Bull. Korean Math. Soc. **54** (2017), No. 1, pp. 43–50
https://doi.org/10.4134/BKMS.b150339
pISSN: 1015-8634 / eISSN: 2234-3016

# THE HEIGHT OF A CLASS OF TERNARY CYCLOTOMIC POLYNOMIALS

Bin Zhang

Abstract. Let $A(n)$ denote the largest absolute value of the coefficients of $n$-th cyclotomic polynomial $\Phi_n(x)$ and let $p < q < r$ be odd primes. In this note, we give an infinite family of cyclotomic polynomials $\Phi_{pqr}(x)$ with $A(pqr) = 3$, without fixing $p$.

## 1. Introduction

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

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

where $\phi$ is the Euler totient function. Let the *height* of $\Phi_n(x)$, written as $A(n)$, be the maximum absolute value of the coefficients of $\Phi_n(x)$. Using basic properties of such polynomials, the height of $\Phi_n(x)$ can be shown to depend only on the set of odd primes dividing $n$. If $n$ has at most two different odd prime factors, then $A(n) = 1$. So the easiest case that we can expect non-trivial behavior of the coefficients of $\Phi_n(x)$ is the *ternary* case, where $n$ is a product of three distinct odd primes. In the remainder of this paper, we assume that $p < q < r$ are odd primes (unless otherwise specified).

Recently there has been much progress in our understanding of the coefficients of $\Phi_{pqr}(x)$, but a number of interesting questions remain open. Various authors have studied the upper bounds for $A(pqr)$. Instead we can give conditions on $p$, $q$, $r$ so that $A(pqr)$ is small.

Received May 8, 2015; Revised March 11, 2016.
2010 *Mathematics Subject Classification.* 11B83, 11C08.
*Key words and phrases.* height of a cyclotomic polynomial, ternary cyclotomic polynomial, coefficient.
This work was supported by National Natural Science Foundation of China (Grant Nos. 11626137, 11471162), Natural Science Foundation of Shandong Province (Grant No. ZR2016AP10) and Science and Technology Project of Qufu Normal University (Grant No. xkj201605).

In 1978, Beiter [4] gave a characterization of $q$ and $r$ such that $A(3qr) = 1$. Bachman [1] was the first to provide an infinite family of cyclotomic polynomials $\Phi_{pqr}(x)$ with $A(pqr) = 1$. Specifically, he showed that if

$$p \geq 5, \quad q \equiv -1 \pmod{p} \quad \text{and} \quad r \equiv +1 \pmod{pq}, \tag{1.1}$$

then $A(pqr) = 1$. This result was generalized by Flanagan [8] and improved by Kaplan [11]. There have been also studies of $\Phi_{pqr}(x)$ with $A(pqr) = 1$, see [6, 7, 10, 16]. In [11], Kaplan established the following periodicity of the function $A(pqr)$.

**Proposition 1.1** (Kaplan). *Let $p < q < r$ be odd primes. Then for any prime $s > q$ such that $s \equiv \pm r \pmod{pq}$, $A(pqr) = A(pqs)$.*

Without fixing $p$, the first infinite family of ternary cyclotomic polynomials $\Phi_{pqr}(x)$ with height exactly 2 was given by Elder [7], which showed that if

$$q \not\equiv 1 \pmod{p} \quad \text{and} \quad r \equiv \pm 2 \pmod{pq},$$

then $A(pqr) = 2$ (see Zhang [15] for another proof of this result).

We now turn our attention to the ternary cyclotomic polynomials with height 3. Many such results can be found in the literature, for instance:

(1) In 1971, Möller [13] showed that $a(pqr, (p-1)(qr+1)/2) = (p+1)/2$ in the case $p \geq 5$, $q \equiv 2 \pmod{p}$ and $2r \equiv -1 \pmod{pq}$. Considering Möller's result with $p = 5$ and using the general fact $A(5qr) \leq 3$ (established independently by Beiter [3] and Bloom [5]), we obtain that $A(5qr) = 3$ when $q \equiv 2 \pmod{5}$ and $2r \equiv -1 \pmod{5q}$. We refer the reader to the paper of Gallot, Moree and Wilms [9] which gives a more detailed description of $A(5qr)$.

