that $f(x) \in \mathscr{N}_{\text{irred}}$ is reciprocal with $\deg f = 2m$ such that $f(x^2)$ is reducible. Then there are unique reciprocal polynomials $f_e(x)$ and $f_o(x)$ in $\mathscr{N}$, as well as a unique odd positive integer ℓ, such that*

$$\deg f_e = m, \quad \deg f_o = m - \ell,$$

and

$$f(x) = f_e(x^2) + x^\ell f_o(x^2) \quad \textit{with} \quad f_e(0) f_o(0) \neq 0. \tag{7}$$

Proof. The conclusion follows from Lemma 1 provided that $f(x) \notin \mathbb{Z}[x^2]$. So, suppose that $f(x) = h(x^2)$ for some $h(x) \in \mathscr{N}$. Observe that $h(x) \in \mathscr{N}_{\text{irred}}$ since $f(x)$ is irreducible. But then Theorem 4 implies that $f(x^2) = h(x^4)$ is irreducible, contradicting our assumption that $f(x^2)$ is reducible. This settles the lemma. □

Observe that the integer ℓ in Lemma 2 is the smallest odd exponent of x in $f(x)$ since $f_o(0) = 1$. Since ℓ is odd, exactly one of the integers $\deg f_e = m$ and $\deg f_o = m - \ell$ is odd. Accordingly, either $f_e(-1) = 0$ or $f_o(-1) = 0$ since these polynomials are reciprocal. Expressing $f(x)$ and $f(-x)$ in terms of $f_e(x)$ and $f_o(x)$, and substituting in Equation (1), we get

$$f(x^2) \equiv f_e(x^2)^2 - x^{2\ell} f_o(x^2)^2 \pmod 4.$$

In other words,

$$f(x) \equiv f_e(x)^2 - x^\ell f_o(x)^2 \pmod 4. \tag{8}$$

We need the following information on ℓ appearing in Equation (8).

Lemma 3. *Let $f(x) \in \mathscr{N}_{\text{irred}}$ be reciprocal non-cyclotomic of degree $2m$. Let $f_e(x)$, $f_o(x)$, and ℓ be as defined in Equation (7). Suppose that $f(x^2)$ is reducible (so that Equation (8) holds). Then, ℓ is the smallest exponent of x appearing in $f(x)$. Moreover, $\ell < m/2$.*

Proof. We first show that ℓ is the smallest nonzero exponent of x in $f(x)$. Suppose that $f(x) = \sum_{j=0}^{2m} \varepsilon_j x^j$, where each $\varepsilon_j \in \{0, 1\}$ with $\varepsilon_{2m} = \varepsilon_0 = 1$. Further, let $f_e(x) = \sum_{j=0}^{m} c_j x^j$, where every $c_j \in \{0, 1\}$ with $c_m = c_0 = 1$. Since $\varepsilon_\ell = 1$ by hypothesis, it suffices to show that $c_k = 0$ for each k satisfying $0 < k < \ell$. After comparing the coefficient of x^k on both sides of Equation (8), we have

$$\varepsilon_k = \begin{cases} 2\displaystyle\sum_{\substack{0<i+j=k\\ i<j}} c_i c_j & \text{if} \quad k \equiv 1 \pmod 2 \\ c_{k/2} + 2\displaystyle\sum_{\substack{i+j=k\\ i<j}} c_i c_j & \text{if} \quad k \equiv 0 \pmod 2. \end{cases} \tag{9}$$

We prove our assertion inductively. For $k = 1$, we have $\varepsilon_1 = 2c_1$. Since $\varepsilon_1 \in \{0, 1\}$, it follows that $c_1 = 0$. Next, assume that $c_i = 0$ for every i satisfying $0 < i < k$. Thus, $\varepsilon_k = 2c_0c_k = 2c_k$. Once again, since $\varepsilon_k \in \{0, 1\}$, it follows that $c_k = 0$, proving our assertion.

We next establish that $\ell < m/2$. The coefficient of x^ℓ in $f_e(x)^2 - x^\ell f_o(x)^2$ is $2c_\ell - 1$. From Equation (8), one has

$$1 = \varepsilon_\ell \equiv 2c_\ell - 1 \pmod 4.$$

Thus, $c_\ell = 1$. Accordingly, it follows from Equation (9) that $\varepsilon_{2\ell} = 1$. We assert that the coefficient of $x^{\ell+k}$ in $f(x)$ is zero whenever k is odd and $0 < k < \ell$. There is nothing to prove if $\ell = 1$. So, assume that $\ell > 1$. Let $f_o(x) = \sum_{j=0}^{m-\ell} b_j x^j$, where each $b_j \in \{0, 1\}$ with $b_0 = b_{m-\ell} = 1$. Since $c_j = 0$ for every j satisfying $0 < j < \ell$, one computes that for an odd $k \in (0, \ell)$, the coefficient of $x^{\ell+k}$ in $f_e(x)^2 - x^\ell f_o(x)^2$ is

$$2c_{\ell+k} - 2\sum_{j=0}^{k} b_j b_{k-j} \equiv 0 \pmod 2.$$

It now follows from Equation (8) that $\varepsilon_{\ell+k} = 0$ for every odd $k \in (0, \ell)$. In particular, $\varepsilon_{2j} = 0$ for each j satisfying $0 < j < \ell$. Next, observe that $\ell < m$. Otherwise, $m - \ell = \deg f_o \geq 0$ would imply that $\ell = m$. In that event, $f(x) = x^{2m} + x^m + 1$, which is cyclotomic, contrary to our assumption.

If $2\ell > m$, then

$$0 < 2m - 2\ell < m < 2\ell,$$

whence, $\varepsilon_{2m-2\ell} = 0$. On the other hand, since $f(x)$ is reciprocal of degree $2m$, one has that $\varepsilon_{2m-2\ell} = \varepsilon_{2\ell} = 1$. It follows that $2\ell \leq m$.

Next, suppose $2\ell = m$. Since $\varepsilon_{2j} = 0$ for every j satisfying $0 < j < \ell$, it follows from the reciprocality of $f(x)$ that $f_e(x) = x^{2\ell} + x^\ell + 1$. Also, in this case, $\deg f_o = m - \ell = \ell$. We claim that $f_o(x) = x^\ell + 1$. If that is not the case, then let k denote the smallest exponent of x in $f_o(x)$ satisfying $0 < k < \ell$. Consider the coefficient of $x^{\ell+k}$ on both sides of Equation (8). While the coefficient of $x^{\ell+k}$ on the right is -2, the same on the left is ε_k. However, this implies $\varepsilon_k \equiv -2 \pmod 4$, which is an impossibility since $\varepsilon_k \in \{0, 1\}$. The claim now follows. Thus,

$f_o(x) = x^\ell + 1$, and

$$f(x) = f_e(x^2) + x^\ell f_o(x^2) = x^{4\ell} + x^{3\ell} + x^{2\ell} + x^\ell + 1 = \Phi_5(x^\ell).$$

This is a contradiction since $f(x)$ is not cyclotomic per our hypothesis. Therefore, $\ell < m/2$, as required. □

Next, assume that $f(x) \in \mathscr{N}_{\text{irred}}$ is reciprocal such that $f(x^2)$ is reducible. It follows from the proof of Theorem 3 that there is an irreducible monic $g(x) \in \mathbb{Z}[x]$ with $\deg g = \deg f = 2m$, such that Equation (2) holds. As mentioned in the introduction, a result of Filaseta and Meade (see [4, Lemma 2]) implies that every irreducible factor of a reciprocal $0,1$-polynomial is reciprocal. So, both $g(x)$ and $g(-x)$ are reciprocal. Observe that $g(x) \notin \mathbb{Z}[x^2]$. Otherwise, Equation (2) would imply that $f(x^2) = g(x)^2$. This is impossible since $f(x)$ is irreducible (so that $f(x^2)$ is separable).

