TERNARY CYCLOTOMIC POLYNOMIALS
WITH AN OPTIMALLY LARGE SET OF COEFFICIENTS

GENNADY BACHMAN

Abstract. Ternary cyclotomic polynomials are polynomials of the form
\[ \Phi_{pqr}(z) = \prod_{\omega} (z - \omega), \]
where \( p < q < r \) are odd primes and the product is
taken over all primitive \( pqr \)-th roots of unity \( \omega \). We show that for every \( p \)
there exists an infinite family of polynomials \( \Phi_{pqr} \) such that the set of coefficients of each of these polynomials coincides with the set of integers in the
interval \( \left[ -\frac{p-1}{2}, \frac{p+1}{2} \right] \). It is known that no larger range is possible
even if gaps in the range are permitted.

1. Introduction and statement of results

The \( n \)-th cyclotomic polynomial \( \Phi_n(z) \) is defined by
\[
\Phi_n(z) = \prod_{1 \leq \alpha \leq n \atop (\alpha, n) = 1} \left( z - e^{2\pi i \alpha/n} \right) = \sum_{m=1}^{\varphi(n)} a_m z^m,
\]
where \( \varphi \) is the Euler totient function and \( a_m = a_m(n) \). The coefficients \( a_m \)
are known to be integral, and there is a considerable amount of literature investigating
their properties. We refer the reader to the papers of H. W. Lenstra \([9]\) and R. C.
Vaughan \([11]\) which, between them, provide an excellent introduction to this topic
and a survey of the literature up to the mid-80s. It turns out that for the purposes
of studying coefficients \( a_m(n) \) it suffices to consider odd square-free integers \( n \),
and that the number of (distinct) prime factors of \( n \) is an important parameter in this
problem. Thus, for an odd prime \( p \) the cyclotomic polynomial \( \Phi_p \) is just
\[
\Phi_p(z) = \frac{1 - z^p}{1 - z} = 1 + z + z^2 + \cdots + z^{p-1}.
\]
The first nontrivial case is when \( n \) is a product of two distinct odd primes \( p \) and \( q \)
and we have
\[
\Phi_{pq}(z) = \frac{(1 - z^{pq})(1 - z)}{(1 - z^q)(1 - z^p)}.
\]
This case has been studied by several authors \([3], [7], [9]\), and our understanding
of it is rather complete. In particular, it is a rather simple matter to use the latter
identity to show that the coefficients of \( \Phi_{pq} \) take on the values 0 and \( \pm 1 \).

Received by the editors July 13, 2002 and, in revised form, April 21, 2003.
2000 Mathematics Subject Classification. Primary 11B83, 11C08.
The term “ternary cyclotomic polynomial” refers to the case where \( n \) is a product of three primes \( p, q, \) and \( r \), with \( p < q < r \), say. The smallest example is \( n = 3 \cdot 5 \cdot 7 = 105 \), which is already of interest since this is the smallest \( n \) for which the coefficients of \( \Phi_n \) are not all 0 or \( \pm 1 \). More precisely, \( a_7(105) = -2 \). On the other hand, a classic result of A. S. Bang [2] gives the bound \( |a_m| \leq p - 1 \). Analogously to the previous cases, ternary cyclotomic polynomials admit a rational representation

\[
\Phi_{pqr}(z) = \frac{(1 - z^{pqr})(1 - z^q)(1 - z^p)}{(1 - z^r)(1 - z^{pr})(1 - z^{pq})(1 - z)},
\]

and even though this is readily seen to lead to rather simple computations with truncated Taylor series, several interesting questions about coefficients of these polynomials remain open. Our main goal here is to establish the following result.

**Theorem.** For every odd prime \( p \) there exists an infinite family of polynomials \( \Phi_{pqr} \) such that the set of coefficients of each of these polynomials coincides with the set of integers in the interval \([- (p - 1)/2, (p + 1)/2]\). Moreover, the latter assertion is also true if we state it with the interval \([- (p + 1)/2, (p - 1)/2]\) instead.

