COEFFICIENTS OF THE CYCLOTOMIC POLYNOMIAL $F_{3qr}(x)$

MARION BEITER
Rosary Hill College, Buffalo, New York 14226

Let F_m be the mth cyclotomic polynomial. Bang [1] has shown that for $m = pqr$, a product of three odd primes with $p < q < r$, the coefficients of $F_m(x)$ do not exceed $p - 1$ in absolute value. The smallest such m is 105 and the coefficient of x^7 in F_{105} is -2. It might be assumed that coefficients 2 and/or -2 occur in every F_{3qr}. This is not so. It is the purpose of this paper to characterize the pairs q, r in $m = 3qr$ such that no coefficient of absolute value 2 can occur in F_{3qr}.

1. PRELIMINARIES

Let $F_m(x) = \sum_{n=0}^{\varphi(m)} c_n x^n$. Then for $m = 3qr$, c_n is determined [1] by the number of partitions of n of the form:

$$n = a + 3\alpha q + 3\beta r + \gamma qr + \delta_1 q + \delta_2 r, \tag{1}$$

$0 \le a < 3$; α, β, γ, nonnegative integers; $\delta_i \in \{0, 1\}$. If n has no such partition, $c_n = 0$. Each partition of n in the form (1) contributes +1 to the value of c_n if $\delta_1 = \delta_2$, but -1 if $\delta_1 \ne \delta_2$. Because $F_m(x)$ is symmetric, we consider only $n \le \varphi(m)/2 = (q-1)(r-1)$. For $n > (q-1)(r-1)$, $c_n = c_{n'}$, with $n' = \varphi(m) - n$. We note that for $n \le (q-1)(r-1)$, γ in (1) must be zero.

A permissible partition of n is therefore one of these four:

$$\begin{aligned} P_1 &= a_1 + 3\alpha_1 q + 3\beta_1 r, & P_2 &= a_2 + 3\alpha_2 q + 3\beta_2 r + q + r, \\ P_3 &= a_3 + 3\alpha_3 q + 3\beta_3 r + q, & P_4 &= a_4 + 3\alpha_4 q + 3\beta_4 r + r. \end{aligned} \tag{2}$$

Partitions P_1 and P_2 will each contribute +1 to c_n, while P_3 and P_4 will each contribute -1. When $n \le (q-1)(r-1)$, only one partition for each P_i, $i = 1, \ldots, 4$, is possible [1].

Lemma 1: For any β_i in (2), $3\beta_i \le q - 2$ for all q.

Proof: Following Bloom [3] we have $3\beta_i r \le (q-1)(r-1) < (q-1)r$. Thus, $3\beta_i < q - 1$.

Corollary: $3\beta_i \le q - 3$ for $i = 2, 4$.

Lemma 2: Either $r + q \equiv 0 \pmod 3$ or $r - q \equiv 0 \pmod 3$, for all primes q and r with $3 < q < r$.

Proof: Let $q = 2k + 1$, $r = 2k_1 + 1$. Since 3 divides one and only one of the numbers $2t$, $2(t+1)$ when $2t+1$ is a prime, it follows that 3 divides one and only one of the numbers $r + q = 2(k + k_1 + 1)$ or $r - q = 2(k - k_1)$.

2. BOUNDS ON THE COEFFICIENTS

We set $3 < q < r$ and make repeated use of the expressions:

$$P_2 - P_1 = a_2 - a_1 + 3(\alpha_2 - \alpha_1)q + 3(\beta_2 - \beta_1)r + q + r = 0; \tag{3}$$

$$P_4 - P_3 = a_4 - a_3 + 3(\alpha_4 - \alpha_3)q + 3(\beta_4 - \beta_3)r + r - q = 0. \tag{4}$$

Theorem 1: In $F_{3qr}(x)$,

(a) if $r - q \equiv 0 \pmod 3$, then $-1 \le c_n \le 2$,

(b) if $r + q \equiv 0 \pmod 3$, then $-2 \le c_n \le 1$.