Let ℓ_g, $g_e(x)$, and $g_o(x)$ be as stated in Lemma 1. Specifically,

$$g(x) = g_e(x^2) + x^{\ell_g} g_o(x^2),$$

where $\deg g_e = m$ and $\deg g_o = m - \ell_g$. We eliminate $g(x)$ from the equation $f(x^2) = g(x)g(-x)$ using the last relation above to obtain

$$f(x^2) = g_e(x^2)^2 - x^{2\ell_g} g_o(x^2)^2.$$

Consequently,

$$f(x) = g_e(x)^2 - x^{\ell_g} g_o(x)^2. \tag{10}$$

Setting $x = 1$ in Equation (10), we obtain

$$f(1) = g_e(1)^2 - g_o(1)^2.$$

Considering that 0, 1, 4, and 9 are the only squares modulo 16, we deduce that $Q = f(1) \equiv r \pmod{16}$, where

$$r \in \{0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15\}.$$

Given that $0 < Q < 15$, we further restrict ourselves to

$$Q \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13\}.$$

It is easily seen that $Q = 1$ implies $f(x) \equiv 1$. We discard this case. We can further eliminate $Q = 3$ and $Q = 4$ from the list since every three or four-term reciprocal $0,1$-polynomial is cyclotomic. To see this, first, observe that there is a unique three-term reciprocal $0,1$-polynomial of degree $2m$. Namely, the polynomial $f(x) = x^{2m} + x^m + 1 = \Phi_3(x^m)$, which is cyclotomic. In the case that $Q = 4$, the polynomial $f(x)$ has the shape $f(x) = x^{2m} + x^{2m-k} + x^k + 1$ for some integer

$k \in (0, m)$. One verifies that $f(x) = (x^{2m-k} + 1)(x^k + 1)$, and hence, $f(x)$ is cyclotomic. From now on, we will limit our discussion to the case where $Q \in \{5, 7, 8, 9, 11, 12, 13\}$.

Some remarks are in order in handling the case where $Q \in \{8, 12\}$. Suppose $f(x) \in \mathscr{N}_{\text{irred}}$ is reciprocal and $f(x^2)$ is reducible. Let $g(x)$ be as stated in Equation (2), and let $g_e(x)$ and $g_o(x)$ be as defined previously. Since $g(x)$ is reciprocal of degree $2m$, we deduce from Lemma 1 that both $g_e(x)$ and $g_o(x)$ are reciprocal. Furthermore, exactly one of them has an odd degree since $\deg g_e - \deg g_o = \ell_g$ is odd. Let $\{g_1(x), g_2(x)\} = \{g_e(x), g_o(x)\}$ be such that $\deg g_1$ is odd. In particular, $g_1(-1) = 0$. Consequently, $f(-1) = g_2(-1)^2$. So, if $Q = f(1)$ is even, then $g_2(1)$ is even. Based on these observations, it is possible to dismiss the scenario where $Q = 8$ in the following manner. Notice that $Q = 8$ arises when $g_e(1)^2 = 9$ and $g_o(1)^2 = 1$. However, this implies $g_2(1) \equiv 1 \pmod 2$, which is a contradiction since $Q = 8$ is even. The next lemma will allow us to handle the case that $f(1) = 12$ with relative ease.

Lemma 4. *Let $f(x)$, $g_1(x)$, and $g_2(x)$ be as described above. Suppose that $g_2(1) \equiv 0 \pmod 4$. If $f(1) \equiv 4\varepsilon \pmod{16}$ for some $\varepsilon \in \{-1, 1\}$, then $f(-1) \equiv 0 \pmod{16}$.*

Proof. Let $g_e(x)$, $g_o(x)$, ℓ_g, $g_1(x)$, and $g_2(x)$ be as stated before. Suppose that

$$f(1) \equiv 4\varepsilon \pmod{16} \quad \text{and} \quad g_2(1) \equiv 0 \pmod 4.$$

Then $g_i(1) \equiv g_i(-1) \equiv 0 \pmod 2$ for each $i \in \{1, 2\}$. Recall that $\deg g_1$ is odd with $g_1(-1) = 0$. Thus, $f(-1) = g_2(-1)^2 \equiv 0 \pmod 4$. We claim that $g_2(-1) \equiv 0 \pmod 4$. For the sake of convenience, we let $G(x)$ denote $g_2(x)$. So, $G(1) \equiv 0 \pmod 4$. If $G(x) \in \mathbb{Z}[x^2]$, then $G(-1) = G(1) \equiv 0 \pmod 4$, as required. Otherwise, let $\ell_G = k$, $G_e(x)$, and $G_o(x)$ be as defined in Lemma 1 for the polynomial $G(x)$. Specifically,

$$G(x) = G_e(x^2) + x^k G_o(x^2) \quad \text{with} \quad k = \deg G_e - \deg G_o.$$

Since $G(x)$ is a reciprocal polynomial of even degree, the polynomials $G_e(x)$ and $G_o(x)$ are reciprocal. This implies that $\deg G_e$ is odd or $\deg G_o$ is odd. Accordingly, $x + 1$ divides either $G_e(x)$ or $G_o(x)$. Therefore, either $G_e(1)$ is even or $G_o(1)$ is even. Since $G(1)$ is even, we can conclude that both $G_e(1)$ and $G_o(1)$ are even.

Next, observe that if $G(-1) \equiv 2 \pmod 4$, then

$$G_e(1) - G_o(1) = G(-1) \equiv 2 \pmod 4. \tag{11}$$

However, the relation

$$G_e(1) + G_o(1) = G(1) \equiv 0 \pmod 4$$

implies, by Equation (11), that $2G_e(1) \equiv 2 \pmod 4$. This leads to a contradiction since $G_e(1)$ is even. Thus, $G(-1) \equiv 0 \pmod 4$, as asserted. Consequently,

$$f(-1) = g_2(-1)^2 = G(-1)^2 \equiv 0 \pmod{16}.$$

The lemma follows. □

Let us illustrate how Lemma 4 helps us to determine the parity of m where $2m = \deg f$. This significantly simplifies our computations when $f(1) = 12$. Suppose that $f(1) = 12$ and $f(x^2)$ is reducible. Since $f(x)$ is irreducible, we have $f(-1) = g_2(-1)^2 > 0$. However, $f(-1) < f(1) = 12$ implies $f(-1) \not\equiv 0 \pmod{16}$. The conclusion of Lemma 4 then implies that $g_2(1) \equiv 2 \pmod 4$. Given $12 = f(1) = g_e(1)^2 - g_o(1)^2$, we have

$$g_e(1)^2 - g_o(1)^2 \equiv -4 \pmod{16}.$$

This implies $g_e(1) \equiv 0 \pmod 4$ and $g_o(1) \equiv 2 \pmod 4$. Consequently, $g_e(x) = g_1(x)$ and $g_o(x) = g_2(x)$, with $\deg g_o = m - \ell$ being even. Therefore, if $f(1) = 12$, we deduce that m is odd.

While discussing our strategy in Section 1, we proposed reducing our problem to a certain polynomial congruence $F_L(x) \equiv F_R(x) \pmod 2$. We will accomplish this over the next few passages.

Lemma 5. *Let $h(x) \in \mathbb{Z}[x]$ be a reciprocal polynomial with $\deg h = n > 0$. Set $d = \lfloor (\deg h)/2 \rfloor$ where $\lfloor x \rfloor$ denotes the greatest integer not exceeding x. Then, there is a unique polynomial $u(x) \in \mathbb{Z}[x]$ with $\deg u < n/2$, and unique integers $M > n/2$ and a, such that $h(x)$ can be expressed as*

$$h(x) = x^M \widetilde{u}(x) + ax^d + u(x).$$

Furthermore, $a = 0$ whenever $h(1)$ is even. In particular, $a = 0$ if n is odd.

Proof. Let $h(x)$, n, and d be as stated in the lemma. Clearly, $h(x)$ is not a monomial. We consider the different cases depending on whether n is even or odd. First, consider that n is even. In that case, $n = 2d$. Since $h(x)$ is reciprocal, there is a nonnegative integer s, nonzero integers $a_0, a_1, \ldots, a_s$, and integers $d = d_0 > d_1 > \cdots > d_s > 0$, such that

$$h(x) = \sum_{j=0}^{s} a_j x^{d+d_j} + ax^d + \sum_{j=0}^{s} a_j x^{d-d_j}$$

for some $a \in \mathbb{Z}$. We take

$$u(x) = \sum_{j=0}^{s} a_j x^{d-d_j} \quad \text{and} \quad M = d + d_s.$$

Thus, $\deg u = d - d_s < d = n/2$ and $M = d + d_s > d = n/2$, so that

$$x^M \widetilde{u}(x) = x^{d+d_s} \sum_{j=0}^{s} a_j x^{d_j - d_s} = \sum_{j=0}^{s} a_j x^{d+d_j}.$$

The assertion now follows in this case.

Next, suppose n is odd. In this case, $n = 2d + 1$. With the above notation, we express $h(x)$ as

$$h(x) = \sum_{j=0}^{s} a_j x^{d+1+d_j} + \sum_{j=0}^{s} a_j x^{d-d_j}.$$

The assertion of the lemma follows after taking $u(x) = \sum_{j=0}^{s} a_j x^{d-d_j}$ and $M = d + 1 + d_s$. □

For future reference, note that if we set $\deg u = q$ in the proof of Lemma 5, then $M = n - q$. To see this, first observe that $d_s = d - q$. Accordingly,

$$M = d + d_s + \delta = 2d - q + \delta,$$

where $\delta = 0$ if n is even, and $\delta = 1$ otherwise. Our assertion follows upon observing that $n = 2d + \delta$.