Polynomials of the theorem possess certain extremal properties, as we now explain. Perhaps the most interesting open problem about the coefficients of ternary cyclotomic polynomials is the following conjecture, due to M. Beiter [4].

**Conjecture.** We have

\[
|a_m| \leq \frac{p + 1}{2}.
\]

Although the closest we have come to (1.3) is the bound

\[
|a_m| \leq p - \left\lfloor \frac{p}{4} \right\rfloor,
\]

we do know that the difference between the largest and the smallest coefficients of \( \Phi_{pqr} \) is at most \( p \). More precisely, setting

\[
A_+ = A_+(pqr) = \max_{1 \leq m \leq \varphi(pqr)} a_m(pqr) \quad \text{and} \quad A_- = A_-(pqr) = \min_{1 \leq m \leq \varphi(pqr)} a_m(pqr),
\]

we have

\[
A_+ - A_- \leq p,
\]

so that either \( A_+ \leq (p - 1)/2 \) or \( A_- \geq -(p - 1)/2 \). In view of (1.5) it follows that the ranges of values attained by the coefficients of the polynomials \( \Phi_{pqr} \) of the theorem cannot be enlarged, even if we permit gaps in those ranges. Moreover, if the conjecture is true, then, by (1.4), the coefficients of the polynomials \( \Phi_{pqr} \) of the theorem take on all possible values that coefficients of ternary cyclotomic polynomials may have, without exception. The existence of polynomials \( \Phi_{pqr} \) with such a striking property appears to have been completely unexpected.

Earlier, H. Möller [10] gave an explicit construction of polynomials \( \Phi_{pqr} \), for every \( p \), with a prescribed coefficient equal to \( (p + 1)/2 \). This showed that the conjecture is best possible, if true. We remark that Möller’s polynomials do not lead to a possible counterexample to the conjecture, for it follows from a recent result of the author [1] that the coefficients of these polynomials do satisfy (1.3). In fact, [1] contains all known upper bound results, and the reader is referred there for a more leisurely discussion of this topic. In particular, estimates (1.4) and (1.5) will be found in [1] Corollaries 2 and 3, respectively. We remark that (1.3) is only
a slight improvement on an earlier estimate of Beiter [4], who had it with \( \lfloor \frac{c}{d} \rfloor \) in place of \( \lceil \frac{c}{d} \rceil \).

We conclude this section with two remarks. First, we note that estimates for coefficients of ternary cyclotomic polynomials have been used as a base case in the inductive argument giving estimates for coefficients of \( \Phi_n \) with \( n \) having \( k > 3 \) (distinct, odd) prime factors. Rather precise results in this direction have been obtained for \( k \) by Bateman, Pomerance and Vaughan [3].

As we mentioned earlier, the smallest \( n \) for which \( \Phi_n \) has coefficients exceeding 1 in absolute value is \( n = 105 \). It was Schur (see [8] or [9]) who first showed that coefficients of cyclotomic polynomials can be arbitrarily large in absolute value. In order to get a coefficient of size \( k \) in a polynomial \( \Phi_n \) his construction required \( n \) to be a product of \( k \) prime factors. The aforementioned result of Möller shows that already the coefficients of ternary cyclotomic polynomials have no bound. We can further conclude from our theorem that every integer occurs as a coefficient of ternary cyclotomic polynomials.

2. Preliminaries

Representation (1.2) immediately suggests several ways of computing the coefficients \( a_m \). Perhaps the most promising approach is to proceed as follows. We have, in view of (1.1),

\[
\Phi_{pqr}(z) = (1 - z^{pqr}) (1 - z^p) (1 - z^q) \sum_{l=0}^{p-1} z^l \sum_{i=0}^{\infty} z^{iqr} \sum_{j=0}^{\infty} z^{jp} \sum_{k=0}^{\infty} z^{kpq} 
\]

\[
\equiv (1 - z^q - z^r + z^{q+r}) \sum_{l=0}^{p-1} z^l \sum_{i=0}^{p-1} z^{iqr} \sum_{j=0}^{q-1} z^{jp} \sum_{k=0}^{r-1} z^{kpq} \quad (\text{mod } z^{\varphi(pqr)+1}).
\]