Proof of (a): Assume $c_n = -2$ for some n, i.e., partitions of n of forms P_3 and P_4 exist. Taking (4), modulo 3, we obtain $a_4 - a_3 \equiv 0 \pmod 3$. But $a < 3$, so that $a_4 = a_3$. Now taking (4), modulo q, we obtain $[3(\beta_4 - \beta_3) + 1]r \equiv 0 \pmod q$. Then $3(\beta_4 - \beta_3) + 1 = \beta q$, for some integer $\beta \neq 0$. Either $3(\beta_4 - \beta_3) = \beta q - 1 \ge q - 1$, or $3(\beta_3 - \beta_4) = |\beta| q + 1 \ge q + 1$. But $3\beta_i \le q - 2$ by Lemma 1. Therefore, P_3 and P_4 cannot both exist and we have $c_n \neq -2$.

The proof of (b) follows from a similar argument by considering (3), modulo 3, and then modulo q.

Remark 1: F_{3qr} may have a coefficient of 2 or of -2 but not of both.

Remark 2: If q and r are twin primes, $c_r = -2$ with $P_3 = 2 + q$, $P_4 = r$.

3. SPECIAL CASES

Before taking up the general case, we consider $r = kq \pm 1$ and $r = kq \pm 2$. We prove a theorem about $r = kq \pm 1$.

Theorem 2: Let $r = kq \pm 1$. In $F_{3qr}(x)$, $|c_n| \le 1$ if and only if $k \equiv 0 \pmod 3$.

Proof: To show the sufficiency of the condition, let $r = 3hq + 1$, with $q \equiv 1 \pmod 3$. Then $r - q \equiv 0 \pmod 3$, and $c_n \neq -2$ by Theorem 1. We show $c_n \neq 2$, i.e., there is no n for which partitions P_1 and P_2 can both exist. Taking (3), modulo 3, we obtain $a_2 - a_1 = 1$ or -2. We note that $r \equiv 1 \pmod q$. Then (3), modulo q, leads to one of the equations:

$$3(\beta_2 - \beta_1) = \beta q - 2 \quad \text{or} \quad 3(\beta_2 - \beta_1) = \beta q + 1$$

with $\beta \equiv 2 \pmod 3$. Obviously, there is no value of β which satisfies Lemma 1. Hence there is no n, $0 \le n \le (q-1)(r-1)$, for which partitions P_1 and P_2 both exist. Similarly, with $q \equiv 2 \pmod 3$, it can be shown that there is no n for which partitions P_3 and P_4 can both exist. When $r = 3hq - 1$, $r \equiv 2$ (mod

3). If $q \equiv 2$, the proof leads to the same two equations as above with $\beta \equiv 1$. Thus both equations are inconsistent with Lemma 1. If $q \equiv 1$, the same equations appear with β_2 and β_1 replaced by β_4 and β_3, respectively, and $\beta \equiv 2$. Thus $|c_n| \leq 1$.

The necessity of the condition $k \equiv 0 \pmod 3$ is shown by the counterexamples in Table 1. Values of k are given modulo 3. For each n, other partitions are not possible. We illustrate with the first counterexample, $r = kq + 1$ with $k \equiv 1$. The only possible r and q are $r \equiv 2$ and $q \equiv 1 \pmod 3$. Note that for $n = r$, $n \equiv 2 \pmod 3$. Thus in partitions P_1 or P_2, $\alpha_1 = \alpha_2 = 2$. Then $P_1 = 2 + 3\alpha_1 q + 3\beta_1 r = r = P_2 = 2 + 3\alpha_2 q + 3\beta_2 r + q + r$. In neither P_1 nor P_2 is it possible to find nonnegative α and β to satisfy the equations. Hence, the coefficient of x^r in F_{3qr} is -2.

