Journal de Théorie des Nombres
de Bordeaux **18** (2006), 357–370

On three questions concerning $0,1$-polynomials

par Michael FILASETA, Carrie FINCH et Charles NICOL

Résumé. Nous répondons à trois questions concernant la réductibilité (ou irréductibilité) de $0,1$-polynômes, polynômes qui n'ont pour seuls coefficients que 0 ou 1. La première question est de déterminer si une suite de polynômes qui se présente naturellement est finie. Deuxièmement, nous discutons si tout sous-ensemble fini d'un ensemble infini de nombres entiers positifs peut être l'ensemble des exposants d'un $0,1$-polynôme réductible. La troisième question est similaire, mais pour l'ensemble des exposants d'un polynôme irréductible.

Abstract. We answer three reducibility (or irreducibility) questions for $0,1$-polynomials, those polynomials which have every coefficient either 0 or 1. The first concerns whether a naturally occurring sequence of reducible polynomials is finite. The second is whether every nonempty finite subset of an infinite set of positive integers can be the set of positive exponents of a reducible $0,1$-polynomial. The third is the analogous question for exponents of irreducible $0,1$-polynomials.

1. Introduction

In this paper, we address three questions related to the reducibility or irreducibility of $0,1$-polynomials.

For the first, we define a sequence of $0,1$-polynomials recursively as follows. Let $f_0(x) = 1$. For j a positive integer, let $f_j(x) = x^{k_j} + f_{j-1}(x)$ where k_j is chosen to be the least positive integer $> \deg f_{j-1}$ such that $f_j(x)$ is reducible. The first several polynomials in this sequence are

$$f_0(x) = 1, \qquad f_1(x) = 1 + x^3, \qquad f_2(x) = 1 + x^3 + x^{15},$$
$$f_3(x) = 1 + x^3 + x^{15} + x^{16}, \qquad f_4(x) = 1 + x^3 + x^{15} + x^{16} + x^{32},$$
$$f_5(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33},$$
$$f_6(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34},$$

Manuscrit reçu le 16 novembre 2004.
The first two authors express their appreciation to the National Science Foundation and the National Security Agency for support during the research for this paper.

and

$$f_7(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}.$$

The problem is to decide whether this sequence is infinite. In other words, is it true that for each positive integer j, there is an integer $k_j > \deg f_{j-1}$ for which $x^{k_j} + f_{j-1}(x)$ is reducible? We show that the sequence is finite and, in fact, $f_7(x)$ is the last element of the sequence.

The next two questions are related to one another. We consider an infinite set

$$S = \{k_1, k_2, \ldots\} \subseteq \mathbb{Z}^+.$$

Is it possible for S to have the property that for every nonempty subset $\{e_1, \ldots, e_n\}$ of S, the polynomial

$$1 + x^{e_1} + \cdots + x^{e_n} \tag{1.1}$$

is reducible? Next, is it possible for S to have the property that for every nonempty subset $\{e_1, \ldots, e_n\}$ of S, the polynomial in (1.1) is irreducible? We show that the answer to the first question here is, "No," and the answer to the second question is, "Yes." This latter result requires a bit more work; as such, Section 4, which addresses this question, can be viewed as containing the main result of the paper.

Throughout the paper, we will make use of the following. A term of a polynomial $\sum_{j=0}^{n} a_j x^j$ refers to one of the monomials $a_j x^j$ with $a_j \neq 0$. The nth cyclotomic polynomial will be denoted by $\Phi_n(x)$. Also, $\zeta_n = e^{2\pi i/n}$. It is well known and easy to show that if n is a positive integer and k is an integer, then $\zeta_n^k = \zeta_{n/d}^{k/d}$ for any common divisor d of n and k. Furthermore, in this case, $\zeta_{n/\gcd(n,k)}^{k/\gcd(n,k)}$ is a primitive mth root of unity where $m = n/\gcd(n,k)$ (i.e., $\zeta_{n/\gcd(n,k)}^{k/\gcd(n,k)}$ is a root of $\Phi_m(x)$). For p a prime, r a nonnegative integer and n an integer, $p^r || n$ means $p^r | n$ and $p^{r+1} \nmid n$. For m a positive integer and r the number of distinct prime factors of m, we use $\mu(m)$ to denote the Möbius function defined by $\mu(m) = 0$ if m is not squarefree and $\mu(m) = (-1)^r$ if m is squarefree. For $f(x) \in \mathbb{C}[x]$ with $f(x) \not\equiv 0$, define $\tilde{f}(x) = x^{\deg f} f(1/x)$. The polynomial $\tilde{f}$ is called the *reciprocal* of $f(x)$. The constant term of $\tilde{f}$ is always non-zero. If the constant term of f is non-zero, then $\deg \tilde{f} = \deg f$ and the reciprocal of $\tilde{f}$ is f. If $\alpha \neq 0$ is a root of f, then $1/\alpha$ is a root of $\tilde{f}$. If $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{C}[x]$, then $\tilde{f} = \tilde{g}\tilde{h}$. If $f = \pm\tilde{f}$, then f is called *reciprocal*. If f is not reciprocal, we say that f is *non-reciprocal*. If f is reciprocal and α is a root of f, then $1/\alpha$ is a root of f. The product of reciprocal polynomials is reciprocal so that a non-reciprocal polynomial must have a non-reciprocal irreducible factor. For $f(x) \in \mathbb{Z}[x]$, we refer to the *non-reciprocal part of* $f(x)$ as the polynomial $f(x)$ removed of its

irreducible reciprocal factors in $\mathbb{Z}[x]$ having a positive leading coefficient. For example, the non-reciprocal part of $3(-x+1)x(x^2+2)$ is $-x(x^2+2)$ (the irreducible reciprocal factors 3 and $x-1$ have been removed from the polynomial $3(-x+1)x(x^2+2)$).