Let $f(x) \in \mathscr{N}_{\text{irred}}$ be a reciprocal polynomial of degree $2m$. Let $f_e(x)$, $f_o(x)$, and ℓ be as defined in Equation (7). According to Lemma 5, for each $j \in \{e, o\}$, there are integers M_j, a_j, d_j, and a polynomial $u_j(x) \in \mathscr{N}$, such that

$$f_j(x) = x^{M_j} \widetilde{u}_j(x) + a_j x^{d_j} + u_j(x), \tag{12}$$

where $d_j = \lfloor (\deg f_j)/2 \rfloor$, and $a_j = 0$ if either $\deg f_j$ is odd or if $f_j(1)$ is even. Furthermore, $\deg u_j < (\deg f_j)/2 < M_j$.

Now, suppose that $f(x^2)$ is reducible. Then, Equation (8) implies that

$$f_e(x^2) + x^\ell f_o(x^2) \equiv f_e(x)^2 - x^\ell f_o(x)^2 \pmod 4. \tag{13}$$

By substituting $f_e(x)$ and $f_o(x)$ from Equation (12) into Equation (13), we obtain

$$\begin{aligned}
x^{2M_e}\widetilde{u}_e(x^2) &+ a_e x^{2d_e} + u_e(x^2) + x^{2M_o+\ell}\widetilde{u}_o(x^2) + a_o x^{2d_o+\ell} + x^\ell u_o(x^2) \\
&\equiv (x^{M_e}\widetilde{u}_e(x) + a_e x^{d_e} + u_e(x))^2 \\
&\quad - x^\ell (x^{M_o}\widetilde{u}_o(x) + a_o x^{d_o} + u_o(x))^2 \\
&\equiv x^{2M_e}\widetilde{u}_e(x)^2 + a_e x^{2d_e} + u_e(x)^2 \\
&\quad + 2a_e x^{M_e+d_e}\widetilde{u}_e(x) + 2a_e x^{d_e} u_e(x) \\
&\quad + 2x^{M_e}\widetilde{u}_e(x)u_e(x) - x^{2M_o+\ell}\widetilde{u}_0(x)^2 \\
&\quad - x^\ell u_o(x)^2 - 2a_o x^{M_o+d_o+\ell}\widetilde{u}_o(x) - a_o x^{2d_o+\ell} \\
&\quad - 2a_o x^{d_o+\ell} u_o(x) - 2x^{M_o+\ell}\widetilde{u}_o(x)u_o(x) \pmod 4.
\end{aligned} \tag{14}$$

We will next compare the terms on the two extreme sides of Equation (14) that have degrees less than m. Recall that $M_e > (\deg f_e)/2 = m/2$. Thus, $2M_e > m$. Furthermore, $d_e = \lfloor (\deg f_e)/2 \rfloor > m/2 - 1$. Therefore,

$$M_e + d_e > \frac{m}{2} + \frac{m}{2} - 1 = m - 1.$$

Similarly, $M_o > (\deg f_o)/2 = (m-\ell)/2$ implies $2M_o + \ell > m$. Additionally,

$$d_o = \left\lfloor \frac{\deg f_o}{2} \right\rfloor > \frac{m-\ell}{2} - 1.$$

Therefore, $M_o + d_o + \ell > m - 1$. Consider for each $j \in \{e, o\}$,

$$d_j + \deg u_j < \frac{\deg f_j}{2} + \frac{\deg f_j}{2} = \deg f_j.$$

Thus, $d_e + \deg u_e < m$ and $d_o + \deg u_o < m - \ell$. Lastly, we observe that the expression

$$2d_o + \ell = 2\left\lfloor \frac{m-\ell}{2} \right\rfloor + \ell \tag{15}$$

equals m if $m - \ell$ is even, and equals $m - 1$ if $m - \ell$ is odd. In the latter case, $a_o = 0$.

If $u(x) = \sum_{i=0}^{d} x^{e_j}$, where $e_0 < e_1 < \cdots < e_d$ are nonnegative integers, then

$$u(x)^2 = u(x^2) + 2L_u(x),$$

where $L_u(x) = \sum_{0 \le i < j \le d} x^{e_i + e_j}$. Moreover, $\deg L_u < 2 \deg u$. Accordingly,

$$\deg L_{u_e} < m \quad \text{and} \quad \deg L_{u_o} < m - \ell.$$

For a polynomial $h(x) \in \mathbb{Z}[x]$ and an integer $k > 0$, let $(h(x))_k \in \mathbb{Z}[x]$ denote the remainder $h(x) \pmod{x^k}$. Next, we substitute $u_e(x)^2$ and $u_o(x)^2$ in Equation (14) with $u_e(x^2) + 2L_{u_e}(x)$ and $u_o(x^2) + 2L_{u_o}(x)$, respectively. After rearranging terms and ignoring those possessing degrees greater than or equal to m, we obtain

$$\begin{aligned} L_{u_e}(x) + a_e x^{d_e} u_e(x) + \left(x^{M_e} \widetilde{u}_e(x) u_e(x)\right)_m \\ \equiv x^{\ell} u_o(x^2) + x^{\ell} L_{u_o}(x) + a_o x^{d_o + \ell} u_o(x) + \left(a_o x^{2d_o + \ell}\right)_m \\ + \left(x^{M_o + \ell} \widetilde{u}_o(x) u_o(x)\right)_m \pmod 2. \end{aligned} \tag{16}$$

Recall that $u_j(x)$ is a $0,1$-polynomial for $j \in \{e, o\}$. If $u_e(x)$ or $u_o(x)$ are not identically zero, we let

$$u_e(x) = 1 + \sum_{i=1}^{s} x^{n_i} \quad \text{and} \quad u_o(x) = 1 + \sum_{i=1}^{t} x^{m_j}, \tag{17}$$

where

$$n_s = \deg u_e < \left\lfloor \frac{\deg f_e}{2} \right\rfloor \leq \frac{m}{2} < M_e,$$

and

$$m_t = \deg u_o < \left\lfloor \frac{\deg f_o}{2} \right\rfloor < M_o. \tag{18}$$

Furthermore,

$$M_e = \deg f_e - \deg u_e = m - n_s \tag{19}$$

and

$$M_o = \deg f_o - \deg u_o = m - \ell - m_t. \tag{20}$$

Now, suppose both $u_e(x)$ and $u_o(x)$ are nonzero. If m is even, then $m - \ell$ is odd, in which case $a_o = 0$. Additionally, in this case $d_e = m/2$ and $d_o = (m - \ell - 1)/2$. Eliminating M_e and M_o from Equation (16) using Equation (19) and Equation (20), and noting that $2d_o + \ell = m$ (see Equation (15)), we obtain

$$\begin{aligned} L_{u_e}(x) + a_e x^{d_e} u_e(x) + x^{m-n_s} \left(\widetilde{u}_e(x) u_e(x)\right)_{n_s} \\ \equiv x^\ell u_o(x^2) + x^\ell L_{u_o}(x) + x^{m-m_t} \left(\widetilde{u}_o(x) u_o(x)\right)_{m_t} \pmod 2. \end{aligned} \tag{21}$$

One computes that

$$\left(\widetilde{u}_e(x) u_e(x)\right)_{n_s} = 1 + \sum_{j=1}^{s} x^{n_j} + \sum_{j=1}^{s-1} x^{n_s - n_j} + \sum_{1 \leq i < j < s} x^{n_s - n_j + n_i} \tag{22}$$

and

$$\left(\widetilde{u}_o(x) u_o(x)\right)_{m_t} = 1 + \sum_{j=1}^{t} x^{m_j} + \sum_{j=1}^{t-1} x^{m_t - m_j} + \sum_{1 \leq i < j < t} x^{m_t - m_j + m_i}. \tag{23}$$

Rewriting Equation (21) by substituting the corresponding expressions from Equation (22) and Equation (23), we get

$$\begin{aligned} \sum_{j=1}^{s} x^{n_j} + \sum_{1 \leq i < j \leq s} x^{n_i + n_j} + a_e x^{m/2} + a_e \sum_{j=1}^{s} x^{m/2 + n_j} \\ + \sum_{j=1}^{s} x^{m - n_j} + \sum_{1 \leq i < j \leq s} x^{m - n_j + n_i} \\ \equiv x^\ell + \sum_{j=1}^{t} x^{m_j + \ell} + \sum_{j=1}^{t} x^{2m_j + \ell} + \sum_{1 \leq i < j \leq t} x^{m_i + m_j + \ell} \\ + \sum_{j=1}^{t} x^{m - m_j} + \sum_{1 \leq i < j \leq t} x^{m - m_j + m_i} \pmod 2. \end{aligned} \tag{24}$$