Table 1 $r = kq \pm 1$

k (mod 3)	r	Partitions of n		Examples c_n	q	r	n
1	$kq + 1$	$P_3 = 1 + (k - 1)q + q$	$P_4 = r$	-2	7	29	29
1	$kq - 1$	$P_3 = (k - 1)q + q$	$P_4 = 1 + r$	-2	5	19	20
2	$kq + 1$	$P_1 = 1 + (k + 1)q$	$P_2 = q + r$	2	5	41	46
2	$kq - 1$	$P_1 = (k + 1)q$	$P_2 = 1 + q + r$	2	7	13	21

Theorem 3: Let $r = kq \pm 2$. In $F_{3qr}(x)$, $|c_n| \leq 1$ if and only if $k \equiv 0$ and $q \equiv 1 \pmod 3$.

The proof follows the method in Theorem 2 and is omitted here. Table 2 gives counterexamples to show the necessity.

Table 2 $r = kq \pm 2$

	k (mod 3)	r	Partitions of n		Examples c_n	q	r	n
$q \equiv 2 \pmod 3$	0	$kq + 2$	$P_1 = 2 + (q + 1)r/2$	$P_2 = 1 + (q - 1)kq/2 + q + r$	2	5	17	53
$q \equiv 2 \pmod 3$	0	$kq - 2$	$P_3 = (q + 1)r/2 + q$	$P_4 = 1 + (q - 1)kq/2 + r$	-2	5	13	44
	1	$kq + 2$	$P_3 = (k - 1)q + q + 2$	$P_4 = r$	-2	5	37	37
	1	$kq - 2$	$P_3 = (k - 1)q + q$	$P_4 = r + 2$	-2	7	47	49
	2	$kq + 2$	$P_1 = (k + 1)q + 2$	$P_2 = q + r$	2	7	37	44
	2	$kq - 2$	$P_1 = (k + 1)$	$P_2 = q + r + 2$	2	5	23	30

4. THE GENERAL CASE

More generally, for all primes q and r with $3 < q < r$, we have $r = (kq + 1)/h$, or $r = (kq - 1)/h$, $h \leq (q - 1)/2$. If $h = 1$, Theorem 2 applies. Therefore we set $1 < h$. In $r = (kq \pm 1)/h$, we may consider r, q, k, ± 1 as four independent variables with h dependent. Since r and q each have two possible values modulo 3 and k has three, there are 24 cases to be examined. We shall examine one of them. Then we shall present Table 3 showing all 24 cases and from the table we form a theorem which states conditions on q and r so that $|c_n| \leq 1$ in F_{3qr}.

First we take $r \equiv q \equiv 1$, $k \equiv 0 \pmod 3$ in $r = (kq-1)/h$, $1 < h \leq (q-1)/2$. Note that $h \equiv 2$. Since $r - q \equiv 0 \pmod 3$, $c \neq -2$ by Theorem 1. We show $c_n \neq 2$. Taking (3), modulo 3, we find $a_2 - a_1 = -2$ or 1. Then taking (3), modulo q, we obtain two possible congruences:

$$-2 + [3(\beta_2 - \beta_1) + 1](-1/h) \equiv 0 \quad \text{and} \quad 1 + [3(\beta_2 - \beta_1) + 1](-1/h) \equiv 0.$$

The first leads to the equation $3(\beta_2 - \beta_1) = \beta q - 2h - 1$ with $\beta \equiv 2$. No such value of β will satisfy Lemma 1. The second congruence leads to the equation $3(\beta_2 - \beta_1) = \beta q + h - 1$ with $\beta \equiv 2$. If $h = 2$, there is no value of β which satisfies Lemma 1, and $c_n \neq 2$. If $h > 2$, then $3\beta_1 = q - h + 1$ satisfies Lemma 1. Substituting this value in (3), we obtain $3\alpha_2 = r - k - 1$. Then $P_1 = (q - h + 1)$ and $P_2 = (r - k - 1)q + q + r$ with $a_1 = 0$, $a_2 = 1$. But when we set $a_3 + 3\alpha_3 q + 3\beta_3 r + q = (q - h + 1)$, we obtain $P_3 = 2 + (r - 2k - 1) + (h + 1)r + q$. Moreover, if we let $a_1 = 1$, $a_2 = 2$, partitions P_1 and P_2 exist but also P_4 exists. Thus, there is no n for which $c_n = 2$.