2. The first question

Let $g(x) = f_7(x)$. We want to show that for every integer $n \geq 36$, the polynomial $F(x) = x^n + g(x)$ is irreducible. We do this in two steps. First, we show that there are no irreducible reciprocal factors of $F(x)$. Then we show that there can be at most one irreducible non-reciprocal factor of $F(x)$. The argument for the first step will work for all positive integers n, and the argument for the second step will require $n \geq 83$. One can check computationally that $F(x)$ is irreducible for $1 \leq n \leq 82$, so in the end the condition $n \geq 36$ for our application can be relaxed to $n \geq 1$.

Assume that $R(x)$ is an irreducible reciprocal factor of $F(x) = x^n + g(x)$. We initially do not use the specific form of $g(x)$. Since $R(x)$ is reciprocal and it divides $F(x)$, we deduce $R(x)$ divides $\widetilde{F}(x) = \tilde{g}(x)x^{n-\deg g} + 1$. Hence, $R(x)$ is a factor of

$$\tilde{g}(x)F(x) - x^{\deg g}\widetilde{F}(x) = g(x)\tilde{g}(x) - x^{\deg g}.$$

Now, we consider the specific form of $g(x)$. We compute the polynomial $g(x)\tilde{g}(x) - x^{\deg g}$ explicitly and factor it. The polynomial has two reciprocal irreducible factors and $R(x)$ must be one of them. More precisely, $R(x)$ is either

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

or

$$x^{64} + x^{61} - x^{60} + x^{54} - \cdots - x^{43} + 2x^{42} + x^{41} - \cdots + x^{10} - x^4 + x^3 + 1.$$

Suppose $R(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Then $R(x)$ divides $x^7 - 1$ so that $x^{7k} \equiv 1 \pmod{R(x)}$ for every positive integer k. If $n \equiv r \pmod 7$ where $r \in \{0, 1, \ldots, 6\}$, then

$$F(x) \equiv x^r + x^6 + x^5 + x^4 + x^3 + x^2 + x + 2 \equiv x^r + 1 \not\equiv 0 \pmod{R(x)}.$$

This contradicts that $R(x)$ is a factor of $F(x)$. So $R(x)$ must be the second polynomial above of degree 64. A computation shows that $R(x)$ then has a root $\alpha = 0.5812485\cdots - 0.9634977\ldots i$ with $1.125 < |\alpha| < 1.126$. We obtain

$$|g(\alpha)| < g(1.126) < 231 < 1.125^{47} < |\alpha|^{47}.$$

By the triangle inequality, $F(\alpha) \neq 0$ for all $n \geq 47$. Therefore, $F(x)$ is not divisible by $R(x)$ for $n \geq 47$. Since $R(x)$ is of degree 64, we deduce that $F(x)$ is not divisible by $R(x)$ for all positive integers n. Thus, we obtain

a contradiction to our assumption that $F(x)$ has an irreducible reciprocal factor.

Next, we consider irreducible non-reciprocal factors of $F(x)$. In this case, we want to show that $F(x)$ has only one non-reciprocal irreducible factor whenever $n \geq 83$. We will make use of the following lemma which follows from Lemma 1 and Lemma 3 in [1].

Lemma 2.1. *The non-reciprocal part of a $0,1$-polynomial $f(x)$ is reducible if and only if there is a $0,1$-polynomial $w(x)$ different from $f(x)$ and $\tilde{f}(x)$ such that $w(1) = f(1)$ and $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.*

Assume that the non-reciprocal part of $F(x)$ is reducible. Taking $f(x) = F(x)$ in Lemma 2.1, we deduce that there is a $0,1$-polynomial $w(x)$ different from $F(x)$ and $\widetilde{F}(x)$ satisfying $w(1) = F(1)$ and $w\widetilde{w} = F\widetilde{F}$.

As $F(1) = 9$, we see that $w(x)$ has 9 terms. Since $n \geq 83$, the polynomial $\widetilde{F}(x)$ has a constant term of 1 and each other term of degree ≥ 48. Hence,

$$F\widetilde{F} = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35} + \cdots,$$

where the remaining exponents are each ≥ 48. Since $w(x)$ is a $0,1$-polynomial with 9 non-zero terms, there are integers $e_1, e_2, \ldots, e_7$, with

$$0 < e_1 < e_2 < \cdots < e_7 < n,$$

such that

$$w(x) = 1 + x^{e_1} + x^{e_2} + \cdots + x^{e_7} + x^n.$$

By replacing w with $\widetilde{w}$ if necessary, we may suppose that $e_1 \leq n - e_7$. With this added condition, our contradiction will be obtained by showing that $w(x) = F(x)$.

From $w\widetilde{w} = F\widetilde{F}$, we deduce

$$\begin{aligned} &\left(1 + x^{e_1} + x^{e_2} + \cdots + x^{e_7} + x^n\right) \\ &\qquad \times \left(1 + x^{n-e_7} + x^{n-e_6} + \cdots + x^{n-e_1} + x^n\right) \\ &\quad = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35} + \cdots. \end{aligned} \tag{2.1}$$

If the product on the left is expanded, then excluding the term 1, the smallest degree term will have exponent e_1 or $n - e_7$. Since $e_1 \leq n - e_7$, we deduce that $e_1 = 3$. The next smallest degree term on the left of (2.1) is either e_2 or $n - e_7$, so that one of these must be 15. On the other hand, if $n - e_7 = 15$, then the exponent $e_1 + n - e_7 = 18$ would also appear on the right of (2.1). It follows that $e_2 = 15$. We consider the next smallest exponent on both sides of (2.1) and deduce that one of e_3 and $n - e_7$ is 16. The equation $n - e_7 = 16$ cannot hold since $3 + 16 = 19$ is not an exponent on the right of (2.1). Thus, $e_3 = 16$. Similarly, we obtain $e_4 = 32$, $e_5 = 33$, $e_6 = 34$, and $e_7 = 35$, the only slight modification being that $n - e_7 \neq 32$

since $15 + 32 = 47$ does not appear as an exponent on the right of (2.1) (the exponent $3 + 32 = 35$ does). We conclude $w(x) = F(x)$ as claimed, obtaining a contradiction to Lemma 2.1. Thus, the non-reciprocal part of $F(x)$ is irreducible. This establishes what we set out to show.