Next, consider the case where m is odd. In this scenario, $\deg f_o = m - \ell$ is even, so $2d_o + \ell = m$. Additionally, $a_e = 0$ since $\deg f_e = m$ is odd. Accordingly, Equation (16) becomes

$$L_{u_e}(x) + x^{m-n_s}\left(\widetilde{u}_e(x)u_e(x)\right)_{n_s} \equiv x^\ell u_o(x^2) + x^\ell L_{u_o}(x) + a_o x^{(m+\ell)/2} u_o(x) + x^{m-m_t}\left(\widetilde{u}_o(x)u_o(x)\right)_{m_t} \pmod 2.$$

Proceeding as we did for even m, we obtain

$$\begin{aligned}\sum_{j=1}^{s} x^{n_j} + \sum_{1\le i<j\le s} x^{n_i+n_j} + \sum_{j=1}^{s} x^{m-n_j} + \sum_{1\le i<j\le s} x^{m-n_j+n_i}\\ \equiv x^\ell + \sum_{j=1}^{t} x^{m_j+\ell} + \sum_{j=1}^{t} x^{2m_j+\ell} + a_o x^{(m+\ell)/2}\\ + a_o \sum_{j=1}^{s} x^{(m+\ell)/2+m_j} + \sum_{1\le i<j\le t} x^{m_i+m_j+\ell}\\ + \sum_{j=1}^{t} x^{m-m_j} + \sum_{1\le i<j\le t} x^{m-m_j+m_i} \pmod 2.\end{aligned} \tag{25}$$

We have now obtained the polynomials $F_L(x)$ and $F_R(x)$ we were seeking. Let $F_L(x)$ and $F_R(x)$ represent the polynomials on the left and right sides of Equation (24) if m is even, and Equation (25) if m is odd. The exponents of x appearing in $F_L(x)$ and $F_R(x)$ are unknowns. We will match these exponents by their sizes and parities in $F_L(x) \equiv F_R(x) \pmod 2$. For instance, if we can identify the smallest (or largest) exponents in both $F_L(x)$ and $F_R(x)$, then they must be equal. Additionally, the total number of exponents of a fixed parity in $F_L(x)$ and $F_R(x)$ combined is always even. Our subsequent arguments are primarily based on these two observations.

Observe that for every $i, j, k \in \{1, 2, \ldots, s\}$ with $k < j$, one has

$$n_i \le n_s < m/2 < m - n_j < m - n_j + n_k.$$

This implies that n_1 and n_2 are, respectively, the smallest and the second smallest exponents on the left sides of both Equation (24) and Equation (25). Similarly, since $\ell < m/2$ (by Lemma 3), the smallest and the second smallest exponents on the right sides of both Equation (24) and Equation (25) are ℓ and $m_1 + \ell$, respectively. Therefore,

$$n_1 = \ell \quad \text{and} \quad n_2 = m_1 + \ell. \tag{26}$$

Proof of Theorem 1. Suppose that $f(x)$ is an irreducible reciprocal $0,1$-polynomial such that $f(x^2)$ is reducible. Further, assume that $f(x)$ has $Q \le 14$ terms. As previously explained, considering $Q \in \{5, 7, 9, 11, 12, 13\}$ suffices. Let $f_e(x)$, $f_o(x)$, and ℓ be as defined in Equation (7). Additionally, let $n_e = f_e(1)$ and $n_o = f_o(1)$. Thus,

$$Q = f(1) = n_e + n_o \quad \text{and} \quad f(-1) = n_e - n_o.$$

For $j \in \{e, o\}$, let M_j, $u_j(x)$, d_j, and a_j have the same meaning as implied in Lemma 5. As noted earlier, exactly one of the integers $\deg f_e$ and $\deg f_o$ is odd. As such, either $a_e = 0$ or $a_o = 0$.

Recall that $f(-1)$ is a square of a nonzero integer in the cases under consideration. Specifically, if $f(1) = 12$, then $n_e + n_o = 12$ and $n_e - n_o = 4$ ($n_e - n_o = 0$ would imply that $f(-1) = 0$, which contradicts the irreducibility of $f(x)$). Therefore, $n_e = 8$ and $n_o = 4$. Given that $f_j(1) = 2u_j(1) + a_j$ for each $j \in \{e, o\}$, it follows from the previous observation that $a_e = a_o = 0$ when $f(1) = 12$. Additionally, as explained in the comments following the proof of Lemma 4, m is odd. In the remaining cases,

$$n_e + n_o \in \{5, 7, 9, 11, 13\} \quad \text{and} \quad n_e - n_o \in \{1, 9\}.$$

From $n_j = f_j(1) = 2u_j(1) + a_j$ for every $j \in \{e, o\}$, it follows that n_j is odd if and only if $a_j = 1$. Since $a_j = 0$ if $\deg f_j$ is odd, we deduce that if n_j is odd, then $a_j = 1$, implying $\deg f_j$ is even. Specifically, if n_e is odd, then $a_e = 1$, and hence, $m = \deg f_e$ is even. Additionally, $a_o = 0$, n_o is even, and $\deg f_o = m - \ell$ is odd. Similarly, if n_o is odd, then $a_o = 1$, and hence, $\deg f_o = m - \ell$ is even. In particular, m is odd. Moreover, $a_e = 0$, n_e is even, and $\deg f_e = m$ is odd. To summarize,

$$m \equiv n_o \pmod 2.$$

Based on this information, we obtain the following eight possibilities for n_e, $u_e(1)$, a_e, n_o, $u_o(1)$, a_o, and the corresponding parities of m.

(i) If $f(1) = 5$, then $f(-1) = 1$; $n_e = 3$, $n_o = 2$; $u_e(1) = 1$, $u_o(1) = 1$; $a_e = 1$, $a_o = 0$, and $m \equiv 0 \pmod 2$

(ii) If $f(1) = 7$, then $f(-1) = 1$; $n_e = 4$, $n_o = 3$; $u_e(1) = 2$, $u_o(1) = 1$; $a_e = 0$, $a_o = 1$, and $m \equiv 1 \pmod 2$

(iii) If $f(1) = 9$, then $f(-1) = 1$; $n_e = 5$, $n_o = 4$; $u_e(1) = 2$, $u_o(1) = 2$; $a_e = 1$, $a_o = 0$, and $m \equiv 0 \pmod 2$

(iv) If $f(1) = 11$, and $f(-1) = 9$, then $n_e = 10$, $n_o = 1$; $u_e(1) = 5$, $u_o(1) = 0$; $a_e = 0$, $a_o = 1$, and $m \equiv 1 \pmod 2$

(v) If $f(1) = 11$, and $f(-1) = 1$, then $n_e = 6$, $n_o = 5$; $u_e(1) = 3$, $u_o(1) = 2$; $a_e = 0$, $a_o = 1$, and $m \equiv 1 \pmod 2$

(vi) If $f(1) = 12$, and $f(-1) = 4$, then $n_e = 8$, $n_o = 4$; $u_e(1) = 4$, $u_o(1) = 2$; $a_e = a_o = 0$, and $m \equiv 1 \pmod 2$

(vii) If $f(1) = 13$, and $f(-1) = 9$, then $n_e = 11$, $n_o = 2$; $u_e(1) = 5$, $u_o(1) = 1$; $a_e = 1$, $a_o = 0$, and $m \equiv 0 \pmod 2$

(viii) If $f(1) = 13$, and $f(-1) = 1$, then $n_e = 7$, $n_o = 6$; $u_e(1) = 3$, $u_o(1) = 3$; $a_e = 1$, $a_o = 0$, and $m \equiv 0 \pmod 2$

We consider (i) – (viii) separately. In each case, we first determine the corresponding forms of $u_e(x)$ and $u_o(x)$ as given by Equation (17), based on the values of $u_e(1)$ and $u_o(1)$. Then, we proceed to match the degrees of terms on both sides of Equation (24) or Equation (25), depending on whether m is even or odd.