In Table 3 the values for r, q, k, and h are all modulo 3. From an inspection of Table 3 for the cases when max $|c_n| = 1$, we state

Theorem 4: Let $r = (kq \pm 1)/h$, $1 < h \leq (q - 1)/2$. In $F_{3qr}(x)$, $|c_n| \leq 1$ if and only if one of these conditions holds: (a) $k \equiv 0$ and $h + q \equiv 0 \pmod 3$ or (b) $h \equiv 0$ and $k + r \equiv 0 \pmod 3$.

Table 3 $r = (kq \pm 1)/h$, $1 < h < (q - 1)/2$

(Values for q, r, h, k are modulo 3)

	k	h	± 1	Partitions of n		max $\lvert c_n \rvert$
$r \equiv q \equiv 1$	0	1	+	$P_1 = 2 + (q - 2h + 1)r$	$P_2 = (r - 2k - 1)q + q + r$	2
	1	2	+	$P_1 = 2 + (2k + 1)q$	$P_2 = (2h - 1)r + q + r$	2
	2	0	+			1
	0	2	-			1
	1	0	-	$P_1 = 2 + (2h + 1)r$	$P_2 = (2k - 1)q + q + r$	2
	2	1	-	$P_1 = 2 + (r - 2k + 1)q$	$P_2 = (q - 2h - 1)r + q + r$	2

(continued)

Table 3—continued

	k	h	±1	Partitions of n		max $\lvert c_n \rvert$
$r \equiv q \equiv 2$	0	2	+	$P_1 = (r - 2k + 1)q$	$P_2 = 2 + (q - 2h - 1)r + q + r$	2
	1	0	+			1
	2	1	+	$P_1 = (2h + 1)r$	$P_2 = 2 + (2k - 1)q + q + r$	2
	0	1	-			1
	1	2	-	$P_1 = (2k + 1)q$	$P_2 = 2 + (2k - 1)r + q + r$	2
	2	0	-	$P_1 = (q - 2h + 1)r$	$P_2 = 2 + (r - 2k - 1)q + q + r$	2
$r \equiv 1,\ q \equiv 2$	0	1	+			1
	1	0	+	$P_3 = 2 + (q - 2h + 1)r + q$	$P_4 = (r - 2k + 1)q + r$	2
	2	2	+	$P_3 = 2 + (2k - 1)q + q$	$P_4 = (2h - 1)r + r$	2
	0	2	-	$P_3 = 2 + (r - 2k - 1)q + q$	$P_4 = (q - 2h - 1)r + r$	2
	1	1	-	$P_3 = (k - 1)q + q$	$P_4 = 1 + (h - 1)r + r$	2
	2	0	-			1
$r \equiv 2,\ q \equiv 1$	0	2	+			1
	1	1	+	$P_3 = 1 + (k - 1)q + q$	$P_4 = (h - 1)r + r$	2
	2	0	+	$P_3 = (r - 2k - 1)q + q$	$P_4 = 2 + (q - 2h - 1)r + r$	2
	0	1	-	$P_3 = (q - 2h + 1)r + q$	$P_4 = 2 + (r - 2k + 1)q + r$	2
	1	0	-			1
	2	2	-	$P_3 = (q - 2h + 1)r + q$	$P_4 = 2 + (r - 2k + 1)q + r$	2

REFERENCES

1. A. S. Bang, "Om Ligningen $\phi_n(x) = 0$," *Nyt Tidsskrift for Mathematic*, Vol. 6 (1895), pp. 6-12.
2. M. Beiter, "Magnitude of the Coefficients of the Cyclotomic Polynomial $F_{pqr}(x)$," *Duke Math. Journal*, Vol. 38 (1971), pp. 591-594.
3. D. M. Bloom, "On the Coefficients of the Cyclotomic Polynomials," *Amer. Math. Monthly*, Vol. 75 (1968), pp. 372-377.

*****