3. The second question

In this section, we establish the following:

Theorem 3.1. *Let S be a set of positive integers having the property that if $\{e_1, \ldots, e_n\}$ is a nonempty subset of S, then the polynomial $1+x^{e_1}+\cdots+x^{e_n}$ is reducible. Then $|S| \leq 2$. More precisely, if a, b, and c are three positive integers, then at least one of the trinomials $1 + x^a + x^b$, $1 + x^a + x^c$, and $1 + x^b + x^c$ is irreducible.*

Observe that the three integers a, b, c above may be assumed to be distinct as it is clear that $1 + 2x^e$ is irreducible for any positive integer e. We will make use of a result observed independently by W. Ljunggren [4] and H. Tverberg [8].

Lemma 3.1. *Let u and v be distinct positive integers. If $1 + x^u + x^v$ is reducible, then it has a cyclotomic factor.*

Another result we will use is due to Schinzel and the first author; it is a consequence of Corollary 1 in [3].

Lemma 3.2. *Suppose $f(x) \in \mathbb{Z}[x]$ has N non-zero terms and is divisible by a cyclotomic polynomial. Then there is an integer m having all its prime factors $\leq N$ such that $\Phi_m(x)$ divides $f(x)$.*

In addition, we use the following simple result.

Lemma 3.3. *Let z_1 and z_2 be arbitrary complex numbers with absolute value 1. If $1 + z_1 + z_2 = 0$, then $\{z_1, z_2\} = \{\zeta_3, \zeta_3^2\}$.*

Proof. Note that $1 + z_1 + z_2 = 0$ implies that $z_1 = a + bi$ and $z_2 = c - bi$ for some a, b, and c. Since z_1 and z_2 are on the unit circle, $c = \pm a$. If $c = -a$, then $1 + z_1 + z_2 = 1 \neq 0$. If $c = a$, then $1 + z_1 + z_2 = 0$ implies $1 + 2a = 0$ so that $a = -1/2$. The conclusion follows. □

We note that the above lemmas allow us to describe the sets $S = \{a, b\}$ of two distinct positive integers with the property that for each nonempty $U \subseteq S$ the polynomial $1 + \sum_{e \in U} x^e$ is reducible. As the binomials $1 + x^a$ and $1 + x^b$ must be reducible, we see that each of a and b must have an odd prime divisor. Lemma 3.1 implies that since $1 + x^a + x^b$ is reducible, the trinomial has a cyclotomic factor. Let ζ_m by a root of $1 + x^a + x^b$. By Lemma 3.3, we must have $\{\zeta_m^a, \zeta_m^b\} = \{\zeta_3, \zeta_3^2\}$. In order for $\zeta_m^a \in \{\zeta_3, \zeta_3^2\}$, it is necessary and sufficient that $m = 3d$ and $a = a'd$ for some positive

integers d and a' with $3 \nmid a'$. We fix a to be an arbitrary positive integer with an odd prime divisor. Then we fix d dividing a such that 3 does not divide a/d. At least one such d always exists, as we can take $d = a$. Setting $m = 3d$, we want that $d|b$, $3 \nmid (b/d)$ and $b/d \not\equiv a/d \pmod 3$. Indeed, with a and d so fixed and $m = 3d$, it is necessary and sufficient for $\{\zeta_m^a, \zeta_m^b\} = \{\zeta_3, \zeta_3^2\}$ that b satisfies these three conditions. With the added condition that b has an odd prime divisor (as does a), this also describes completely the sets $S = \{a, b\}$ with the property that for each nonempty $U \subseteq S$ the polynomial $1 + \sum_{e \in U} x^e$ is reducible.

Let a, b, and c be distinct positive integers, and assume $1 + x^a + x^b$, $1 + x^a + x^c$, and $1 + x^b + x^c$ are all reducible. From Lemma 3.1, we deduce that there are positive integers m_1, m_2 and m_3, not necessarily distinct, satisfying

$$\begin{aligned} &\zeta_{m_1} \text{ is a root of } 1 + x^a + x^b \\ &\zeta_{m_2} \text{ is a root of } 1 + x^a + x^c \\ &\zeta_{m_3} \text{ is a root of } 1 + x^b + x^c. \end{aligned}$$

We may suppose by Lemma 3.2 that each m_j has only prime factors from the set $\{2, 3\}$. For $j \in \{1, 2, 3\}$, we define nonnegative integers k_j and ℓ_j by $m_j = 2^{k_j} 3^{\ell_j}$. Let $k = \max\{k_1, k_2, k_3\}$ and $\ell = \max\{\ell_1, \ell_2, \ell_3\}$. Observe that from Lemma 3.3, we have $\{\zeta_{m_1}^a, \zeta_{m_1}^b\} = \{\zeta_3, \zeta_3^2\}$, $\{\zeta_{m_2}^a, \zeta_{m_2}^c\} = \{\zeta_3, \zeta_3^2\}$, and $\{\zeta_{m_3}^b, \zeta_{m_3}^c\} = \{\zeta_3, \zeta_3^2\}$.

