MATH. SCAND. 110 (2012), 75–81

SEQUENCES OF {0, 1}-POLYNOMIALS WITH EXPONENTS IN ARITHMETIC PROGRESSION

CARRIE E. FINCH

Abstract

This paper finds the first irreducible polynomial in the sequence $f_1(x)$, $f_2(x)$, ..., where $f_k(x) = 1 + \sum_{i=0}^{k} x^{n+id}$, based on the values of n and d. In particular, when d and n are distinct, the author proves that if p is the smallest odd prime not dividing $d - n$, then $f_{p-2}(x)$ is irreducible, except in a few special cases. The author also completely characterizes the appearance of the first irreducible polynomial, if any, when $d = n$.

1. Introduction

Fix natural numbers d and n and consider a sequence of {0, 1}-polynomials formed in the following manner:

$$1 + x^n + x^{n+d}, \quad 1 + x^n + x^{n+d} + x^{n+2d}, \quad 1 + x^n + x^{n+d} + x^{n+2d} + x^{n+3d},$$

and so on. The question we explore in this paper is when the first irreducible polynomial appears in this sequence. The occurrence of the first irreducible polynomial depends on the values of n and d; in particular, the prime factors of $d - n$ dictate the appearance of the first irreducible polynomial. When d and n have the same value, we show (in Section 2) that when n is a power of 2 or contains more than two distinct prime factors there are no irreducible polynomials in the sequence, but when n is a power of an odd prime there is precisely one irreducible polynomial in the sequence, occurring when the polynomial has p terms.

When n and d are distinct, the smallest prime not appearing in the factorization of $d - n$ dictates the appearance of the first irreducible polynomial. This is formalized in the main result of Section 3, shown below.

THEOREM 2. *Let n and d be arbitrary distinct positive integers. Let $g = \gcd(d, n)$, and set $a = n/g$, $b = (n + d)/g$ and $c = (n + 2d)/g$. Let p be the smallest odd prime not dividing $(n - d)/g$. Then the least positive integer k*

Received 4 May 2010, in final form 3 November 2010.

such that $1 + x^n + x^{n+d} + x^{n+2d} + \cdots + x^{n+kd}$ *is irreducible is* $k = p - 2$, *except in the case that* $p > 3$ *and exactly one or exactly three of a, b and c are odd. In this exceptional case,* $k = 2$.

In the remainder of the paper, we use $\Phi_n(x)$ to denote the n^{th} cyclotomic polynomial, whose roots will be denoted $\zeta_n^j = e^{2\pi ij/n}$, where $(n, j) = 1$. The *noncyclotomic part* of a polynomial $f(x)$ refers to the product of the factors of $f(x)$ which are not cyclotomic polynomials. The reciprocal of a polynomial $g(x)$ is given by $x^{\deg g(x)} g(1/x)$, and is denoted by $\tilde{g}(x)$. A polynomial is reciprocal if $\tilde{g}(x) = \pm g(x)$. The *reciprocal part* of $f(x)$ is the product of all irreducible reciprocal factors of $f(x)$ taken with positive leading coefficient, and the *nonreciprocal part* of $f(x)$ is the product of the remaining factors when the reciprocal part has been removed.

2. Exponents congruent to 0 (mod d)

We first consider the case when the common difference of the exponents is equal to the smallest positive exponent, i.e., $d = n$. That is, we investigate the sequence

$$1 + x^n + x^{2n}, \quad 1 + x^n + x^{2n} + x^{3n}, \quad 1 + x^n + x^{2n} + x^{3n} + x^{4n},$$

and so on.

LEMMA 1. *Let* $n = p^r$ *with* p *an odd prime and* r *a positive integer. Then* $f(x) = 1 + x^n + x^{2n} + \cdots + x^{kn}$ *is irreducible exactly when* $k = p - 1$.

