Bull. Korean Math. Soc. **51** (2014), No. 4, pp. 949–955
http://dx.doi.org/10.4134/BKMS.2014.51.4.949

A NOTE ON TERNARY CYCLOTOMIC POLYNOMIALS

Bin Zhang

Abstract. Let $\Phi_n(x) = \sum_{k=0}^{\phi(n)} a(n,k)x^k$ denote the n-th cyclotomic polynomial. In this note, let $p < q < r$ be odd primes, where $q \not\equiv 1 \pmod p$ and $r \equiv -2 \pmod{pq}$, we construct an explicit k such that $a(pqr, k) = -2$.

1. Introduction

The n-th cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{\substack{1\le j\le n \\ (j,n)=1}} (x - e^{2\pi i j/n}) = \sum_{k=0}^{\phi(n)} a(n,k)x^k,$$

where ϕ is the Euler totient function. The coefficients $a(n,k)$ are known to be integral. Let $A(n)$ be the largest absolute value of the coefficients of $\Phi_n(x)$. We say that a cyclotomic polynomial is *flat* if $A(n) = 1$. It is easy to see that $A(n) = A(m)$, where $n > 1$ is a positive integer and m is the product of the distinct primes dividing n. It is also easy to verify that if n is odd, then $A(2n) = A(n)$. Thus for the purpose of studying coefficients of $\Phi_n(x)$, it suffices to consider only odd square-free integers n.

Obviously, $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ is flat, where p is a prime. Let $\omega(n)$ be the number of distinct odd prime factors of n. For square-free n, this number $\omega(n)$ is the *order* of the cyclotomic polynomial $\Phi_n(x)$. The case where $\omega(n) = 2$ has been studied by several authors (see [4, 8, 10, 13]), and our understanding of it is rather complete. In particular, the coefficients of $\Phi_{pq}(x)$ are computed in the following lemma. For a proof, see, for example, Lam and Leung [8] or Thangadurai [13].

Received June 25, 2013; Revised November 13, 2013.
2010 *Mathematics Subject Classification.* 11B83, 11C08, 11N56.
Key words and phrases. cyclotomic polynomial, coefficients of cyclotomic polynomial, ternary cyclotomic polynomial.
This work was supported by Project of Graduate Education Innovation of Jiangsu Province (Grant No. KYLX_0690), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20133207110012) and National Natural Science Foundation of China (Grant No. 10971098).

Lemma 1.1. *Let $p < q$ be odd primes. Let s and t be positive integers such that $pq + 1 = ps + qt$ written uniquely. Then we have*

$$a(pq, i) = \begin{cases} 1 & \text{if } i = up + vq \text{ for some } 0 \le u \le s-1,\ 0 \le v \le t-1; \\ -1 & \text{if } i = up + vq - pq \text{ for some } s \le u \le q-1,\ t \le v \le p-1; \\ 0 & \text{otherwise.} \end{cases}$$

There have been extensive studies on the coefficients of cyclotomic polynomials of order three. If $\omega(n) = 3$, then $\Phi_n(x)$ is also said to be *ternary*.

Let $3 < p < q < r$ be primes satisfying $q \equiv 2 \pmod p$ and $2r \equiv -1 \pmod{pq}$. In 1936, Lehmer [9] proved that $a(pqr, (p-3)(qr+1)/2) = (p-1)/2$, and in 1971, Möller [11] showed that $a(pqr, (p-1)(qr+1)/2) = (p+1)/2$.

In 2006, Bachman [1] first established the existence of an infinite family of flat ternary cyclotomic polynomials.

Given odd primes $p < q$, in 2007, Kaplan [7] proved that $A(pqr) = 1$ for every prime $r \equiv \pm 1 \pmod{pq}$. The author also showed that

$$A(pqr) = A(pqs) \tag{1.1}$$

whenever $s > q$ is a prime congruent to $\pm r \pmod{pq}$.

Let $p < q < r$ be odd primes. In 2010, Zhao and Zhang [14] showed that

$$A(pqr) \le \min\{\overline{r}, pq - \overline{r}\}, \tag{1.2}$$

where $\overline{r}$ is the unique integer such that $0 \le \overline{r} \le pq - 1$ and $\overline{r} \equiv r \pmod{pq}$ (see Bachman and Moree [2] or Elder [5] for different proofs).