Given this set-up, we have the following lemma.

Lemma 3.4. *For each $j \in \{1, 2, 3\}$, 3^ℓ exactly divides m_j. Furthermore, $3^{\ell-1}$ exactly divides each of a, b, and c.*

Proof. By the definition of ℓ, $3^\ell || m_j$ for some $j \in \{1, 2, 3\}$. Without loss of generality, we may suppose that $3^\ell || m_1$. Since $\zeta_{m_1}^a \in \{\zeta_3, \zeta_3^2\}$, we must have $3^{\ell-1} || a$. Also, $\zeta_{m_1}^b \in \{\zeta_3, \zeta_3^2\}$ implies $3^{\ell-1} || b$. As $\zeta_{m_2}^a \in \{\zeta_3, \zeta_3^2\}$ and $3^{\ell-1} || a$, we deduce $3^\ell || m_2$. Now, $\zeta_{m_2}^c \in \{\zeta_3, \zeta_3^2\}$ implies $3^{\ell-1} || c$. Finally, since $\zeta_{m_3}^b \in \{\zeta_3, \zeta_3^2\}$ and $3^{\ell-1} || b$, we deduce $3^\ell || m_3$, completing the proof. □

We use Lemma 3.4 to establish the following lemma, which allows us to complete the proof of Theorem 3.1.

Lemma 3.5. *Let $d \in \{a, b, c\}$. Suppose i and j are such that $1 \le i, j \le 3$ with $i \ne j$.*

(i) *If $\{\zeta_{m_i}^d, \zeta_{m_j}^d\} = \{\zeta_3\}$ or $\{\zeta_3^2\}$, then $k_i \equiv k_j \pmod 2$.*
(ii) *If $\{\zeta_{m_i}^d, \zeta_{m_j}^d\} = \{\zeta_3, \zeta_3^2\}$, then $k_i \not\equiv k_j \pmod 2$.*

Proof. We first prove (i). If $\{\zeta_{m_i}^d, \zeta_{m_j}^d\} = \{\zeta_3\}$ or $\{\zeta_3^2\}$, then the ratio of $\zeta_{m_i}^d$ to $\zeta_{m_j}^d$ is 1. Recall from Lemma 3.4 that $3^{\ell-1} || d$, $3^\ell || m_i$ and $3^\ell || m_j$. Write

$d = 3^{\ell-1}d'$; then we have $3 \nmid d'$ and

$$1 = \frac{\zeta_{m_i}^d}{\zeta_{m_j}^d} = \frac{\zeta_{2^{k_i}3^\ell}^{3^{\ell-1}d'}}{\zeta_{2^{k_j}3^\ell}^{3^{\ell-1}d'}} = \zeta_{2^{k_i+k_j}3}^{d'(2^{k_j}-2^{k_i})}.$$

We deduce that $3|(2^{k_j} - 2^{k_i})$. As the order of 2 modulo 3 is 2, we obtain $k_i \equiv k_j \pmod 2$, completing the proof of (i). For (ii), we use essentially the same technique. Suppose $\zeta_{m_i}^d = \zeta_3$ and $\zeta_{m_j}^d = \zeta_3^2$. Then we have

$$1 = \frac{\zeta_{m_i}^{2d}}{\zeta_{m_j}^d} = \zeta_{2^{k_i+k_j}3}^{d'(2^{k_j+1}-2^{k_i})}.$$

We deduce $3|(2^{k_j+1} - 2^{k_i})$ so that $k_j + 1 \equiv k_i \pmod 2$. Hence, $k_i \not\equiv k_j \pmod 2$ in this case. This completes the proof of Lemma 3.5. □

We are now ready to complete the proof of Theorem 3.1. We use that $\{\zeta_{m_1}^a, \zeta_{m_1}^b\} = \{\zeta_3, \zeta_3^2\}$, $\{\zeta_{m_2}^a, \zeta_{m_2}^c\} = \{\zeta_3, \zeta_3^2\}$, and $\{\zeta_{m_3}^b, \zeta_{m_3}^c\} = \{\zeta_3, \zeta_3^2\}$. We deduce that it is not possible for all three of the equations

$$\zeta_{m_1}^a = \zeta_{m_2}^a, \quad \zeta_{m_1}^b = \zeta_{m_3}^b, \quad \text{and} \quad \zeta_{m_2}^c = \zeta_{m_3}^c$$

to hold (since, for example, exactly three of the expressions above are ζ_3). Relabeling if necessary, we may suppose that $\zeta_{m_1}^a = \zeta_3$ and $\zeta_{m_2}^a = \zeta_3^2$. By Lemma 3.5, $k_1 \not\equiv k_2 \pmod 2$.

The equations $1 + \zeta_{m_1}^a + \zeta_{m_1}^b = 0$ and $1 + \zeta_{m_2}^a + \zeta_{m_2}^c = 0$ imply $\zeta_{m_1}^b = \zeta_3^2$ and $\zeta_{m_2}^c = \zeta_3$, respectively. From $\{\zeta_{m_3}^b, \zeta_{m_3}^c\} = \{\zeta_3, \zeta_3^2\}$, we must have one of the following:

(I) $\zeta_{m_3}^b = \zeta_3$ and $\zeta_{m_3}^c = \zeta_3^2$.
(II) $\zeta_{m_3}^b = \zeta_3^2$ and $\zeta_{m_3}^c = \zeta_3$.