PROOF. Notice that

$$1 + x^{p^r} + x^{2p^r} + \cdots + x^{kp^r} = \frac{x^{(k+1)p^r} - 1}{x^{p^r} - 1} = \frac{\prod_{d|(k+1)p^r} \Phi_d(x)}{\prod_{d|p^r} \Phi_d(x)}. \tag{1}$$

So the left side of (1) contains exactly $\tau((k+1)p^r) - \tau(p^r)$ irreducible factors, where $\tau(m)$ denotes the number of divisors of m. For $k = p^e - 1$, we have

$$\tau((k+1)p^r) - \tau(p^r) = \tau(p^{e+r}) - \tau(p^r) = e,$$

and hence at least two irreducible factors for $e > 1$. For all other values of k, write $k + 1 = p^e k'$, where $k' > 1$, $(k', p) = 1$ and $e \geq 0$. Then we have

$$\begin{aligned} \tau((k+1)p^r) - \tau(p^r) &= \tau(k')\tau(p^{r+e}) - \tau(p^r) \geq 2\tau(p^{r+e}) - \tau(p^r) \\ &= 2(r + e + 1) - (r + 1) = r + 2e + 1 \geq 2 \end{aligned}$$

The result follows.

In the following lemma, we show that if n has at least two distinct prime factors, then the sequence $1+x^n+x^{2n}$, $1+x^n+x^{2n}+x^{3n}$, etc. contains only reducible polynomials.

LEMMA 2. *Let n be a positive integer with at least two distinct prime divisors. Then the polynomial $f(x) = 1 + x^n + x^{2n} + \cdots + x^{kn}$ is reducible for all natural numbers k.*

PROOF. As $(x^n - 1)f(x) = x^{(k+1)n} - 1$, it follows that $\Phi_{(k+1)n}(x)$ is a factor of $f(x)$ since the only factors of $x^n - 1$ are the cyclotomic polynomials $\Phi_m(x)$ where m is a divisor of n. As the degree of $\Phi_{(k+1)n}(x)$ is $\varphi((k+1)n)$ and the degree of $f(x)$ is kn, it suffices to show that $\varphi((k+1)n) < kn$. Let p and q be distinct prime factors of n. Observe that $k+1$ cannot divide both p and q; suppose $k+1$ does not divide p. Then the $n+1$ numbers $k+1, 2(k+1), 3(k+1), \ldots, n(k+1)$ and p are distinct positive integers that are each $\leq (k+1)n$ and not relatively prime to $(k+1)n$. It follows then that $\varphi((k+1)n) \leq (k+1)n - (n+1) < kn$, completing the proof.

Finally, in the following lemma we consider the sequence of polynomials when n is a power of 2.

LEMMA 3. *Let $n = 2^e$, where e is a positive integer, and let $k > 1$ be an integer. Then the polynomial $f(x) = 1 + x^n + x^{2n} + \cdots + x^{kn}$ is reducible.*

PROOF. Write $n = 2^e$. Then we have

$$f(x) = \frac{x^{(k+1)n} - 1}{x^n - 1} = \frac{(x^{(k+1)2^{e-1}} - 1)(x^{(k+1)2^{e-1}} + 1)}{(x^{2^{e-1}} - 1)(x^{2^{e-1}} + 1)},$$

so that $f(x)$ has at least two irreducible factors.

A corollary of the previous lemma is that the sequence $1+x^2+x^4$, $1+x^2+x^4+x^6$, etc. has only reducible polynomials. We gather together the results of the lemmata of this section and the observation that $1+x+x^2$ is a cyclotomic polynomial into the following theorem.

THEOREM 1. *If n is a positive integer, then either*

$$1 + x^n + x^{2n} + \cdots + x^{kn} \tag{2}$$

is reducible for every positive integer k, or n is a power of an odd prime. If $n = 1$, then (2) is irreducible for $k = 2$. If $n = p^e$, where p is an odd prime and e is a positive integer, then the only k for which (2) is irreducible is $k = p - 1$.