In 2012, Elder [5] analyzed the coefficients of $\Phi_n(x)$ by considering it as a gcd of simpler polynomials. In the case where $r \equiv \pm 2 \pmod{pq}$, the author used this theory to prove that $A(pqr) = 1$ if and only if $q \equiv 1 \pmod p$.

There are also papers on the coefficients of inverse cyclotomic polynomials (see Moree [12], Bzdęga [3]) and on maximum gap in (inverse) cyclotomic polynomials (see Hong, Lee, Lee and Park [6]).

In this note, we continue the discussion of ternary cyclotomic polynomials. Our purpose here is to establish the following main result, giving a prescribed coefficient of ternary cyclotomic polynomial $\Phi_{pqr}(x)$ which equals -2.

Theorem 1.2. *Let $p < q < r$ be odd primes, where $q = kp + \ell$ for some $2 \le \ell \le p - 1$, and $r \equiv -2 \pmod{pq}$.*

(a) *If ℓ is odd, then $a(pqr, pqr - pr - 2qr + p - \ell - 2) = -2$.*

(b) *If ℓ is even, then $a(pqr, pqr - pr - 2qr + \ell r + \ell - 2) = -2$.*

Together with (1.1), (1.2) and Theorem 1.2, we obtain:

Corollary 1.3. *Let $p < q < r$ be odd primes such that $r \equiv \pm 2 \pmod{pq}$. If $q \not\equiv 1 \pmod p$, then $A(pqr) = 2$.*

2. Preliminaries

We will first introduce some lemmas which are useful to prove our theorem.

Lemma 2.1. *The nonzero coefficients of $\Phi_{pq}(x)$ alternate between $+1$ and -1.*

Proof. See Lam and Leung [8]. □

Let $p < q < r$ be odd primes and $\Phi_{pqr}(x) = \sum_{n=0}^{\phi(pqr)} a(pqr, n)x^n$. Kaplan [7] proved the following two lemmas.

Lemma 2.2. *Let $p < q < r$ be odd primes. Let n be a non-negative integer and $f(i)$ be the unique value $0 \le f(i) < pq$ such that*

$$rf(i) + i \equiv n \pmod{pq}. \tag{2.1}$$

Then

$$\sum_{i=0}^{p-1} a(pq, f(i)) = \sum_{j=0}^{p-1} a(pq, f(q + j)).$$

Lemma 2.3. *Let $p < q < r$ be odd primes. Let $0 \le n \le \phi(pqr)$ be an integer. Put*

$$a^*(pq, i) = \begin{cases} a(pq, i) & \text{if } ri \le n; \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$a(pqr, n) = \sum_{i=0}^{p-1} a^*(pq, f(i)) - \sum_{j=0}^{p-1} a^*(pq, f(q + j)),$$

where $f(i)$ is the unique value $0 \le f(i) < pq$ such that $rf(i) + i \equiv n \pmod{pq}$.

We now provide bounds for the values s and t in the equation $pq+1 = ps+qt$ used in the proof of main theorem.

Lemma 2.4. *Let $p < q$ be odd primes with $q = kp + \ell$ for some $2 \le \ell \le p - 1$. Let s, t be the unique integers $1 \le s \le q - 1$, $1 \le t \le p - 1$, such that $pq + 1 = ps + qt$. Then* (i) $2 \le t \le p - 1$; (ii) $s \le q - k - 2$; (iii) $s \ge k + 1$.

Proof. (i) Since $t = 1$ if and only if $q \equiv 1 \pmod p$, we have $2 \le t \le p - 1$.

(ii) To prove this statement, we will show that $ps \le p(q - k - 2)$. Note that $\ell t \equiv 1 \pmod p$ and $t \ge 2$. So $\ell t \ge p + 1$. Then $tkp + \ell t - 1 \ge kp + 2p$. Since

$$ps = pq + 1 - qt = pq - (tkp + \ell t - 1),$$
$$p(q - k - 2) = pq - kp - 2p = pq - (kp + 2p),$$

we have $ps \le p(q - k - 2)$, implying that $s \le q - k - 2$, as desired.