`Case (i).` If $f(1) = 5$, then $u_e(x)$ and $u_o(x)$ are both identically 1. Thus, $n_s = 0 = m_t$. Consequently, from Equation (19) and Equation (20), we have $M_e = m$ and $M_o = m - \ell$. Also, $d_e = m/2$. Therefore, $f_e(x) = x^m + x^{m/2} + 1$ and $f_o(x) = x^{m-\ell} + 1$. Accordingly,

$$f(x) = x^{2m} + x^{2m-\ell} + x^{m/2} + x^{\ell} + 1. \tag{27}$$

Furthermore, in this scenario, Equation (24) transforms into

$$x^{m/2} \equiv x^{\ell} \pmod 2.$$

It follows that $m = 2\ell$. Setting $m = 2\ell$ in Equation (27), we obtain

$$f(x) = x^{4\ell} + x^{3\ell} + x^{2\ell} + x^{\ell} + 1 = \Phi_5(x^{\ell}).$$

This settles the case that $f(1) = 5$.

`Case (ii).` Next, consider the case where $f(1) = 7$. In this case, $u_o(x) = 1$ and $u_e(x) = 1 + x^{n_1} = 1 + x^{\ell}$ (by Equation (26)). Furthermore, based on Equation (19) and Equation (20), we find that $M_e = m - n_1 = m - \ell$ and $M_o = m - \ell$. Additionally, $d_o = (m - \ell)/2$. Thus,

$$f_e(x) = x^{m-\ell}(x^{\ell} + 1) + x^{\ell} + 1 = x^m + x^{m-\ell} + x^{\ell} + 1 \tag{28}$$

and

$$f_o(x) = x^{m-\ell} + x^{(m-\ell)/2} + 1. \tag{29}$$

Since m is odd, we consider Equation (25), which transforms into

$$x^{\ell} + x^{m-\ell} \equiv x^{\ell} + x^{(m+\ell)/2} \pmod 2.$$

We deduce that $m - \ell = (m + \ell)/2$. Therefore, $m = 3\ell$. Setting $m = 3\ell$ in Equation (28) and Equation (29), we find that $f_e(x) = x^{3\ell} + x^{2\ell} + x^{\ell} + 1$, and $f_o(x) = x^{2\ell} + x^{\ell} + 1$. In that scenario,

$$\begin{aligned} f(x) &= x^{6\ell} + x^{4\ell} + x^{2\ell} + 1 + x^{\ell}(x^{4\ell} + x^{\ell} + 1) \\ &= x^{6\ell} + x^{5\ell} + x^{4\ell} + x^{3\ell} + x^{2\ell} + x^{\ell} + 1 = \Phi_7(x^{\ell}), \end{aligned}$$

and the present case is settled.

To streamline our presentation, from now on, we will represent the polynomial $x^{d_1} + x^{d_2} + \cdots + x^{d_r}$ by the tuple $[d_1, d_2, \ldots, d_r]$, without imposing any specific ordering of the entries. Rewriting Equation (24) and Equation (25) in tuple notation, we obtain, respectively,

$$\begin{aligned}\Big[&(n_j)_j, (n_i+n_j)_{i<j}, a_e m/2, a_e (m/2+n_j)_j, \\ &(m-n_j)_j, (m-n_j+n_i)_{i<j} \Big] \\ &= \Big[\ell, (m_j+\ell)_j, (2m_j+\ell)_j, (m_i+m_j+\ell)_j, \\ &\quad (m-m_j)_j, (m-m_j+m_i)_{i<j}\Big]\end{aligned} \tag{30}$$

and

$$\begin{aligned}\Big[&(n_j)_j, (n_i+n_j)_{i<j}, (m-n_j)_j, (m-n_j+n_i)_{i<j} \Big] \\ &= \Big[\ell, (m_j+\ell)_j, (2m_j+\ell)_j, a_o(m+\ell)/2, \\ &\quad a_o ((m+\ell)/2+m_j)_j, (m_i+m_j+\ell)_j, \\ &\quad (m-m_j)_j, (m-m_j+m_i)_{i<j}\Big],\end{aligned} \tag{31}$$

where each indexed parenthesis represents the collection of exponents of terms in a specific sum within Equation (24) and Equation (25). For brevity, we have omitted the condition (mod 2) from Equation (30) and Equation (31).

`Case (iii).` In the case where $f(1) = 9$, one finds that

$$u_e(x) = 1 + x^{n_1} = 1 + x^{\ell} \quad \text{and} \quad u_o(x) = 1 + x^{m_1}.$$

From Equation (19) and Equation (20), we deduce that

$$M_e = m - n_1 = m - \ell \quad \text{and} \quad M_o = m - \ell - m_1.$$

Additionally, $d_e = m/2$, $a_e = 1$, and $a_o = 0$ here. Thus, we can express $f_e(x)$ and $f_o(x)$ as

$$f_e(x) = x^{m-\ell}(x^{\ell}+1) + x^{m/2} + x^{\ell} + 1 = x^m + x^{m-\ell} + x^{m/2} + x^{\ell} + 1 \tag{32}$$

and

$$f_o(x) = x^{m-\ell-m_1}(x^{m_1}+1) + x^{m_1} + 1 = x^{m-\ell} + x^{m-\ell-m_1} + x^{m_1} + 1. \tag{33}$$

Since m is even here, canceling the common terms ℓ and n_1 from Equation (30), we obtain

$$[m/2, m/2+\ell, m-\ell] = [m_1+\ell, 2m_1+\ell, m-m_1]. \tag{34}$$

Recall that $m_1 < (\deg f_o)/2 = (m-\ell)/2$ (from Equation (18)). Accordingly, the smallest exponent appearing on the right side of Equation (34) is $m_1 + \ell$. Furthermore, based on Lemma 3, which states that $\ell < m/2$, we deduce that $m/2$ is the smallest exponent on the left side of Equation (34). It follows that $m/2 = m_1 + \ell$, leading to $m = 2m_1 + 2\ell$. Substituting m by $2m_1 + 2\ell$ in Equation (32) and Equation (33), one obtains

$$f_e(x) = x^{2m_1+2\ell} + x^{2m_1+\ell} + x^{m_1+\ell} + x^{\ell} + 1,$$

and

$$f_o(x) = x^{2m_1+\ell} + x^{m_1+\ell} + x^{m_1} + 1.$$

Accordingly, from Equation (7), we get that

$$f(x) = x^{4m_1+4\ell} + x^{4m_1+3\ell} + x^{4m_1+2\ell} + x^{2m_1+3\ell} + x^{2m_1+2\ell} + x^{2m_1+\ell} + x^{2\ell} + x^{\ell} + 1.$$

It can be verified that $f(x) = \Phi_3(x^{2\ell})\Phi_3(x^{2m_1+\ell})$. This settles the present case.

`Case (iv).` Next, consider the case where $f(1) = 11$ and $f(-1) = 9$. From (iv), we find that $u_o(x) \equiv 1$, and $a_o = 1$. Thus,

$$u_e(x) = 1 + x^{\ell} + x^{n_2} + x^{n_3} + x^{n_4}.$$

After eliminating the common terms ℓ and n_1 from Equation (31), we find that n_2 is the smallest exponent on the left side of Equation (31), while the right side of Equation (31) comprises a single term, $(m+\ell)/2$. Since, $n_2 < m/2$, the term x^{n_2} remains intact in Equation (25), leading to a contradiction.

`Case (v).` Next, suppose that $f(1) = 11$ and $f(-1) = 1$. In this case, one verifies that

$$u_e(x) = 1 + x^{n_1} + x^{n_2} = 1 + x^{\ell} + x^{m_1+\ell}$$

and

$$u_o(x) = 1 + x^{m_1}.$$

Additionally, from Equation (19) and Equation (20), we have

$$M_e = m - n_2 = m - m_1 - \ell \quad \text{and} \quad M_o = m - \ell - m_1.$$

Furthermore, $d_o = (m-\ell)/2$, $a_o = 1$, and $a_e = 0$ here. We use Equation (26) to cancel ℓ with n_1, and $m_1 + \ell$ with n_2 in Equation (31), to obtain

$$\begin{aligned}&[m_1 + 2\ell, m - \ell, m - \ell - m_1, m - m_1]\\ &\quad = [2m_1 + \ell, (m+\ell)/2, (m+\ell)/2 + m_1, m - m_1].\end{aligned}$$

After eliminating $m - m_1$, we have

$$[m_1 + 2\ell, m - \ell, m - \ell - m_1] = [2m_1 + \ell, (m+\ell)/2, (m+\ell)/2 + m_1]. \tag{35}$$

Recall that m and ℓ are odd in the present case. Thus, if m_1 is even, then all the exponents on the left of Equation (35) are even. Conversely, there is at least one odd exponent on the right side. Specifically, $2m_1+\ell$. Thus, one of the integers $(m+\ell)/2$ and $(m+\ell)/2+m_1$ is odd. Since m_1 is even, we deduce that both $(m+\ell)/2$ and $(m+\ell)/2+m_1$ are odd. However, this results in having three even exponents on the left side and three odd exponents on the right side of Equation (35). Consequently, at least one even (respectively, one odd) power of x remains intact on the left (respectively, right) side of Equation (25), which is impossible.