So the key to our problem is seen to be linear combinations of \( qr, pr, \) and \( pq \) with nonnegative coefficients. To this end we observe that each natural number \( n \) has a unique representation in the form

\[
n = x_n qr + y_n pr + z_n pq + \delta_n pqr,
\]

with \( 0 \leq x_n < p, 0 \leq y_n < q, 0 \leq z_n < r, \) and \( \delta_n \in \mathbb{Z} \), so that \( n \mapsto (x_n, y_n, z_n, \delta_n) \) is well defined. Furthermore, we have

\[
x_n \equiv x_1 n \quad (\text{mod } p), \quad y_n \equiv y_1 n \quad (\text{mod } q), \quad z_n \equiv z_1 n \quad (\text{mod } r).
\]

Of interest to us are only \( 0 \leq n \leq \varphi(pqr) \), and in this range the quantity \( \delta_n \) takes on one of three values: \(-2, -1, \) or 0. Set

\[
\chi(n) = \begin{cases} 1, & \text{if } \delta_n = 0, \\ 0, & \text{otherwise}, \end{cases}
\]

and define

\[
S(x) = \sum_{x-p<n \leq x} \chi(n).
\]

The following identity then follows immediately from (2.1), (2.2), (2.3), and (2.4).

Lemma 1. We have

\[
a_m = S(m) - S(m-q) - S(m-r) + S(m-r-q).
\]
Despite the apparent simplicity of this identity, evaluation/estimation of $a_m$ is a challenging problem, as we already noted. This is due to the fact that it is difficult to get good estimates of just how many linear combinations (2.2) with $\delta_n = 0$ will contribute to $S(x)$. The following observation permits the simplification of considering two-term inequalities instead.

**Lemma 2.** For $0 \leq n \leq \varphi(pqr)$, $\chi(n) = 1$ if and only if $n$ satisfies the inequality

\[(2.6) \left\{ \frac{x_1n}{p} \right\} + \left\{ \frac{y_1n}{q} \right\} \leq \frac{n}{pqr},\]

where $\{x\}$ denotes the fractional part of $x$.

**Proof.** Dividing (2.2) by $pqr$ and using (2.3) gives

\[(2.7) \left\{ \frac{x_1n}{p} \right\} + \left\{ \frac{y_1n}{q} \right\} + \left\{ \frac{z_1n}{r} \right\} = \frac{n}{pqr} - \delta_n,\]

from which the claim readily follows. \qed

We conclude this section with two remarks. First, it is clear from (2.7) that we could have used any two terms on the left of (2.7) in (2.6). But we will use this particular choice for the proof of our theorem in the next section. Second, the approach to $a_m$ given in this section holds promise for further investigations of coefficients of ternary cyclotomic polynomials beyond our present goals.

### 3. Proof of the Theorem

Fix an odd prime $p$. Let $q$ be any prime of the form

\[(3.1) q = \tau p + 2,\]

and $r$ any prime satisfying $r > pq$ and $r \equiv (pq - 1)/2 \pmod{pq}$, so that

\[(3.2) r \equiv \frac{p - 1}{2} \pmod{p} \quad \text{and} \quad r \equiv \frac{q - 1}{2} \pmod{q}.\]

The existence of infinitely many such primes $q$ and $r$ is guaranteed by Dirichlet’s theorem for primes in arithmetic progressions (see, for example, [6]). We will show that every integer $c$, $-\frac{(p - 1)/2}{2} \leq c \leq \frac{(p + 1)/2}{2}$, occurs as a coefficient in $P_{pqr}$. In view of (1.4) this is sufficient to establish the first claim of the theorem.

First, observe that for $c = 0$ and $\pm 1$ the claim follows immediately from (3.1). Indeed, for every $P_{pqr}$, we have $a_0 = a_1 = 1$, $a_p = 0$, and $a_q = -1$. To establish the rest of the claim, we consider positive and negative values of $c$ separately. So let $1 \leq c \leq (p + 1)/2$, be arbitrary but fixed. We will show that there exists an integer $m = m_c$ such that

\[(3.3) S(m) = c\]

while

\[(3.4) S(m - q) = S(m - r) = S(m - q - r) = 0.\]

From this the desired conclusion follows from Lemma 2.