If (I) holds, then $\{\zeta_{m_1}^b, \zeta_{m_3}^b\} = \{\zeta_{m_2}^c, \zeta_{m_3}^c\} = \{\zeta_3, \zeta_3^2\}$. Then Lemma 3.5 implies $k_1 \not\equiv k_3 \pmod 2$ and $k_2 \not\equiv k_3 \pmod 2$. This is a contradiction since, of the three integers k_1, k_2 and k_3, at least two must share the same parity. If (II) holds, then $\{\zeta_{m_1}^b, \zeta_{m_3}^b\} = \{\zeta_3^2\}$ and $\{\zeta_{m_2}^c, \zeta_{m_3}^c\} = \{\zeta_3\}$. In this case, $k_1 \equiv k_3 \pmod 2$ and $k_2 \equiv k_3 \pmod 2$. This is a contradiction since k_1 and k_2 have different parity but both have the same parity as k_3.

This completes the proof of Theorem 3.1.

4. The third question

To resolve the third question mentioned in the introduction, we obtain a result of a more general nature that doesn't restrict ourselves to $0,1$-polynomials.

Theorem 4.1. *Fix $a_0, a_1, a_2, \ldots$ to be an infinite bounded sequence of non-negative integers with $a_0 \neq 0$. Suppose further that there are infinitely many positive integers j such that a_{4j}/a_0 is not 4 times a fourth power in $\mathbb{Q}$. Then*

there is an infinite set S of positive integers (depending on the sequence of a_j) having the property that for each finite subset T of S, the polynomial $a_0 + \sum_{t\in T} a_t x^t$ is irreducible over the rationals.

We begin with some preliminary lemmas. The first such lemma is a special case of a theorem due to A. Schinzel [6] (see [2]).

Lemma 4.1. *Let $f(x)$ and $g(x)$ be relatively prime polynomials in $\mathbb{Z}[x]$ with $f(0)g(0) \neq 0$. Suppose that $-f(x)g(x)$ is not a square and $f(x)g(x)$ is not 4 times a fourth power in $\mathbb{Z}[x]$. Then there exists a natural number K_0 such that, for every $k \geq K_0$, either $f(x)x^{4^k} + g(x)$ is irreducible or it has an irreducible reciprocal factor.*

For our application of the above lemma, we use the following.

Lemma 4.2. *For $f(x) = b \in \mathbb{Z}^+$ and $g(x) = a_0 + \sum_{k\in V} bx^{4^k}$ with V a nonempty set of nonnegative integers, each of $f(x)g(x)$ and $-f(x)g(x)$ is not a square in $\mathbb{Z}[x]$.*

Proof. Suppose $A(x) = B(x)^2$ for some $B(x) \in \mathbb{Z}[x]$. Suppose further that $A(x)$ has at least two terms so that $B(x)$ does as well. If the highest two degree terms in $B(x)$ are of degrees $n_1 = \deg B$ and n_2, then it is easy to see that the highest two degree terms in $A(x)$ are of degrees $2n_1$ and $n_1 + n_2$. It follows that the two highest degree terms of $A(x)$ have degrees $\geq (\deg A)/2$. One checks that this is impossible for $A(x) = f(x)g(x)$ and $A(x) = -f(x)g(x)$, completing the proof. □

Our next lemma, concerns polynomials of the form

$$F(x) = c_0 + c_1 x + c_2 x^{2^{u_2}} + \cdots + c_r x^{2^{u_r}},$$

where r is a positive integer, the c_j's are non-zero integers and the u_j's are all positive integers.

Lemma 4.3. *Let $F(x)$ be as above, and suppose m is a positive integer such that $F(\zeta_m) = 0$. Then m is squarefree.*

Proof. The lemma follows from a result of H. B. Mann [5] which asserts that if

$$a_0 + a_1\zeta_m^{e_1} + \cdots + a_r\zeta_m^{e_r} = 0 \tag{4.1}$$

where the $a_j \in \mathbb{Q}$ and the e_j are positive integers and if no proper sub-sum of the terms on the left of (4.1) is equal to zero, then $m/\gcd(m, e_1, \ldots, e_r)$ divides the product of the primes $\leq r + 1$. We start with $F(\zeta_m) = 0$ and break this sum of $r + 1$ terms into sub-sums adding to zero maximized in the sense that each sub-sum cannot itself be broken up further into proper sub-sums adding to zero. Thus, we have $F(x) = G_1(x) + \cdots + G_t(x)$, say, where for each $j \in \{1, 2, \ldots, t\}$, the sum $G_j(\zeta_m)$ divided by a power of

ζ_m is an equation of the form (4.1) for which Mann's theorem applies. If the constant and linear term of $F(x)$ both belong to the same $G_j(x)$, then the expression $m/\gcd(m, e_1, \ldots, e_r)$ in Mann's result is m and we deduce immediately that m is squarefree. On the other hand, suppose c_0 is a term in $G_i(x)$ and $c_1 x$ is a term in $G_j(x)$ with $i \neq j$. As $G_i(\zeta_m) = 0$ and $G_j(\zeta_m) = 0$, we deduce that each of $G_i(x)$ and $G_j(x)$ have at least two terms. Mann's result applied to $G_i(\zeta_m)$ implies that m is not divisible by the square of an odd prime. On the other hand, if we apply the result instead to $G_j(\zeta_m)/\zeta_m$, an expression of the form given in (4.1) with $a_0 = c_1$ and every e_j odd, then we deduce that m cannot be divisible by 4. The conclusion that m is squarefree follows. □

The next two lemmas will be used to establish the subsequent lemma. We omit their proofs as they are fairly easy to obtain.

Lemma 4.4. *Let m be a positive integer. Then*

$$\Phi_m(x) = x^{\varphi(m)} - \mu(m)x^{\varphi(m)-1} + \cdots .$$

In other words, the sum of the roots of $\Phi_m(x)$ is $\mu(m)$.