It follows that m_1 is odd. In that event, $m-\ell$ is the only even exponent on the left side of Equation (35). The possible even exponents on the right side of Equation (35) are $(m+\ell)/2$ or $(m+\ell)/2+m_1$, but not both. We consider the two possibilities separately.

If $(m+\ell)/2$ is even, then $m-\ell=(m+\ell)/2$. This implies $m=3\ell$. In that event,

$$(m+\ell)/2+m_1=m_1+2\ell.$$

Consequently, $m-\ell-m_1=2m_1+\ell$ in Equation (35) whence, $\ell=3m_1$. Now, expressing M_e, M_o (using Equation (19) and Equation (20)), and d_o (using Equation (15)) in terms of m_1, we have

$$M_e=M_o=m-m_1-\ell=5m_1 \quad \text{and} \quad d_o=(m-\ell)/2=3m_1.$$

Based on the information one obtains

$$\begin{aligned} f_e(x)&=x^{5m_1}(1+x^{m_1}+x^{4m_1})+(1+x^{3m_1}+x^{4m_1})\\ &=x^{9m_1}+x^{6m_1}+x^{5m_1}+x^{4m_1}+x^{3m_1}+1, \end{aligned}$$

and

$$f_o(x)=x^{5m_1}(1+x^{m_1})+x^{3m_1}+x^{m_1}+1=x^{6m_1}+x^{5m_1}+x^{3m_1}+x^{m_1}+1.$$

Accordingly,

$$\begin{aligned} f(x)=x^{18m_1}&+x^{15m_1}+x^{13m_1}+x^{12m_1}+x^{10m_1}+x^{9m_1}\\ &+x^{8m_1}+x^{6m_1}+x^{5m_1}+x^{3m_1}+1. \end{aligned}$$

It is easily verified that $f(\zeta)=0$ where $\zeta=e^{2\pi i/11m_1}$.

Next, consider the possibility that

$$m-\ell=(m+\ell)/2+m_1.$$

In this case, $m-\ell-m_1=(m+\ell)/2$. Consequently, we have $m_1+2\ell=2m_1+\ell$ in Equation (35). This simplifies to $m_1=\ell$. Substituting this into $m-\ell=(m+\ell)/2+m_1$, we find that $m=5\ell$. Thus,

$$u_e(x)=1+x^{\ell}+x^{2\ell},$$

and

$$u_o(x) = 1 + x^{\ell}.$$

It is not hard to show from here that $f(x) = \Phi_{11}(x^{\ell})$. We omit the details.

`Case (vi).` Next, if $f(1) = 12$, then

$$u_e(x) = 1 + x^{n_1} + x^{n_2} + x^{n_3}$$

and

$$u_o(x) = 1 + x^{m_1}.$$

Recall that m is odd in the present scenario. We proceed as before by eliminating the terms ℓ and $m_1 + \ell$ from Equation (31), to obtain

$$\begin{aligned}&[n_3, n_1 + n_2, n_1 + n_3, n_2 + n_3, m - n_1, m - n_2, m - n_3,\\ &\quad m - n_2 + n_1, m - n_3 + n_1, m - n_3 + n_2]\\ &\qquad = [2m_1 + \ell, m - m_1].\end{aligned}$$

Based on Equation (26), we have $m - n_2 + n_1 = m - m_1$. By canceling these terms above, we get

$$\begin{aligned}&[n_3, n_1 + n_2, n_1 + n_3, n_2 + n_3, m - n_1, m - n_2, m - n_3,\\ &\quad m - n_3 + n_1, m - n_3 + n_2]\\ &\qquad = [2m_1 + \ell].\end{aligned} \tag{36}$$

Next, we search for the biggest exponent L on the left side above. To this end, we note that $m - n_3 + n_2 > n_3 + n_2$ since $n_3 < m/2$. So, the probable candidates for L are $m - n_1$ and $m - n_3 + n_2$. We consider the three cases: $m - n_1 > m - n_3 + n_2$, $m - n_3 + n_2 > m - n_1$, and $m - n_3 + n_2 = m - n_1$. In the first case, Equation (36) implies $m - n_1 = 2m_1 + \ell$, which simplifies to

$$m = 2m_1 + \ell + n_1 = 2m_1 + 2\ell.$$

However, this is absurd since m is odd.

Next, if $m - n_3 + n_2 > m - n_1$, then $m - n_3 + n_2 = 2m_1 + \ell$. In this scenario,

$$m = n_3 - n_2 + 2m_1 + \ell = n_3 - m_1 - \ell + 2m_1 + \ell = n_3 + m_1,$$

where, we have used that $n_2 = m_1 + \ell$ from Equation (26). This, in turn, implies that

$$n_3 + m_1 = m > 2n_2 = 2m_1 + 2\ell.$$

In other words, $n_3 > m_1 + 2\ell$. On the other hand, $m - n_3 + n_2 > m - n_1$ implies that $n_3 < n_1 + n_2 = m_1 + 2\ell$, leading to a contradiction.

Thus, we are left with the possibility that $m - n_3 + n_2 = m - n_1$. In that event, Equation (26) implies $n_3 = n_1 + n_2 = m_1 + 2\ell$. By substituting n_1 with ℓ, n_2 with $m_1 + \ell$, and n_3 with $m_1 + 2\ell$ in Equation (36), we get

$$\begin{aligned}&[m_1 + 2\ell, m_1 + 2\ell, m_1 + 3\ell, 2m_1 + 3\ell, m - \ell, m - m_1 - \ell,\\ &\quad m - m_1 - 2\ell, m - m_1 - \ell, m - \ell]\\ &\qquad = [2m_1 + \ell].\end{aligned}$$

Eliminating the common exponents on the left side above, we obtain

$$[m_1 + 3\ell, 2m_1 + 3\ell, m - m_1 - 2\ell] = [2m_1 + \ell]. \tag{37}$$

Since $2m_1 + 3\ell$ is bigger than both $m_1 + 3\ell$ and $2m_1 + \ell$, Equation (37) leaves us with the possibility that

$$2m_1 + 3\ell = m - m_1 - 2\ell.$$

Therefore, $m = 3m_1 + 5\ell$. Additionally, from Equation (37), we get that $m_1 + 3\ell = 2m_1 + \ell$. Thus, $m_1 = 2\ell$, and

$$m = 3m_1 + 5\ell = 11\ell \quad \text{and} \quad n_2 = m_1 + \ell = 3\ell.$$

Accordingly, one computes that $n_3 = m_1 + 2\ell = 4\ell$. Thus, $\deg u_e = n_3 = 4\ell$ and $\deg u_o = m_1 = 2\ell$. We further determine from Equation (19) and Equation (20) that $M_e = m - n_3 = 7\ell$ and $M_o = m - \ell - m_1 = 8\ell$. Thus,

$$u_e(x) = 1 + x^{\ell} + x^{3\ell} + x^{4\ell} \quad \text{and} \qquad u_o(x) = 1 + x^{2\ell}.$$

It is easily verified that

$$f_e(x) = (x^{7\ell} + 1)(x^{4\ell} + x^{3\ell} + x^{\ell} + 1) \quad \text{and} \quad f_o(x) = (x^{8\ell} + 1)(x^{2\ell} + 1).$$

Finally, one computes $f(x) = f_e(x^2) + x^{\ell} f_o(x^2)$, to obtain

$$f(x) = x^{22\ell} + x^{21\ell} + x^{20\ell} + x^{17\ell} + x^{16\ell} + x^{14\ell} + x^{8\ell} + x^{6\ell} + x^{5\ell} + x^{2\ell} + x^{\ell} + 1.$$

It is not hard to verify that $f(\zeta) = 0$, where $\zeta = e^{2\pi i/9\ell}$.

`Case (vii).` The scenario, where $f(1) = 13$ and $f(-1) = 9$, can be handled in a precisely similar manner as Case (iv). These details are omitted.