The integer $m$ that we are looking for will be of the form

\[(3.5) m = m_0 + tpq,\]
where $t = t_c$ is a parameter to be specified later and $m_0$ is the smallest positive integer that has the representation (2.2) with $x_{m_0} = 0$ and $y_{m_0} = (q - \tau - 2)/2$. Note that we certainly have

$$m_0 = \frac{q - \tau - 2}{2} pr + z_{m_0}pq - pqr \leq pq,$$

and that every integer of the form (3.5) satisfies

$$x_m = 0 \quad \text{and} \quad y_m = \frac{q - \tau - 2}{2}.$$ 

In addition to (3.7), we will also need the values of the coefficients $x_n$ and $y_n$ for several other special values of $n$. Considering the representation (2.2) of 1 modulo $p$ and $q$, one readily verifies that, by (3.1) and (3.2), we have

$$x_1 = p - 1 \quad \text{and} \quad y_1 = \tau.$$

Combining this with (2.3) yields, by (2.3) and (3.7),

$$x_{m-q} = 2, \quad x_{m-r} = \frac{p - 1}{2}, \quad x_{m-q-r} = \frac{p + 3}{2},$$

$$y_{m-q} = \frac{q - \tau - 2}{2}, \quad y_{m-r} = q - 1 = y_{m-q-r}. $$

Let us now consider the left side of (2.6) for $m - p < n \leq m$. Setting $n = m - k, 0 \leq k < p$, we rewrite it as

$$f_1(k) = \left\{ \frac{x_1(m - k)}{p} \right\} + \left\{ \frac{y_1(m - k)}{q} \right\} = \left\{ \frac{x_{m-k}^1}{p} \right\} + \left\{ \frac{y_{m-k}^1}{q} \right\}$$

$$= \frac{k}{p} + \left\{ \frac{q - \tau - 2 - 2\tau k}{2q} \right\},$$

by (2.3), (3.7), and (3.8). Set

$$\rho = f_1(c - 1).$$

Since $0 \leq c - 1 \leq (p - 1)/2$, it follows from (3.10) and (3.1) that for $0 \leq k \leq c - 1$ we have

$$f_1(k) \leq \rho \leq f_1 \left( \frac{p - 1}{2} \right) = \frac{1}{2} - \frac{1}{2p},$$

and that for $k \geq c$ we certainly have

$$f_1(k) \geq \rho + \frac{2}{pq}.$$ 

Analogously, considering the left side of (2.6) for the ranges $m - q - p < n \leq m - q, m - r - p < n \leq m - r, \text{ and } m - q - r - p < n \leq m - q - r$, yields, by (2.3) and (3.7)–(3.9),

$$f_2(k) = \left\{ \frac{2 + k}{p} \right\} + \left\{ \frac{q - \tau - 2 - 2\tau k}{2q} \right\},$$

$$f_3(k) = \left\{ \frac{p - 1 + 2k}{2p} \right\} + \left\{ \frac{q - 1 - \tau k}{q} \right\},$$