3. Exponents congruent to n (mod d)

Next we consider the case where the common difference is distinct from the smallest positive exponent, i.e., $d \neq n$. The theorem below shows that the prime factorization of $d-n$ plays a critical role in determining the appearance of the first irreducible polynomial in the sequence. We assume now that $d > n$. The case $d < n$ needs only trivial modifications.

THEOREM 2. *Let d and n be arbitrary distinct positive integers. Let $g = \gcd(d, n)$, and set $a = n/g$, $b = (n+d)/g$ and $c = (n+2d)/g$. Let p be the smallest odd prime not dividing $(n-d)/g$. Then the least positive integer k such that $1 + x^n + x^{n+d} + x^{n+2d} + \cdots + x^{n+kd}$ is irreducible is $k = p-2$, except in the case that $p > 3$ and exactly one or exactly three of a, b and c are odd. In this case, $k = 2$.*

In the proof of Theorem 2, we employ the following lemma due to Ljunggren [3], Mills [4] and Tverberg [6].

LEMMA 4. *Suppose $g(x) = x^a \pm x^b \pm 1$ or $g(x) = x^a \pm x^b \pm x^c \pm 1$ with $a > b > c > 0$. Then the noncyclotomic part of $g(x)$ is irreducible or identically 1 unless $g(x)$ has one of the following four forms:*

- $x^{8r} + x^{7r} + x^r - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^r + 1)$
- $x^{8r} - x^{7r} - x^r - 1 = (x^{2r}+1)(x^{3r} - x^{2r} + 1)(x^{3r} - x^r + 1)$
- $x^{8r} + x^{4r} + x^{2r} - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^{2r} + 1)$
- $x^{8r} - x^{6r} - x^{4r} - 1 = (x^{2r}+1)(x^{3r} - x^r - 1)(x^{3r} - x^r + 1)$

We also use the following lemma, which follows from Theorem 5 of [5], due to Selmer.

LEMMA 5. *Let $g(x) = 1 \pm x^a \pm x^b$ with $0 < a < b$. Let $d = \gcd(a, b)$. Any cyclotomic factor of $g(x)$ has the form $1 + x^d + x^{2d}$, and occurs if $a/d + b/d \equiv 0 \pmod 3$.*

We will also employ the following lemma due to Jones and the author [2].

LEMMA 6. *Let $g(x) = 1 + x^a + x^b + x^c$, where $0 < a < b < c$ are integers. Let $\gcd(a, b, c) = 2^k m$, where m is odd. Set $a' = a/2^k$, $b' = b/2^k$ and $c' = c/2^k$. Then $g(x)$ is reducible if and only if exactly one of a', b', and c' is even.*

Finally, we will use the following lemma due to Filaseta [1].

LEMMA 7. *If $g(x)$ is an irreducible $\{0, 1\}$-polynomial with $g(x)$ nonreciprocal and $g(0) = 1$, then $g(x^k)$ is irreducible for any positive integer k.*

PROOF OF THEOREM 2. Consider the polynomial $f(x) = 1 + x^n + x^{n+d} + x^{n+2d} + \cdots + x^{n+kd}$. Let $g = \gcd(d, n)$, and set $a = n/g$, $b = (n + d)/g$ and $c = (n + 2d)/g$. Let p be the smallest odd prime not dividing $(n - d)/g$. If $p = 3$, then consider the polynomial $1 + x^n + x^{n+d}$. By Lemma 4, the noncyclotomic part of $f(x)$ is irreducible, and by Lemma 5, $f(x)$ has a cyclotomic factor if $a + b \equiv 0 \pmod 3$, which is impossible. Thus, if $p = 3$, then $k = 1$.

Assume now that $p > 3$. If exactly one or three of a, b and c are odd, then by Lemma 6, $1 + x^n + x^{n+d} + x^{n+2d}$ is irreducible. Moreover, this is the first irreducible polynomial in the sequence since $\Phi_3(x)$ is a factor of $1 + x^n + x^{n+d}$ since 3 divides $(n - d)/g$.