`Case (viii).` It remains to consider the case where $f(1) = 13$ and $f(-1) = 1$. One verifies that

$$u_e(x) = 1 + x^{\ell} + x^{m_1 + \ell} \quad \text{and} \quad u_o(x) = 1 + x^{m_1} + x^{m_2}.$$

Based on Equation (19) and Equation (20), we have

$$M_e = m - \ell - m_1 \quad \text{and} \quad M_o = m - \ell - m_2.$$

Additionally, $a_e = 1$, $a_o = 0$, and $d_e = m/2$. As before, we begin by canceling ℓ and $m_1 + \ell$ from Equation (30), to obtain

$$\begin{aligned}&[m_1 + 2\ell, m/2, m/2 + \ell, m/2 + \ell + m_1, m - \ell, m - \ell - m_1, m - m_1]\\ &\quad = [m_2 + \ell, 2m_1 + \ell, 2m_2 + \ell, m_1 + m_2 + \ell, m - m_1, m - m_2, m - m_2 + m_1].\end{aligned}$$

Eliminating $m - m_1$ from both sides above, we get

$$\begin{aligned}&[m_1 + 2\ell, m/2, m/2 + \ell, m/2 + \ell + m_1, m - \ell, m - \ell - m_1]\\ &\quad = [m_2 + \ell, 2m_1 + \ell, 2m_2 + \ell, m_1 + m_2 + \ell, m - m_2, m - m_2 + m_1].\end{aligned} \tag{38}$$

We analyze the various possible parities of m_1, m_2, and $m/2$. For a tuple of exponents $[d_1, d_2, \ldots, d_r]$, we consider the vector $(d'_1, d'_2, \ldots, d'_r) \in \mathbb{F}_2^r$ where $d_j \equiv d'_j$ (mod 2). Observe that if the equation

$$[d_1, d_2, \ldots, d_r] = [e_1, e_2, \ldots, e_k]$$

has a solution in positive integers d_i and e_j, then $r + k$ is even. Furthermore, considering parity, the total number of 0's (and hence, the total number of 1's) in the set $\{d'_1, d'_2, \ldots, d'_r, e'_1, e'_2, \ldots, e'_k\}$ is even. We will refer to two tuples of the same length as *equivalent* if they both reduce to the same vector over $\mathbb{F}_2$. We will establish a specific parity condition on m_1 and $m/2$ using these observations. Namely, that

$$m/2 \equiv m_1 \pmod{2}.$$

First, consider the case where $m_1 \equiv m_2$ (mod 2). Assume that $m_1 \equiv m_2 \not\equiv m/2$ (mod 2). The tuple $[m_1 + 2\ell, m/2, m/2 + \ell, m/2 + \ell + m_1, m - \ell, m - \ell - m_1]$ on the left side of Equation (38) is equivalent to the tuple

$$v = [m_1, m_1 + 1, m_1, 0, 1, m_1 + 1].$$

While the tuple $[m_2 + \ell, 2m_1 + \ell, 2m_2 + \ell, m_1 + m_2 + \ell, m - m_2, m - m_2 + m_1]$ on the right side of Equation (38) is equivalent to

$$w = [m_1 + 1, 1, 1, 1, m_1, 0].$$

If $m_1 \equiv 0 \pmod{2}$, the $\mathbb{F}_2$-vectors associated with v and w are respectively,

$$v' = (0, 1, 0, 0, 1, 1) \quad \text{and} \quad w' = (1, 1, 1, 1, 0, 0).$$

Thus, v' and w' together contain five, an odd number of zeros. As explained above, this implies that Equation (38) does not hold in this case.

If $m_1 \equiv 1 \pmod 2$, then

$$v' = (1, 0, 1, 0, 1, 0) \quad \text{and} \quad w' = (0, 1, 1, 1, 1, 0).$$

Once again, there are an odd number of zeros in v' and w', leading us to conclude that Equation (38) does not hold in this case. Thus, if $m_1 \equiv m_2 \pmod 2$, then $m_1 \equiv m_2 \equiv m/2 \pmod 2$.

Next, consider the case that $m_1 \not\equiv m_2 \pmod 2$. We claim that $m/2 \equiv m_1 \pmod 2$ in this scenario. Suppose instead that $m/2 \not\equiv m_1 \pmod 2$. One verifies that the equivalent tuples v and w, associated with the left and the right sides of Equation (38), respectively, are

$$v = [m_1, m_1 + 1, m_1, 0, 1, m_1 + 1] \quad \text{and} \quad w = [m_1, 1, 1, 0, m_1 + 1, 1].$$

We next consider the associated $\mathbb{F}_2$-vectors v' and w'. If $m_1 \equiv 0 \pmod 2$, then we easily verify that

$$v' = (0, 1, 0, 0, 1, 1) \quad \text{and} \quad w' = (0, 1, 1, 0, 1, 1).$$

We find that five zeros appear in v' and w' together. Accordingly, we discard this case. If $m_1 \equiv 1 \pmod 2$, then

$$v' = (1, 0, 1, 0, 1, 0) \quad \text{and} \quad w' = (1, 1, 1, 0, 0, 1).$$

Since there are five zeros in this case, our claim is settled by similar arguments.

Based on the preceding discussion, we have two possibilities outlined below.

$$m_1 \equiv m_2 \equiv m/2 \pmod 2 \quad \text{and} \quad m/2 \equiv m_1 \not\equiv m_2 \pmod 2.$$

First, suppose that $m_1 \equiv m_2 \equiv m/2 \equiv 0 \pmod 2$. Restricting our attention to the even exponents on the two sides of Equation (38), we find that

$$[m_1 + 2\ell, m/2] = [m - m_2, m - m_2 + m_1].$$

We eliminate this possibility as follows. Since $m_2 < m/2$, we have $m - m_2 > m/2$. Therefore, $m/2 = m - m_2 + m_1$, in which case, $m_2 = m/2 + m_1$, leading to a contradiction given that $m_2 < m/2$.

Next, suppose $m_1 \equiv m_2 \equiv m/2 \equiv 1 \pmod 2$. Restricting to the even exponents in Equation (38), this time, we obtain

$$[m/2 + \ell, m - \ell - m_1] = [m_2 + \ell, m - m_2 + m_1].$$

Since $m_2 < m/2$, we deduce that

$$m/2 + \ell = m - m_2 + m_1 \quad \text{and} \quad m - \ell - m_1 = m_2 + \ell.$$

Upon solving, we find that $m_2 = 3m_1$ and $2m_1 + \ell = m/2$. Now, rewriting Equation (38) with $m/2 = 2m_1 + \ell$ and $m_2 = 3m_1$, and ignoring the even exponents, we obtain

$$[m_1 + 2\ell, 2m_1 + \ell, 3m_1 + 2\ell, 4m_1 + \ell] = [2m_1 + \ell, 6m_1 + \ell, 4m_1 + \ell, m_1 + 2\ell].$$

Eliminating the common exponents, one obtains

$$3m_1 + 2\ell = 6m_1 + \ell.$$

This simplifies to $\ell = 3m_1$. Thus, $m = 10m_1$. Next, expressing the exponents of the terms of $u_e(x)$ and $u_o(x)$ in terms of m_1, we have

$$u_e(x) = 1 + x^{3m_1} + x^{4m_1} \quad \text{and} \quad u_o(x) = 1 + x^{m_1} + x^{3m_1}.$$

Additionally, from Equation (19) and Equation (20), we verify that

$$M_e = m - \ell - m_1 = 6m_1 \quad \text{and} \quad M_o = m - \ell - m_2 = 4m_1.$$

Finally, $d_e = m/2 = 5m_1$. Consequently,

$$\begin{aligned} f_e(x) &= x^{6m_1}(x^{4m_1} + x^{m_1} + 1) + x^{5m_1} + x^{4m_1} + x^{3m_1} + 1 \\ &= x^{10m_1} + x^{7m_1} + x^{6m_1} + x^{5m_1} + x^{4m_1} + x^{3m_1} + 1, \end{aligned}$$

and

$$\begin{aligned} f_o(x) &= x^{4m_1}(x^{3m_1} + x^{2m_1} + 1) + x^{3m_1} + x^{m_1} + 1 \\ &= x^{7m_1} + x^{6m_1} + x^{4m_1} + x^{3m_1} + x^{m_1} + 1. \end{aligned}$$

One further computes that

$$\begin{aligned} f(x) = x^{20m_1} &+ x^{17m_1} + x^{15m_1} + x^{14m_1} + x^{12m_1} + x^{11m_1} + x^{10m_1} \\ &+ x^{9m_1} + x^{8m_1} + x^{6m_1} + x^{5m_1} + x^{3m_1} + 1. \end{aligned}$$

Setting $\zeta = e^{2\pi i/13m_1}$, we find that $f(\zeta) = 0$.