(iii) Note that $t = p - 1$ if and only if $\ell = p - 1$. If $t = p - 1$, then

$$ps = pq + 1 - qt = q + 1 = kp + p,$$

implying that $s = k+1$. If $t < p-1$, then $ps = pq+1-qt \ge 2q+1 > (k+1)p$. So $s \ge k + 1$. This completes the proof of Lemma 2.4. □

3. The Proof of Theorem 1.2(a)

For any positive integer n, by using the condition of Lemma 2.2, we have

$$rf(i) \equiv n - i \pmod{pq}, \quad 0 \leq f(i) \leq pq - 1.$$

It follows from $r \equiv -2 \pmod{pq}$ that

$$f(i+1) \equiv f(i) + \frac{pq+1}{2} \pmod{pq}; \tag{3.1}$$

$$f(i+2) \equiv f(i) + 1 \pmod{pq}. \tag{3.2}$$

In this section, let $q = kp + \ell$, $3 \leq \ell \leq p-2$ and ℓ is odd. We will show that $a(pqr, n) = -2$, where

$$n = pqr - pr - 2qr + p - \ell - 2.$$

Since $3 \leq \ell \leq p-2$, we have $p \geq 5$ and $t \leq p-2$. For $pq + 1 = ps + qt$, where s and t are positive integers, by Lemma 2.4, we have

$$2 \leq t \leq p-2 \ \text{ and } \ s \leq q - k - 2.$$

In order to use Lemma 2.3, we need to determine for which k will $rf(k) > n$. We will now prove that $rf(k) > n$ whenever $k \in \{p-\ell, p-\ell+2, \ldots, p-1\} \cup \{q+1, q+3, \ldots, q+p-2\}$, and $rf(k) \leq n$ whenever $k \in \{0, 2, \ldots, p-\ell-2\} \cup \{1, 3, \ldots, p-2\} \cup \{q, q+2, \ldots, q+p-1\}$.

It follows from (2.1), (3.1) and (3.2) that $f(p-\ell) = pq - p - 2q + 1$, $f(p-\ell-2) = pq - p - 2q$; $f(p-2) = \frac{pq+\ell}{2} - p - 2q$; $f(q+p-1) = \frac{pq-3q}{2} - p + \frac{\ell+1}{2}$; $f(q+p-2) = pq - p - \frac{3q-\ell}{2}$, $f(q+1) = pq - \frac{3p+3q}{2} + \frac{\ell+3}{2}$. Then one readily verifies the assertion.

Together with Lemma 2.3, we obtain that

$$\begin{aligned} a(pqr, n) &= \sum_{i=0}^{p-1} a^*(pq, f(i)) - \sum_{j=0}^{p-1} a^*(pq, f(q+j)) \\ &= \sum_{i=0}^{\frac{p-3}{2}} a(pq, f(2i+1)) + \sum_{i=0}^{\frac{p-\ell}{2}-1} a(pq, f(2i)) - \sum_{j=0}^{\frac{p-1}{2}} a(pq, f(q+2j)). \end{aligned}$$

Applying Lemma 2.2 to the above equation yields

$$\begin{aligned} a(pqr, n) &= \sum_{j=0}^{\frac{p-3}{2}} a(pq, f(q+2j+1)) - \sum_{i=0}^{\frac{p-1}{2}} a(pq, f(2i)) + \sum_{i=0}^{\frac{p-\ell}{2}-1} a(pq, f(2i)) \\ &= \sum_{j=0}^{\frac{p-3}{2}} a(pq, f(q+2j+1)) - \sum_{i=\frac{p-\ell}{2}}^{\frac{p-1}{2}} a(pq, f(2i)). \end{aligned} \tag{3.3}$$

It is easy to see

$$f(p-\ell) = (s-1)p + (t-2)q \ \text{ and } \ 0 \leq t-2 < t-1;$$

$$f(q+p-2) = (q - \frac{k}{2} - 1)p + (p-1)q - pq \quad \text{and}$$
$$s < q - \frac{k}{2} - 1 < q - 1.$$

Thus, by Lemma 1.1, we have

$$a(pq, f(p-\ell)) = 1, \quad a(pq, f(q+p-2)) = -1.$$

So equation (3.3) becomes

$$a(pqr, n) = \sum_{j=0}^{\frac{p-5}{2}} a(pq, f(q+2j+1)) - 1 - \sum_{i=\frac{p-\ell}{2}+1}^{\frac{p-1}{2}} a(pq, f(2i)) - 1.$$