$$f_4(k) = \left\{ \frac{p + 3 + 2k}{2p} \right\} + \left\{ \frac{q - 1 - \tau k}{q} \right\}.$$
respectively, with $0 \leq k < p$. In particular, one readily verifies that
\begin{equation}
(3.14) \quad f_2(k), f_3(k), f_4(k) \geq \frac{1}{2} - \frac{1}{2p} + \frac{1}{pq}.
\end{equation}
Next we consider the right side of (2.6) for $n = m - (p - 1)/2$. We have, by (3.5),
\begin{equation}
(3.15) \quad \frac{m - (p - 1)/2}{pq} = \frac{m_0}{pq} - \frac{p - 1}{2pq} + \frac{t}{r}.
\end{equation}
Therefore, by (3.10)–(3.12) and (3.6), and since $r > pq$, we are able to choose $t$ so that
\begin{equation}
(3.16) \quad \rho \leq \frac{m - (p - 1)/2}{pq} < \rho + \frac{1}{pq},
\end{equation}
as we now assume. Using (3.15), we bound the right side of (2.6) for the other values of $n$ involved in computing $a_m$ as follows. First, for $0 \leq k \leq c - 1$ we take the lower bound
\begin{equation}
(3.17) \quad \frac{m - k}{pq} \geq \frac{m - (p - 1)/2}{pq} \geq \rho,
\end{equation}
while for $c \leq k < p$ we take the upper bound
\begin{equation}
(3.18) \quad \frac{m - k}{pq} = \frac{m - (p - 1)/2}{pq} + \frac{(p - 1)/2 - k}{pq} < \rho + \frac{2}{pq}.
\end{equation}
Furthermore, for $0 \leq k < p$ we also take the upper bound
\begin{equation}
(3.19) \quad \phi(k) = \frac{m - k}{pq} = \frac{m - (p - 1)/2}{pq} < \rho + \frac{1}{pq}.
\end{equation}
We are now ready to apply Lemma 2 to evaluate $\chi(n)$ for $n$ in the ranges under consideration. Thus, for $0 \leq k \leq c - 1$, we have, by (3.12) and (3.16),
\begin{equation}
(3.20) \quad \chi(m - k) = 1,
\end{equation}
while (3.13) and (3.17) yield
\begin{equation}
(3.21) \quad \chi(m - k) = 0,
\end{equation}
for $c \leq k < p$. Furthermore, (3.11), (3.12), and (3.18) give
\begin{equation}
(3.22) \quad \chi(m - q - k) = \chi(m - r - k) = \chi(m - q - r - k) = 0,
\end{equation}
for $0 \leq k < p$. Finally, recalling the definition (2.5) of the function $S$, we see that (3.3) and (3.4) indeed hold, by (3.19)–(3.21).

Next we consider negative coefficients of $\Phi_{pqr}$. We wish to show that for every $1 \leq c \leq (p - 1)/2$ we have $a_l = -c$ for some $l = l_c$. Our argument in this case will closely parallel our argument for positive coefficients with one important difference—we cannot take $c = (p + 1)/2$ in this case. In fact, we will take $l = m + r$ with $m$ given by (3.5) for an appropriate choice of the parameter $t$. We begin by rewriting the identity of Lemma 1 in the form
\begin{equation}
(3.23) \quad -a_{m+r} = S(m) - S(m-q) - S(m+r) + S(m-q+r).
\end{equation}
Basically this has the effect of casting $+r$ in the role of $-r$ in the previous argument with everything else being the same. In particular, the desired conclusion follows from (3.3) and from (3.4) with $-r$ replaced by $+r$.

Proceeding as before, we wish to supplement (3.9) with
\begin{equation}
(3.24) \quad x_{m+r} = \frac{p + 1}{2}, \quad x_{m-q+r} = \frac{p + 5}{2}, \quad y_{m+r} = q - \tau - 1 = y_{m-q+r},
\end{equation}
which are computed in the same fashion.

Next come computations of the left side of (2.6). The ranges \(m - p < n \leq m\) and \(m - q - p < n \leq m - q\) lead to functions \(f_1\) and \(f_2\), as before. For the new ranges \(m + r - p < n \leq m + r\) and \(m - q + r - p < n \leq m - q + r\) we proceed as before but use (3.22) in place of (3.9) to get

\[
(3.23) \quad f_5(k) = \left\{ \frac{p + 1 + 2k}{2p} \right\} + \left\{ \frac{q - \tau - 1 - \tau k}{q} \right\},
\]

\[
(3.24) \quad f_6(k) = \left\{ \frac{p + 5 + 2k}{2p} \right\} + \left\{ \frac{q - \tau - 1 - \tau k}{q} \right\},
\]

respectively, with \(0 \leq k < p\). In particular, one readily verifies that, as in (3.14), we have

\[
(3.25) \quad f_2(k), f_5(k), f_6(k) \geq \frac{1}{2} - \frac{1}{2p} + \frac{1}{pq},
\]