Finally, assume that $p > 3$ and exactly two of a, b and c are odd. Notice that again $\Phi_3(x)$ is a factor of $1 + x^n + x^{n+d}$. By Lemma 6, $1 + x^n + x^{n+d} + x^{n+2d}$ is also reducible. Suppose now that $3 \leq k < p - 2$. Notice that

$$(x^d - 1) f(x) = x^{(k+1)d+n} - 1 + x^n(x^{d-n} - 1) \tag{3}$$

We show that $f(x)$ is reducible by finding a factor of the right side of (3) that does not divide $x^d - 1$. Let Π denote the product of the primes less than p. Let $n' = n/g$ and $d' = d/g$. Notice that since $a = n'$ and $c = n' + 2d'$, $a \equiv c \pmod 2$, so that $b = n' + d'$ must be even. Since $(n', d') = 1$, n' and d' are both necessarily odd. Thus $n' - d'$ is also even; that is $(d - n)/g$ is divisible by 2. Combining this with the hypothesis, this implies $d = n + g\ell\Pi$, where $p \nmid \ell$ and $\ell > 0$. Then $(k + 1)d + n = n(k + 2) + \Pi(gk\ell + g\ell)$.

Since $k + 2 < p$, there is a largest prime $q < p$ dividing $k + 2$, and hence, $(k + 1)d + n$. If q does not divide n, then q divides $d - n = g\ell\Pi$ but $q \nmid d$. Thus $x^q - 1$ divides each of $x^{(k+1)d+n} - 1$ and $x^{d-n} - 1$ (and hence the right side of (3)), but $x^q - 1$ does not divide $x^d - 1$.

On the other hand, if q divides n, then q^e divides g for some positive integer e. Thus q^{e+1} divides $(k + 1)d + n = n(k + 2) + \Pi(gk\ell + g\ell)$ since q divides both $k + 2$ and Π and q^e divides both n and g. Also, q^{e+1} divides $d - n = g\ell\Pi$. However, since $d = n + g\ell\Pi$, q^e is the highest power of q dividing d. Thus, $\Phi_{q^{e+1}}(x)$ divides the right side of (3), but does not divide $x^d - 1$. Thus, the polynomials in the sequence with fewer than p terms are reducible.

We now turn our attention to showing that $f(x)$ is irreducible when it has p terms. We do this in several steps: first we show that any reciprocal factor is one of several cyclotomic factors; we then show that none of these cyclotomic factors polynomials divides $f(x)$; finally, we show that the nonreciprocal part of $f(x)$ (which is all of $f(x)$) is irreducible.

Since d and n are distinct, $f(x)$ is nonreciprocal. If $(d, n) = g$, then we can write $f(x) = f_1(x^g)$. Thus it suffices by Lemma 7 to show that the

nonreciprocal polynomial $f_1(x)$ is irreducible. Hence, for the rest of the proof, we assume that d is relatively prime to n.

Suppose $r(x)$ is an irreducible reciprocal factor of $f(x)$. Then $r(x)$ also divides $\tilde{f}(x) = 1 + x^d + x^{2d} + \cdots + x^{(p-2)d} + x^{(p-2)d+n}$. Since $r(x)$ divides both $f(x)$ and $\tilde{f}(x)$, $r(x)$ also divides any combination of them. In particular, $r(x)$ divides $x^n\tilde{f}(x) - f(x) = x^{2n+(p-2)d} - 1$, which shows that $r(x)$ is a cyclotomic polynomial. Moreover, $r(x)$ also divides

$$(x^d - 1)(\tilde{f}(x) - f(x)) = x^n(x^{d-n} - 1)(x^{(p-2)d} - 1).$$

Since $r(x)$ does not divide x^2, $r(x)$ must divide $x^{d-n} - 1$ or $x^{(p-2)d} - 1$.