Lemma 4.5. *Let $m = p_1 p_2 \cdots p_\ell$ where the p_j are distinct odd primes. Then the number of squares modulo m that are relatively prime to m is $\varphi(m)/2^\ell$.*

A lemma that will play a crucial role in our approach is the following.

Lemma 4.6. *Let r be an integer ≥ 2, let $c_0, c_1, \ldots, c_r$ be arbitrary non-zero integers, and let $k_1', k_2', \ldots, k_r'$ be integers satisfying $0 \leq k_1' < k_2' < \cdots < k_r'$. Suppose the polynomial*

$$F(x) = c_0 + c_1 x^{4^{k_1'}} + \cdots + c_r x^{4^{k_r'}}$$

has a cyclotomic factor $\Phi_m(x)$. Then m divides $2^{2k_1'+1}$.

Proof. Let $F(x)$ be as in the lemma. Then $\Phi_m(x) \mid F(x)$ implies

$$c_0 + c_1 \zeta_m^{4^{k_1'}} + \cdots + c_r \zeta_m^{4^{k_r'}} = 0.$$

Setting $\xi = \zeta_m^{4^{k_1'}}$, we have that ξ is a cyclotomic root of unity and

$$c_0 + c_1 \xi^{4^{k_1'-k_1'}} + \cdots + c_r \xi^{4^{k_r'-k_1'}} = 0.$$

In other words, ξ is a root of the polynomial $c_0 + c_1 x + \sum_{j=2}^{r} c_j x^{4^{k_j'-k_1'}}$. Thus, without loss of generality, we may restrict our consideration to the case that $k_1' = 0$. So we now want to show that if

$$F(x) = c_0 + c_1 x + c_2 x^{4^{k_2'}} + \cdots + c_r x^{4^{k_r'}} \quad (1 \leq k_2' < \cdots < k_r', r \geq 2), \tag{4.2}$$

is divisible by a cyclotomic polynomial $\Phi_m(x)$, then m is either 1 or 2.

By Lemma 4.3, we have m is squarefree. Observe that if m is odd, then we want to show $m = 1$. Thus, in this case, it suffices to show that m cannot be an odd squarefree integer ≥ 3. Now, consider the case that m is even. Set $m' = m/2$. We want to show that $m' = 1$. Suppose otherwise. Since m' is odd, we have $m' \geq 3$. Also,

$$\zeta_m = \zeta_m^{m'} \zeta_m^{m'+1} = -\zeta_{m'}^{(m'+1)/2}.$$

Let

$$G(x) = c_0 - c_1 x + c_2 x^{4^{k_2'}} + \cdots + c_r x^{4^{k_r'}} = F(-x).$$

Since $G(\zeta_{m'}^{(m'+1)/2}) = F(\zeta_m) = 0$, we obtain that $-\zeta_m = \zeta_{m'}^{(m'+1)/2}$ is a root of $G(x)$. Also, $\gcd(m', (m'+1)/2) = 1$ so that $G(x)$ has $\zeta_{m'}$ as a root where m' is squarefree, odd, and ≥ 3. By replacing c_1 in (4.2) with $-c_1$ and m by m', we see that (now regardless of whether m is even or not) it suffices to show that if $F(x)$ is as in (4.2) and $F(\zeta_m) = 0$, then m cannot be an odd squarefree integer ≥ 3. We assume otherwise and obtain a contradiction.

We let ℓ denote the number of prime factors of m as in Lemma 4.5, and note that $\ell \geq 1$. For j relatively prime to m, define σ_j to be the automorphism of $\mathbb{Q}(\zeta_m)$ sending ζ_m to ζ_m^j. By Lemma 4.4, we have

$$\begin{aligned} 0 &= \sum_{\substack{1 \leq j \leq m \\ (j,m)=1}} \sigma_j(F(\zeta_m)) \\ &= c_0\varphi(m) + \mu(m)(c_1 + \cdots + c_r) \end{aligned}$$

which implies that

$$c_1 + \cdots + c_r = -c_0\mu(m)\varphi(m). \tag{4.3}$$

Observe that $c_1 + \cdots + c_r$ is non-zero since m is squarefree and $c_0 \neq 0$.

Now, set

$$C = \sum_{\substack{1 \leq j \leq m \\ \gcd(j,m)=1 \\ j \text{ is a square mod } m}} \sigma_j(\zeta_m).$$

Since the squares modulo m relatively prime to m form a subgroup of $\mathbb{Z}_m^*$, we see that

$$C = \sum_{\substack{1 \leq j \leq m \\ \gcd(j,m)=1 \\ j \text{ is a square mod } m}} \sigma_j(\zeta_m^{a^2}) \qquad \text{for every } a \in \mathbb{Z} \text{ with } \gcd(a,m) = 1.$$

By Lemma 4.5,

$$0 = \sum_{\substack{1 \leq j \leq m \\ (j,m)=1 \\ j \text{ is a square mod } m}} \sigma_j(F(\zeta_m)) = c_0\varphi(m)/2^\ell + C \cdot (c_1 + \cdots + c_r).$$

From (4.3), we deduce that

$$C = \mu(m)/2^{\ell}.$$

However, this is a contradiction since, by definition, C is an algebraic integer but $\mu(m)/2^{\ell} = \pm 1/2^{\ell}$ is not an integer. This contradiction finishes the proof of Lemma 4.6. □

Proof of Theorem 4.1. Let $b_j = a_{4^j}$ for each nonnegative integer j. For the proof, we construct a set $S \subseteq \{4^n : n \in \{0,1,2,\dots\}\}$ recursively with the property indicated in the theorem. In other words, we show that there exist integers k_j with $j \in \{1,2,\dots\}$ satisfying $0 \le k_1 < k_2 < \cdots$ such that for every finite set $U \subset \{k_1, k_2, \dots\}$, the polynomial $f(x) = a_0 + \sum_{k\in U} b_k x^{4^k}$ is irreducible. Thus, in Theorem 4.1, we can take $S = \{4^{k_j} : j \in \{1,2,\dots\}\}$.