Next, suppose $m/2 \equiv m_1 \not\equiv m_2 \pmod 2$. We start by considering the possibility that $m/2 \equiv m_1 \equiv 0 \pmod 2$ and $m_2 \equiv 1 \pmod 2$. Constraining ourselves to the even exponents in Equation (38), we have

$$[m_1 + 2\ell, m/2] = [m_2 + \ell, m_1 + m_2 + \ell].$$

We consider the two possibilities;

(A) $m_1 + 2\ell = m_2 + \ell$, and $m/2 = m_1 + m_2 + \ell$,

(B) $m/2 = m_2 + \ell$, and $m_1 + 2\ell = m_1 + m_2 + \ell$.

Set $q = m/2$. In case (A), $m_2 = m_1 + \ell$ and $q = 2(m_1 + \ell)$. Restricting to the odd exponents in Equation (38), we get

$$[2m_1 + 3\ell, 3m_1 + 3\ell, 4m_1 + 3\ell, 3m_1 + 3\ell] = [2m_1 + \ell, 2m_1 + 3\ell, 3m_1 + 3\ell, 4m_1 + 3\ell].$$

Comparing the smallest exponents above, we obtain $2m_1 + 3\ell = 2m_1 + \ell$, which is absurd since $\ell > 0$.

In case (B), we have $m_2 = \ell$, and $q = 2\ell$. Consider the odd exponents appearing in Equation (38). One has

$$[3\ell, m_1 + 3\ell, 3\ell, 3\ell - m_1] = [2m_1 + \ell, 3\ell, 3\ell, m_1 + 3\ell].$$

After canceling 3ℓ with $m_1 + 3\ell$, we deduce that $3\ell - m_1 = 2m_1 + \ell$. This, in particular, implies that 3 divides ℓ. Let $\ell = 3k$ where k is a positive integer. We conclude that $m_1 = 2k$. Additionally, we have $m_2 = \ell = 3k$ and $m = 4\ell = 12k$ in the current scenario. One can now compute that

$$u_e(x) = x^{5k} + x^{3k} + 1 \quad \text{and} \quad u_o(x) = x^{3k} + x^{2k} + 1,$$

and that

$$M_e = m - \deg u_e = m - 5k = 7k \quad \text{and} \quad M_o = m - \ell - \deg u_o = 6k.$$

Now, we can express $f_e(x)$ as

$$\begin{aligned} f_e(x) &= x^{M_e}\widetilde{u_e}(x) + a_e x^{m/2} + u_e(x) \\ &= x^{7k}(x^{5k} + x^{2k} + 1) + x^{6k} + x^{5k} + x^{3k} + 1 \\ &= x^{12k} + x^{9k} + x^{7k} + x^{6k} + x^{5k} + x^{3k} + 1. \end{aligned}$$

Similarly, one computes that

$$f_o(x) = x^{9k} + x^{7k} + x^{6k} + x^{3k} + x^{2k} + 1.$$

Finally,

$$\begin{aligned} f(x) &= f_e(x^2) + x^{\ell} f_o(x^2) \\ &= x^{24k} + x^{18k} + x^{14k} + x^{12k} + x^{10k} + x^{6k} + 1 \\ &\quad + x^{3k}(x^{18k} + x^{14k} + x^{12k} + x^{6k} + x^{4k} + 1) \\ &= x^{24k} + x^{21k} + x^{18k} + x^{17k} + x^{15k} + x^{14k} + x^{12k} \\ &\quad + x^{10k} + x^{9k} + x^{7k} + x^{6k} + x^{3k} + 1. \end{aligned}$$

It can be verified that $f(x)$ is divisible by $\Phi_{13}(x^k)$, and the assertion of the theorem follows in this case.

It remains to consider the case where $m/2 \equiv m_1 \equiv 1 \pmod 2$ and $m_2 \equiv 0 \pmod 2$. Restricting to the even exponents in Equation (38), now we have

$$[m/2 + \ell, m - \ell - m_1] = [m_1 + m_2 + \ell, m - m_2].$$

There are two possibilities here, specifically,

(C) $q + \ell = m_1 + m_2 + \ell$, and $m - \ell - m_1 = m - m_2$ and

(D) $q + \ell = m - m_2$, and $m - \ell - m_1 = m_1 + m_2 + \ell$,

where $q = m/2$. In the scenario (C), one has $m_2 = m_1 + \ell$ and $q = m_1 + m_2 = 2m_1 + \ell$. As before, we express the odd exponents in Equation (38) in terms of m_1 and ℓ, to get

$$[m_1 + 2\ell, 2m_1 + \ell, 3m_1 + 2\ell, 4m_1 + \ell] = [m_1 + 2\ell, 2m_1 + \ell, 2m_1 + 3\ell, 4m_1 + \ell].$$

We immediately deduce that $3m_1 + 2\ell = 2m_1 + 3\ell$, in which case, $m_1 = \ell$. Accordingly, $m_2 = m_1 + \ell = 2\ell$ and

$$m = 2q = 2m_1 + 2m_2 = 6\ell.$$

One now computes that

$$u_e(x) = x^{2\ell} + x^{\ell} + 1 = u_o(x)$$

and

$$M_e = m - \deg u_e = 4\ell \quad \text{and} \quad M_o = m - \ell - \deg u_o = 3\ell.$$

We accordingly obtain

$$\begin{aligned} f_e(x) &= x^{4\ell}(x^{2\ell} + x^{\ell} + 1) + x^{3\ell} + x^{2\ell} + x^{\ell} + 1 \\ &= x^{6\ell} + x^{5\ell} + x^{4\ell} + x^{3\ell} + x^{2\ell} + x^{\ell} + 1, \end{aligned}$$

and

$$\begin{aligned} f_o(x) &= x^{3\ell}(x^{2\ell} + x^{\ell} + 1) + x^{2\ell} + x^{\ell} + 1 \\ &= x^{5\ell} + x^{4\ell} + x^{3\ell} + x^{2\ell} + x^{\ell} + 1. \end{aligned}$$

Putting this information together, one obtains that $f(x) = \Phi_{13}(x^{\ell})$.

Next, in case (D), we get $m_2 = 2m_1$ and $q = m_2 + \ell = 2m_1 + \ell$. Expressing the odd exponents in Equation (38) in terms of m_1 and ℓ, we get

$$[m_1 + 2\ell, 2m_1 + \ell, 3m_1 + 2\ell, 4m_1 + \ell] = [2m_1 + \ell, 2m_1 + \ell, 4m_1 + \ell, 3m_1 + 2\ell].$$

After removing the common exponents, we obtain $m_1 + 2\ell = 2m_1 + \ell$. Thus, $m_1 = \ell$. Accordingly, $m_2 = 2\ell$ and $m = 6\ell$. It is readily verified that the present case is identical to (C) whence, one concludes that $f(x) = \Phi_{13}(x^{\ell})$. Theorem 1 is thus settled. □

Acknowledgements. The authors sincerely appreciate the referee's thorough examination of the manuscript. The referee's feedback was instrumental in identifying critical errors and significantly enhancing the presentation. The first named author's research was partially supported by MATRICS grant no. MTR/2021/000015 of SERB, India.

References

[1] A. Capelli, Sulla riduttibilitá delle equazioni algebriche, *Nota prima, Rend. Accad. Sci. Fis. Mat. Soc. Napoli* **3** (1897), 243 – 252.

[2] M. Filaseta and S. Konyagin, Squarefree values of polynomials all of whose coefficients are 0 and 1, *Acta Arith.* **74** (1996), 191 – 205.

[3] M. Filaseta, On the factorization of polynomials with small Euclidean norm, *Number Theory in Progress*, Vol. 1 (Zakophane-Kościelisko, 1997), 143 – 163, de Gruyter, Berlin, 1999.

[4] M. Filaseta and D. Meade, Irreducibility testing of lacunary $0,1$-polynomials, *J. Algorithms.* **55** (2005), 21 – 28.

[5] M. Filaseta, C. Finch and C. Nicol, On three questions concerning 0, 1-polynomials, *J. Théor. Nombres Bordeaux* **18** (2006), 257 – 270.

[6] J. Konvalina and V. Matache, Palindrome-polynomials with roots on the unit circle, *C. R. Math. Acad. Sci. Soc. R. Can.* **26** (2004), 39 – 44.

[7] W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, *Math. Scand.* **8** (1960), 65–70.

[8] A. M. Odlyzko and B. Poonen, Zeros of polynomials with 0, 1 coefficients, *Enseign. Math.* (2) **39** (1993), 317 – 348.

[9] A. Schinzel, Selected topics on polynomials, *Ann Arbor, Mich.*: University of Michigan Press, 1982.

[10] A. Schinzel, Polynomials with special regard to reducibility, *Encyclopedia of Mathematics and its applications* **77**. Cambridge University Press, Cambridge, 2000.