If $r(x)$ divides both $x^{2n+(p-2)d} - 1$ and $x^{(p-2)d} - 1$, then $r(x)$ divides $x^t - 1$, where t divides both $2n + (p-2)d$ and $(p-2)d$. Thus, t also divides $2n$. Since $r(x)$ is irreducible, we can replace $r(x)$ by $\Phi_q(x)$, where $q = 1, 2$, or an odd prime. It is obvious that q cannot be 1 or 2, as this implies $x = 1$ or $x = -1$ is a root of $r(x)$, and hence of $f(x)$. However, $f(1) = p$ and $f(-1) = 1$ or p. Hence q is an odd prime. As q divides both n and $2n + (p-2)d$ but not d, it divides $p - 2$. Let ζ be any zero of $\Phi_q(x)$ and let $p - 2 = hq$. Then, as $\zeta^n = 1$, $f(\zeta)$ equals

$$1 + 1 + \zeta^d + \cdots + \zeta^{hqd} = 2 + (\zeta^d + \cdots + \zeta^{qd})(1 + \zeta^{qd} + \cdots + \zeta^{(h-1)qd}) = 2.$$

Hence $\Phi_q(x)$ does not divide $f(x)$, so $r(x)$ does not exist.

The other possibility is that $r(x)$ divides both $x^{2n+(p-2)d} - 1$ and $x^{d-n} - 1$. This implies $r(x)$ divides $x^t - 1$, where t divides both $2n + (p-2)d$ and $d - n$. Again, we may replace $r(x)$ by $\Phi_q(x)$, where q is an odd prime dividing t. So q also divides $2n + (p-2)d + 2(d-n) = pd$. Then $q = p$ or q divides d. If $q = p$, then p divides $d - n$, a contradiction. On the other hand, if q divides d, then q divides both d and $d - n$, and hence also n. Again we reach a contradiction.

So $f(x)$ has no reciprocal factors. To complete the proof, we use Lemma 4 applied to $(x^d - 1)f(x) = x^{(p-1)d+n} + x^d - x^n - 1$ to see that the noncyclotomic part of $f(x)$ is irreducible.

We conclude by highlighting two corollaries of Theorem 2.

COROLLARY 1. *For $d > n$, there is always an irreducible polynomial in the sequence $1 + x^n + x^{n+d}$, $1 + x^n + x^{n+d} + x^{n+2d}$, etc.*

COROLLARY 2. *Let $d > 2$. The first irreducible polynomial in the sequence $1 + x^2 + x^{2+d}$, $1 + x^2 + x^{2+d} + x^{2+2d}$, etc. has*

- *4 terms when $d \equiv 5, 8$ or $11 \pmod{12}$*

- *p terms when $d \equiv 2 \pmod{12}$, where p is the smallest prime not dividing $d - 2$.*

ACKNOWLEDGEMENTS. The author thanks the referee for the valuable suggestions. This paper also benefited from helpful discussions with Michael Filaseta, for which the author is very appreciative. Finally, the author gratefully acknowledges support from the Lenfest Summer Research Grant at Washington and Lee University.

REFERENCES

1. Filaseta, M., *On the factorization of polynomials with small Euclidean norm*, pp. 143–163 in: Number Theory in Progress 1 (Proc. Zakopane-Kościelisko 1997), de Gruyter, Berlin 1999.
2. Finch, C., and Jones, L., *On the irreducibility of* $\{-1, 0, 1\}$*-quadrinomials*, Integers 6 (2006), A16, 4 pp.
3. Ljunggren, W., *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), 65–70.
4. Mills, W. H., *The factorization of certain quadrinomials*, Math. Scand. 57 (1985), 44–50.
5. Selmer, E. S., *On the irreducibility of certain trinomials,* Math. Scand. 4 (1956), 287–302.
6. Tverberg, H., *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$, Math. Scand. 8 (1960), 121–126.

MATHEMATICS DEPARTMENT
WASHINGTON & LEE UNIVERSITY
LEXINGTON, VA 24450
U.S.A.
E-mail: finchc@wlu.edu