On invoking Lemma 2.1 we have

$$\min\{x \mid x > f(p-\ell), a(pq,x) \neq 0\} = pq - p - 2q + \ell > f(p-1);$$
$$\max\{y \mid y < f(q+p-2), a(pq,y) \neq 0\} = pq - \frac{kp}{2} - 2p - q + 1 < f(q+1).$$

By using (3.2), we have $f(p-\ell), f(p-\ell+2), \ldots, f(p-1)$ are consecutive integers. So are $f(q+1), f(q+3), \ldots, f(q+p-2)$. Thus we obtain $a(pq, f(2i)) = 0$ for $\frac{p-\ell}{2} + 1 \leq i \leq \frac{p-1}{2}$ and $a(pq, f(q+2j+1)) = 0$ for $0 \leq j \leq \frac{p-5}{2}$.

Therefore, we get

$$a(pqr, n) = -1 - 1 = -2,$$

as desired.

4. The Proof of Theorem 1.2(b)

In this section, let $2 \leq \ell \leq p-1$ and ℓ is even, and we will show that $a(pqr, n) = -2$, where

$$n = pqr - pr - 2qr + \ell r + \ell - 2.$$

If $p = 3$, $q \equiv 2 \pmod 3$, we will prove $a(3qr, qr - r) = -2$. By using (2.1), we obtain $f(0) = q-1$, $f(2) = q$, $f(1) = \frac{5q-1}{2}$, $f(q) = 3q-1$, $f(q+2) = 0$ and $f(q+1) = \frac{3q-1}{2}$.

It is clear that

$$rf(1) > rf(2) > n = rf(0); \quad rf(q) > rf(q+1) > n > rf(q+2).$$

By using Lemma 2.3, we have

$$a(3qr, n) = a(3q, f(0)) - a(3q, f(q+2)).$$

Obviously, $a(3q, f(q+2)) = a(3q, 0) = 1$. We can rewrite $f(0) = q-1 = (\frac{2q-1}{3}) \cdot 3 + 2 \cdot q - 3q$, and so by Lemma 1.1, $a(3q, f(0)) = -1$. Hence, $a(3qr, qr-r) = -2$.

In what follows, we consider the case $p \geq 5$.

Proceeding as Section 3, for $pq+1 = ps+qt$, $q = kp+\ell$, by Lemma 2.4, we have

$$2 \leq t \leq p-1 \text{ and } k+1 \leq s \leq q-k-2.$$

In order to use Lemma 2.3, we need to determine for which k will $rf(k) > n$. We will now prove that $rf(k) > n$ whenever $k \in \{\ell, \ell+2, \ldots, p-1\} \cup \{q+1, q+3, \ldots, q+p-2\}$, and $rf(k) \leq n$ whenever $k \in \{0, 2, \ldots, \ell-2\} \cup \{1, 3, \ldots, p-2\} \cup \{q, q+2, \ldots, q+p-1\}$.

It follows from (2.1), (3.1) and (3.2) that $f(\ell) = pq - p - 2q + \ell + 1$, $f(\ell - 2) = pq - p - 2q + \ell$; $f(p-2) = \frac{pq-p-4q+\ell}{2}$; $f(q+p-1) = \frac{pq-p-3q+\ell+1}{2}$; $f(q+p-2) = pq - \frac{p+3q}{2} + \frac{\ell}{2}$, $f(q+1) = pq - p - \frac{3q-3}{2} + \frac{\ell}{2}$. Then one readily verifies the assertion.

Note that

$$f(\ell) = (s-k-1)p + (t-1)q \text{ and } 0 \leq s-k-1 < s-1;$$

$$f(q+p-2) = (q-1-\frac{k-1}{2})p + (p-1)q - pq \text{ and } s \leq q-1-\frac{k-1}{2} \leq q-1.$$