(2) Given any triplet of odd primes $p_0 < q_0 < r_0$ such that $A(p_0q_0r_0) = 3$, we can use Proposition 1.1 to produce an infinite family of $\Phi_{p_0q_0r}(x)$ satisfying $A(p_0q_0r) = 3$: For any prime $r \equiv \pm r_0 \pmod{p_0q_0}$, $A(p_0q_0r) = 3$.

(3) In 2011, Gallot, Moree and Wilms [9] proved that if $p \geq 5$ and $2p - 1$ is a prime, then for appropriate $r$, $A(p(2p-1)r) = 3$.

Note that we do not know whether there are infinitely many prime-pairs $(p, 2p-1)$. We remark that as far as we are aware, there were no published results on the existence of an infinite family of ternary cyclotomic polynomials $\Phi_{pqr}(x)$ with $A(pqr) = 3$, without fixing $p$. It is for this reason that we write this paper to establish the following result.

**Theorem 1.2.** *For every prime $p \equiv 1 \pmod{3}$, there exist infinitely many pairs of primes $q$ and $r$, $p < q < r$, such that $A(pqr) = 3$. In particular, this is certainly true for any $q$ and $r$ of the form*

$$q \equiv 2p + 2 \pmod{3p} \quad \textit{and} \quad r \equiv \pm 3 \pmod{pq}.$$

*Remark* 1.3. (1) Note that $\gcd(2p+2, 3p) = 1$ when $p \equiv 1 \pmod{3}$. The existence of infinitely many triples of primes $(p, q, r)$ satisfying the condition of Theorem 1.2 is guaranteed by Dirichlet's theorem on primes in arithmetic progressions.

(2) As far as we can see, this is the first infinite family of ternary cyclotomic polynomials $\Phi_{pqr}(x)$ with height exactly 3, without fixing $p$.

## 2. Preliminaries

In this section, we introduce several lemmas which are useful to prove our theorem.

**Lemma 2.1.** *Let $p < q$ be odd primes, and let $s$ and $t$ be positive integers such that $pq + 1 = ps + qt$. Then*

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

*Proof.* See Lam and Leung [12] or Thangadurai [14]. □

**Lemma 2.2.** *Let $p < q$ be odd primes with $q \equiv 2 \pmod p$. Then*

$$a(pq, j) = \begin{cases} 1 & \text{if } j = up + vq \text{ with } 0 \le u \le \frac{pq-2p-q+2}{2p},\ 0 \le v \le \frac{p-1}{2}; \\ -1 & \text{if } j = up + vq + 1 \text{ with } 0 \le u \le \frac{pq-2p+q-2}{2p},\ 0 \le v \le \frac{p-3}{2}; \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* A consequence of the fact $pq + 1 = p \cdot \frac{pq-q+2}{2p} + q \cdot \frac{p+1}{2}$ and Lemma 2.1. □

**Lemma 2.3.** *Let $p < q < r$ be odd primes. Let $n \ge 0$ be an integer and $f(i)$ be the unique value $0 \le f(i) \le pq - 1$ such that*

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

*Put*

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

*Then*

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

*Proof.* See Kaplan [11]. □

**Lemma 2.4.** *Let $p < q < r$ be odd primes and $w$ be an integer such that $0 < w \le pq - 1$ and $r \equiv \pm w \pmod{pq}$. Then*

$$A(pqr) \le w.$$

*Proof.* See Zhao and Zhang [17], Bachman and Moree [2] or Elder [7]. □

## 3. Proof of Theorem 1.2

By Proposition 1.1, we only consider primes $r$ such that $r \equiv 3 \pmod{pq}$. On considering Lemma 2.4 with $w = 3$, we know that, to prove Theorem 1.2, it suffices to specify a coefficient $a(pqr, n)$ which equals 3 or $-3$ for any triple $(p, q, r)$ of the form $p \equiv 1 \pmod 3$, $q \equiv 2p + 2 \pmod{3p}$ and $r \equiv 3 \pmod{pq}$. Now according to the values of $p$, we distinguish the following two parts to give the desired coefficients.