Now, the evaluation of \(f_1\) is given in (3.10) and, as before, we define \(\rho\) by (3.11). This time, however, we have a smaller range \(0 \leq c - 1 \leq (p - 3)/2\), which leads us to replace (3.12) by

\[
(3.26) \quad f_1(k) \leq \rho \leq f_1\left(\frac{p - 3}{2}\right) = \frac{1}{2} - \frac{1}{2p} - \frac{2}{pq},
\]

for \(0 \leq k \leq c - 1\). Of course, for \(k \geq c\) the inequality (3.13) is in effect.

Next come computations of the right side of (2.6). Once again we fix the parameter \(t\) in the definition (3.5) of \(m\) so that (3.15) and hence (3.16)–(3.18) hold. In addition to these we now need the upper bounds

\[
(3.27) \quad \frac{m + r - k}{pqr}, \quad \frac{m + r - q - k}{pqr} \leq \frac{m - (p - 1)/2}{pqr} + \frac{r + (p - 1)/2}{pqr} < \rho + \frac{3}{pq},
\]

Finally, we come to the last stage of our argument where we use Lemma 2 and (2.5) to evaluate \(\chi\) and \(S\) respectively. The identities (3.19)–(3.21) and hence (3.3) and (5.4) hold as before. In addition, by (3.25)–(3.27), we have

\[
\chi(m + r - k) = \chi(m - q + r - k) = 0,
\]

for \(0 \leq k < p\). This implies the validity of (3.14) with \(-r\) replaced by \(+r\), and completes the proof of the first claim of the theorem.

Before continuing to the second claim of the theorem we remark that the choice \(c = (p + 1)/2\) does not yield a coefficient \(a_i = -(p + 1)/2\). Indeed, taking this value of \(c\) does give \(S(m) = (p + 1)/2\), as we have seen in (3.3), but it also leads to \(S(m + r) = 1\). To see this, consider (2.6) for \(n = m + r - (p - 1)/2\). On the left side we get, by (3.22) and (3.12),

\[
f_5\left(\frac{p - 1}{2}\right) = \frac{1}{2} - \frac{1}{2p} + \frac{1}{pq} = f_1\left(\frac{p - 1}{2}\right) + \frac{r}{pq},
\]

and comparing this to the right side we see that

\[
\chi(m + r - (p - 1)/2) = \chi(m - (p - 1)/2) = 1.
\]

We now consider the second claim of the theorem. This is settled by an argument essentially identical to the one given in support of the first claim. Consequently, we will not reproduce it here but, instead, specify the choices of all the crucial
parameters so that the reader will have no difficulty reproducing this argument by mimicking the proof of the first claim.

Fixing an odd prime $p$, we take $q$ of the form (3.3), as before. This time, however, we take $r$ satisfying, in addition to $r > pq$, the congruence $r \equiv (pq+1)/2 \pmod{pq}$, so that in place of (3.2) we have $r \equiv (p+1)/2 \pmod{p}$ and $r \equiv (q+1)/2 \pmod{q}$. Our choice of $m$ will be the same as before and is given in (3.5).

We will also want to rewrite the identity of Lemma 1 in the form

$$-a_{m+p-1+q} = S(m+p-1) - S(m+p-1+q) - S(m+p-1-r) + S(m+p-1+q-r).$$

This specifies all the crucial parameters needed for the proof, and we end with one final remark. In the present case the representation (2.2) of 1 has coefficients $u = 1$ and $v = q - r$. Comparing this with (3.3), we see that $+1$ acts as $-1$ did before, and it is now more convenient to do computations of the left side of (2.6) with $m + k$, $0 \leq k < p$.

REFERENCES


[2] A. S. Bang, Om Ligningen $\Phi_n(x) = 0$, Tidsskrift for Mathematic 6 (1895), 6–12.


Department of Mathematical Sciences, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, Nevada 89154-4020

E-mail address: bachman@unlv.nevada.edu