From the conditions in Theorem 4.1, the values of b_j are bounded. We deduce that there is an integer b for which $b_j = b$ for infinitely many choices of j and such that b/a_0 is not 4 times a fourth power in $\mathbb{Q}$. We fix such a b. This is the only place we use that the sequence of b_j is bounded, so this condition in Theorem 4.1 can be relaxed. What we really require is simply that some value of a_{4^j} is repeated infinitely often and that this common value we are calling b satisfies the condition b/a_0 is not 4 times a fourth power in $\mathbb{Q}$. In particular, this implies $b \neq 0$. We will choose our k_j forming the set S in such a way that $b_{k_j} = b$ for each j.

We begin by taking k_1 to be any nonnegative integer for which $b_{k_1} = b$. The significance of the condition that b/a_0 is not 4 times a fourth power in $\mathbb{Q}$ is that a classical theorem of Capelli assures us then that $a_0 + bx^{4^{k_1}}$ is irreducible (cf. Theorem 21 in [7]). Indeed, Capelli's theorem implies that all of the various binomial expressions $a_0 + b_{k_j} x^{4^{k_j}} = a_0 + bx^{4^{k_j}}$ that will appear in our construction are irreducible.

Now, suppose that we have already obtained $k_1, \dots, k_t$, with $t \ge 1$, such that $U \subseteq \{k_1, k_2, \dots, k_t\}$ implies

$$f(x) = a_0 + \sum_{k\in U} b_k x^{4^k} = a_0 + \sum_{k\in U} b x^{4^k}$$

is irreducible. We want to find $k_{t+1} \notin \{k_1, k_2, \dots, k_t\}$ so that each of the 2^t polynomials of the form $a_0 + \sum_{k\in V} b_k x^{4^k} + b_{k_{t+1}} x^{4^{k_{t+1}}}$ is irreducible, where $V \subseteq \{k_1, \dots, k_t\}$. We also want $b_{k_{t+1}} = b$. We justify that we can find such a k_{t+1}.

For each fixed $V \subseteq \{k_1, \dots, k_t\}$, we apply Lemma 4.1 with $f(x) = b$ and $g(x) = a_0 + \sum_{k\in V} b_k x^{4^k}$. Observe that if $V = \emptyset$, then as indicated above $f(x)x^{4^k} + g(x)$ is a binomial expression which is irreducible. We will concentrate then on the case that $|V| \ge 1$.

For each $V \subseteq \{k_1, \dots, k_t\}$, $V \neq \emptyset$, we obtain from Lemma 4.1 and Lemma 4.2 that there is a $K_1(V)$ such that if we choose $k_{t+1} \geq K_1(V)$ with $b_{k_{t+1}} = b$, then $a_0 + \sum_{k \in V} bx^{4^k} + bx^{4^{k_{t+1}}}$ either has an irreducible reciprocal factor or is irreducible. Momentarily, we will show that there is also a $K_2(V)$ such that if we choose $k_{t+1} \geq K_2(V)$ with $b_{k_{t+1}} = b$, then $a_0 + \sum_{k \in V} bx^{4^k} + b_{k_{t+1}} x^{4^{k_{t+1}}}$ does not have an irreducible reciprocal factor. Then we can take

$$k_{t+1} \geq \max\Big\{k_t + 1, \max_{\substack{V \subseteq \{k_1,\dots,k_t\} \\ V \neq \emptyset}} \{K_1(V)\}, \max_{\substack{V \subseteq \{k_1,\dots,k_t\} \\ V \neq \emptyset}} \{K_2(V)\}\Big\}$$

with $b_{k_{t+1}} = b$. It will follow then that the 2^t polynomials of the form $a_0 + \sum_{k \in V} b_k x^{4^k} + b_{k_{t+1}} x^{4^{k_{t+1}}}$ are all irreducible, where V ranges over the subsets of $\{k_1, \dots, k_t\}$.

We first deal with possible non-cyclotomic irreducible reciprocal factors of $a_0 + \sum_{k \in V} bx^{4^k} + bx^{4^{k_{t+1}}}$. We put this in a more general setting. Fix $g(x)$ of degree ≥ 1 with $g(0) \neq 0$. Let b be as above. Suppose that $bx^n + g(x)$ has an irreducible reciprocal factor $r(x)$. Then $r(x)$ also divides the reciprocal of $bx^n + g(x)$, that is $x^{n - \deg g}\tilde{g}(x) + b$. Hence, $r(x)$ divides

$$\tilde{g}(x)(bx^n + g(x)) - bx^{\deg g}(x^{n-\deg g}\tilde{g}(x) + b) = g(x)\tilde{g}(x) - b^2 x^{\deg g}.$$

Since $\deg g \geq 1$, we have $g(x)\tilde{g}(x) - b^2 x^{\deg g}$ is not identically 0. Since also $g(x)\tilde{g}(x) - b^2 x^{\deg g}$ does not depend on n, we deduce that there are a finite number of possible values for $r(x)$ (depending only on $g(x)$ and b and not on n). In particular, we note that as n varies over the positive integers, there are only a finite number of distinct non-cyclotomic irreducible reciprocal factors occurring among the polynomials $bx^n + g(x)$.