• **Part 1:** $p = 7$**.**

For primes $7 < q < r$ satisfying $q \equiv 16 \pmod{21}$ and $r \equiv 3 \pmod{7q}$, we claim that

$$a(7qr, \frac{7qr + 2r}{3} + q + 5) = 3.$$

Let $n = (7qr+2r)/3+q+5$. In order to use Lemma 2.3, we need to determine for which $l$ will $rf(l) > n$. Note that $rf(l) + l \equiv n \pmod{7q}$, where $0 \leq l \leq 6$ and $q \leq l \leq q + 6$.

For $i = 0, 1, 2$, we have

$$\begin{aligned} rf(3i) + 3i &\equiv (7qr + 2r)/3 + q + 5 \pmod{7q}; \\ rf(q + 3i) + q + 3i &\equiv (7qr + 2r)/3 + q + 5 \pmod{7q}. \end{aligned}$$

It follows from $r \equiv 3 \pmod{7q}$ that

$$\begin{aligned} 3f(3i) &\equiv q + 7 - 3i \pmod{7q}; \\ 3f(q + 3i) &\equiv 7 - 3i \pmod{7q}. \end{aligned}$$

Since $0 \leq f(l) \leq 7q - 1$, we obtain

$$f(3i) = \frac{8q + 7}{3} - i \quad \text{and} \quad f(q + 3i) = \frac{14q + 7}{3} - i.$$

For $j = 0, 1$, we get

$$\begin{aligned} rf(3j + 1) + 3j + 1 &\equiv (7qr + 2r)/3 + q + 5 \pmod{7q}; \\ rf(q + 3j + 1) + q + 3j + 1 &\equiv (7qr + 2r)/3 + q + 5 \pmod{7q}; \\ rf(3j + 2) + 3j + 2 &\equiv (7qr + 2r)/3 + q + 5 \pmod{7q}; \\ rf(q + 3j + 2) + q + 3j + 2 &\equiv (7qr + 2r)/3 + q + 5 \pmod{7q}. \end{aligned}$$

Similarly, by using $r \equiv 3 \pmod{7q}$ and $0 \leq f(l) \leq 7q - 1$, we infer that

$$\begin{aligned} f(3j + 1) &= 5q + 2 - j, \qquad & f(q + 3j + 1) &= 2 - j; \\ f(3j + 2) &= \frac{q + 5}{3} - j, \qquad & f(q + 3j + 2) &= \frac{7q + 5}{3} - j. \end{aligned}$$

Then one readily verifies that $rf(l) < n$ whenever $l \in I_1 := \{2, 5, q + 1, q + 4, q + 5\}$, and $rf(l) > n$ whenever $l \in I_2 := \{0, 1, 3, 4, 6, q, q + 2, q + 3, q + 6\}$. So

$$a^*(7q, f(l)) = \begin{cases} a(7q, f(l)) & \text{if } l \in I_1; \\ 0 & \text{if } l \in I_2. \end{cases}$$

By Lemma 2.3, it follows that

$$\begin{aligned} a(7qr, n) = &\sum_{i=0}^{6} a^*(7q, f(i)) - \sum_{j=0}^{6} a^*(7q, f(q+j)) \\ &= a(7q, f(2)) + a(7q, f(5)) - a(7q, f(q+1)) - a(7q, f(q+4)) \\ &\quad - a(7q, f(q+5)). \end{aligned}$$

Observe that

$$\begin{aligned} f(2) &= \frac{q+5}{21} \cdot 7 + 0 \cdot q \text{ and } 0 \le \frac{q+5}{21} \le \frac{7q - 2\cdot 7 - q + 2}{2 \cdot 7}; \\ f(q+4) &= 0 \cdot p + 0 \cdot q + 1; \\ f(q+5) &= \frac{4q-1}{21} \cdot 7 + 1 \cdot q + 1 \text{ and } 0 \le \frac{4q-1}{21} \le \frac{7q - 2 \cdot 7 + q - 2}{2 \cdot 7}. \end{aligned}$$

Considering Lemma 2.2 with $p = 7$, we have

$$a(7q, f(2)) = 1 \text{ and } a(7q, f(q+4)) = a(7q, f(q+5)) = -1.$$

Note that $f(5) = (q+2)/3$ and $f(q+1) = 2$. By using Lemma 2.2, it is straightforward to show that $a(7q, f(5)) = a(7q, f(q+1)) = 0$. Hence

$$a(7qr, n) = 1 + 0 - 0 - (-1) - (-1) = 3.$$

• **Part 2:** $p > 7$.