By Lemma 1.1, we have

$$a(pq, f(\ell)) = 1, \quad a(pq, f(q+p-2)) = -1. \tag{4.1}$$

Together with Lemma 2.3, Lemma 2.2 and (4.1), we obtain that

$$\begin{aligned}
a(pqr, n) &= \sum_{i=0}^{p-1} a^*(pq, f(i)) - \sum_{j=0}^{p-1} a^*(pq, f(q+j)) \\
&= \sum_{i=0}^{\frac{p-3}{2}} a(pq, f(2i+1)) + \sum_{i=0}^{\frac{\ell}{2}-1} a(pq, f(2i)) - \sum_{j=0}^{\frac{p-1}{2}} a(pq, f(q+2j)) \\
&= \sum_{j=0}^{\frac{p-3}{2}} a(pq, f(q+2j+1)) - \sum_{i=0}^{\frac{p-1}{2}} a(pq, f(2i)) + \sum_{i=0}^{\frac{\ell}{2}-1} a(pq, f(2i)) \\
&= \sum_{j=0}^{\frac{p-3}{2}} a(pq, f(q+2j+1)) - \sum_{i=\frac{\ell}{2}}^{\frac{p-1}{2}} a(pq, f(2i)) \\
&= \sum_{j=0}^{\frac{p-5}{2}} a(pq, f(q+2j+1)) - 1 - \sum_{i=\frac{\ell}{2}+1}^{\frac{p-1}{2}} a(pq, f(2i)) - 1.
\end{aligned}$$

On invoking Lemma 2.1 we have

$$\min\{x \mid x > f(\ell), a(pq, x) \neq 0\} = pq - 2q + \ell > f(p-1);$$

$$\max\{y \mid y < f(q+p-2), a(pq, y) \neq 0\} = pq - \frac{3p+3q-\ell}{2} + 1 < f(q+1).$$

By using (3.2), we have $f(\ell), f(\ell+2), \ldots, f(p-1)$ are consecutive integers. So are $f(q+1), f(q+3), \ldots, f(q+p-2)$. Thus we obtain $a(pq, f(2i)) = 0$ for $\frac{\ell}{2} + 1 \leq i \leq \frac{p-1}{2}$ and $a(pq, f(q+2j+1)) = 0$ for $0 \leq j \leq \frac{p-5}{2}$.

Finally, we have

$$a(pqr, n) = -1 - 1 = -2.$$

This completes the proof of Theorem 1.2.

Acknowledgements. I would like to thank Professor Chun-Gang Ji for useful discussions. I would also like to thank the referee for very valuable comments and helpful suggestions.

References

[1] G. Bachman, *Flat cyclotomic polynomials of order three*, Bull. London Math. Soc. **38** (2006), no. 1, 53–60.

[2] G. Bachman and P. Moree, *On a class of ternary inclusion-exclusion polynomials*, Integers **11** (2011), A8, 14 pp.

[3] B. Bzdęga, *On the height of cyclotomic polynomials*, Acta Arith. **152** (2012), no. 4, 349–359.

[4] L. Carlitz, *The number of terms in the cyclotomic polynomial* $F_{pq}(x)$, Amer. Math. Monthly **73** (1966), 979–981.

[5] S. Elder, *Flat Cyclotomic Polynomials*: *A New Approach*, arXiv:1207.5811v1, 2012.

[6] H. Hong, E. Lee, H. S. Lee, and C. M. Park, *Maximum gap in* (*inverse*) *cyclotomic polynomial*, J. Number Theory **132** (2012), no. 10, 2297–2315.

[7] N. Kaplan, *Flat cyclotomic polynomials of order three*, J. Number Theory **127** (2007), no. 1, 118–126.

[8] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly **103** (1996), no. 7, 562–564.

[9] E. Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomials*, Bull. Amer. Math. Soc. **42** (1936), no. 6, 389–392.

[10] H. W. Lenstra, *Vanishing sums of roots of unity*, in: Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, pp. 249–268, Math. Centre Tracts, 101, Math. Centrum, Amsterdam, 1979.

[11] H. Möller, *Über die Koeffizienten des n-ten Kreisteilungspolynoms*, Math. Z. **119** (1971), 33–40.

[12] P. Moree, *Inverse cyclotomic polynomials*, J. Number Theory **129** (2009), no. 3, 667–680.

[13] R. Thangadurai, *On the coefficients of cyclotomic polynomials*, in: Cyclotomic fields and related topics (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.

[14] J. Zhao and X. K. Zhang, *Coefficients of ternary cyclotomic polynomials*, J. Number Theory **130** (2010), no. 10, 2223–2237.

School of Mathematical Sciences
Nanjing Normal University
Nanjing 210023, P. R. China
E-mail address: zhangbin100902025@163.com