Suppose n and n' are positive integers with $n' > n$. Observe that if $h(x)$ is an arbitrary irreducible polynomial dividing both $bx^n + g(x)$ and $bx^{n'} + g(x)$, then $h(x)$ divides the difference

$$\big(bx^{n'} + g(x)\big) - \big(bx^n + g(x)\big) = bx^n\big(x^{n'-n} - 1\big).$$

Given that $g(0) \neq 0$, we deduce that $h(x)$ divides $x^{n'-n} - 1$ and, hence, is cyclotomic. Thus, a non-cyclotomic irreducible polynomial $h(x)$ can divide $bx^n + g(x)$ for at most one positive integer n. Since we have just seen that there are only a finite number of distinct non-cyclotomic irreducible reciprocal factors occurring among the polynomials $bx^n + g(x)$, we deduce that there is an N such that if $n \geq N$, then $bx^n + g(x)$ is not divisible by a non-cyclotomic irreducible reciprocal polynomial.

We are interested in the case that $g(x) = a_0 + \sum_{k \in V} bx^{4^k}$ where V is a nonempty subset of $\{k_1, \dots, k_t\}$. For each such V, we deduce that there is an $N(V)$ such that if $n \geq N(V)$, then $bx^n + g(x)$ is not divisible by a non-cyclotomic irreducible reciprocal polynomial. We will show that we can take

$K_2(V) = N(V)$, that is that if $k_{t+1} \geq N(V)$, then $bx^{4^{k_{t+1}}} + g(x)$ cannot have a cyclotomic factor. Once we establish that we can take $K_2(V) = N(V)$, the proof of Theorem 4.1 will be complete.

We show how Lemma 4.6 implies we can take $K_2(V) = N(V)$. Let V be a nonempty subset of $\{k_1, \ldots, k_t\}$ as above. In Lemma 4.6, we take $r = |V| + 1$, $c_0 = a_0$ and $c_j = b$ for $1 \leq j \leq r$. The integers k'_j are chosen so that $V = \{k'_1, k'_2, \ldots, k'_{r-1}\}$ and $k'_r = k_{t+1}$. With m dividing $2^{2k'_1+1}$, we see that $\zeta_m^{4^{k'_1}} = \pm 1$ and $\zeta_m^{4^{k'_j}} = 1$ for $2 \leq j \leq r$. As $r \geq 2$, we obtain that $F(\zeta_m) \geq a_0 + (r-2)b > 0$. Thus, Lemma 4.6 implies $F(x)$ does not have a cyclotomic factor. We deduce that we can take $K_2(V) = N(V)$, as desired. □

Comments: Although the statement of Theorem 4.1 may seem awkward, this is somewhat hard to avoid largely due to the situation with the binomials $a_0 + a_s x^s$ where $s \in S$. Observe that if $S = \{e_1, e_2, \ldots\}$, then the binomial $a_0 + a_{e_j} x^{e_j}$ will be reducible if $a_{e_j} = a_0$ and e_j is not a power of 2. In particular, in the case of $0,1$-polynomials, it is necessary to take the elements of S to be powers of 2. Now, if $s \in S$, $s > 2$ and s is a power of 2, then the condition that a_s/a_0 is not 4 times a square in $\mathbb{Q}$ can be seen to be necessary as well. In this case, $s = 4e$ for some integer e. If $a_s/a_0 = 4r^4$ for some rational number r, then

$$a_0 + a_s x^s = a_0\big(1 + 4r^4 x^{4e}\big) = a_0\big(1 + 2rx^e + 2r^2 x^{2e}\big)\big(1 - 2rx^e + 2r^2 x^{2e}\big),$$

so the binomial $a_0 + a_s x^s$ is reducible.

As a consequence of Lemma 4.6, a $0,1$-polynomial with the degree of each term a power of 4 and with at least 3 terms is not divisible by a cyclotomic polynomial. There are other variations of this result. For example, the degrees being powers of 4 can be replaced by the degrees being of the form 2^{2k+1}. This can be seen by considering such a polynomial $f(x)$ and making the substitution $y = x^e$ where x^e is the non-constant term of smallest degree in $f(x)$. This transforms the polynomial to one of the form (4.2) with x there replaced by y. Hence, the result of Lemma 4.6 can be used to handle this case.

Acknowledgements: The authors express their gratitude to the referee for some helpful comments. In particular, the idea of obtaining Lemma 4.3 as a consequence of [5] was the referee's.

References

[1] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*. Number theory in progress, Vol. **1** (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 143–163.
[2] M. Filaseta, K. Ford, S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*. Illinois J. Math. **44** (2000), 633–643.
[3] M. Filaseta, A. Schinzel, *On testing the divisibility of lacunary polynomials by cyclotomic polynomials*. Math. Comp. **73** (2004), 957–965.
[4] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. **8** (1960), 65–70.
[5] H. B. Mann, *On linear relations between roots of unity*. Mathematika **12** (1965), 107–117.
[6] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. **11** (1965), 1–34.
[7] A. Schinzel, *Selected topics on polynomials*. Ann Arbor, Mich., University of Michigan Press, 1982.
[8] H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$. Math. Scand. **8** (1960), 121–126.

Michael Filaseta
Mathematics Department
University of South Carolina
Columbia, SC 29208, USA
E-mail : filaseta@math.sc.edu
URL: http://www.math.sc.edu/~filaseta/

Carrie Finch
Mathematics Department
University of South Carolina
Columbia, SC 29208, USA
E-mail : cfinch@math.sc.edu

Charles Nicol
Mathematics Department
University of South Carolina
Columbia, SC 29208, USA
E-mail : cnicol@math.sc.edu