For primes $7 < p < q < r$ such that $p \equiv 1 \pmod 3$, $q \equiv 2p + 2 \pmod{3p}$ and $r \equiv 3 \pmod{pq}$, we will show that

$$a(pqr, \frac{pqr + 2r}{3} + qr + p + q - 2) = 3.$$

Let $n = (pqr + 2r)/3 + qr + p + q - 2$. For the purpose of using Lemma 2.3, we first need to determine for which $l$ will $rf(l) > n$. As in the proof of Part 1, by substituting $n$ into congruence $rf(l) + l \equiv n \pmod{pq}$, where $l \in [0, p-1] \cup [q, q+p-1]$, we have

$$\begin{aligned} rf(3i) + 3i &\equiv (pqr + 2r)/3 + qr + p + q - 2 \pmod{pq}, \\ rf(q+3i) + q + 3i &\equiv (pqr + 2r)/3 + qr + p + q - 2 \pmod{pq} \end{aligned}$$

for $0 \le i \le \frac{p-1}{3}$. From this and $r \equiv 3 \pmod{pq}$ it follows that

$$\begin{aligned} 3f(3i) &\equiv p + 4q - 3i \pmod{pq}; \\ 3f(q+3i) &\equiv p + 3q - 3i \pmod{pq}. \end{aligned}$$

Therefore, by $0 \le f(l) \le pq - 1$, we have

$$f(3i) = \frac{pq + p + q}{3} + q - i \quad \text{and} \quad f(q+3i) = \frac{2pq + p}{3} + q - i.$$

For $0 \le j \le \frac{p-4}{3}$, we have the following congruences

$$\begin{aligned} rf(3j+1) + 3j + 1 &\equiv (pqr + 2r)/3 + qr + p + q - 2 \pmod{pq}; \\ rf(q+3j+1) + q + 3j + 1 &\equiv (pqr + 2r)/3 + qr + p + q - 2 \pmod{pq}; \end{aligned}$$

$$rf(3j+2)+3j+2 \equiv (pqr+2r)/3+qr+p+q-2 \pmod{pq};$$
$$rf(q+3j+2)+q+3j+2 \equiv (pqr+2r)/3+qr+p+q-2 \pmod{pq}.$$

It follows from $r \equiv 3 \pmod{pq}$ and $0 \le f(l) \le pq-1$ that

$$f(3j+1)=\frac{2pq+p+q-1}{3}+q-j, \qquad f(q+3j+1)=\frac{p-1}{3}+q-j;$$
$$f(3j+2)=\frac{p+q-2}{3}+q-j, \qquad f(q+3j+2)=\frac{pq+p-2}{3}+q-j.$$

Then it is easy to check that $rf(l)<n$ whenever $l \in I_3 := \{2,5,\dots,p-2\} \cup \{q+1,q+4,\dots,q+p-3\} \cup \{q+p-2\}$, and $rf(l)>n$ whenever $l \in I_4 := \{0,3,\dots,p-1\} \cup \{1,4,\dots,p-3\} \cup \{q,q+3,\dots,q+p-1\} \cup \{q+2,q+5,\dots, q+p-5\}$. Thus

$$a^*(pq,f(l))=\begin{cases} a(pq,f(l)) & \text{if } l \in I_3; \\ 0 & \text{if } l \in I_4. \end{cases}$$

So, by Lemma 2.3,

$$a(pqr,n)=\sum_{j=0}^{\frac{p-4}{3}} a(pq,f(3j+2)) - \sum_{j=0}^{\frac{p-4}{3}} a(pq,f(q+3j+1)) - a(pq,f(q+p-2)). \tag{3.1}$$

On noting that $f(2)=\frac{p+q-2}{3p}p+q$, $f(5)=\frac{p+4q-8}{3p}p+1$, $f(8)=\frac{p+4q-8}{3p}p$, $f(q+p-3)=q+1$ and $f(q+p-2)=\frac{pq+q-2}{6p}p+\frac{p+5}{6}q+1$, we infer from Lemma 2.2 that $a(pq,f(2))=a(pq,f(8))=1$ and $a(pq,f(5))=a(pq,f(q+p-3))=a(pq,f(q+p-2))=-1$. Then the equality (3.1) becomes

$$a(pqr,n)=3+\sum_{j=3}^{\frac{p-4}{3}} a(pq,f(3j+2)) - \sum_{j=0}^{\frac{p-7}{3}} a(pq,f(q+3j+1)). \tag{3.2}$$

Let $3 \le j \le \frac{p-4}{3}$. Now we claim that $a(pq,f(3j+2)) \ne -1$. If the assertion would not hold, by Lemma 2.2, then there exist non-negative integers $u$ and $v$ such that

$$f(3j+2)=\frac{p+q-2}{3}+q-j=up+vq+1. \tag{3.3}$$

Note that $0<f(3j+2)<2q$. So $v=0$ or 1. On the other hand, taking the latest equality of (3.3) modulo $p$ gives

$$2v+j-1 \equiv 0 \pmod{p}, \tag{3.4}$$

thus

$$j \pm 1 \equiv 0 \pmod{p},$$

which is impossible, since $3 \le j \le \frac{p-4}{3}$.

Let $0 \le j \le \frac{p-7}{3}$. Analogously, we show that $a(pq, f(q+3j+1)) \neq 1$. If otherwise, by Lemma 2.2, then there exist $u, v \in \mathbb{Z}_{\ge 0}$ satisfying

$$f(q+3j+1) = \frac{p-1}{3} + q - j = up + vq. \tag{3.5}$$

According to $0 < f(q+3j+1) < 2q$, we also have $v = 0$ or $1$. On taking (3.5) modulo $p$, we obtain

$$6v + 3j - 5 \equiv 0 \pmod{p}. \tag{3.6}$$

Since $0 \le j \le \frac{p-7}{3}$, congruence (3.6) is invalid for both $v = 0$ and $v = 1$, a contradiction.

Finally, by Lemma 2.2 and (3.2), we deduce that $a(pqr, n) \ge 3$, and then, by Lemma 2.4, $a(pqr, n) = 3$. This completes the proof of Theorem 1.2.

**Acknowledgements.** We would like to thank the referees for 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, 1–14.

[3] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}$. II*, Duke Math. J. **38** (1971), 591–594.

[4] ———, *Coefficients of the cyclotomic polynomial $F_{3qr}(x)$*, Fibonacci Quart. **16** (1978), no. 4, 302–306.

[5] D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly **75** (1968), 372–377.

[6] D. Broadhurst, *Flat ternary cyclotomic polynomials*, http://tech.groups.yahoo.com/group/primenumbers/message/20305(2009).

[7] S. Elder, *Flat cyclotomic polynomials: a new approach*, arXiv:1207.5811v1, 2012.

[8] T. J. Flanagan, *On the coefficients of ternary cyclotomic polynomials*, MS Thesis, University of Nevada Las Vegas, 2006.

[9] Y. Gallot, P. Moree, and R. Wilms, *The family of ternary cyclotomic polynomials with one free prime*, Involve **4** (2011), no. 4, 317–341.

[10] C. G. Ji, *A special family of cyclotomic polynomials of order three*, Science China Math. **53** (2010), 2269–2274.

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

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

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

[14] R. Thangadurai, *On the coefficients of cyclotomic polynomials*, in: Cyclotomic Fields and Related Topics, Pune, 1999, 311–322, Bhaskaracharya Pratishthana, Pune, 2000.

[15] B. Zhang, *A note on ternary cyclotomic polynomials*, Bull. Korean Math. Soc. **51** (2014), no. 4, 949–955.

[16] B. Zhang and Y. Zhou, *On a class of ternary cyclotomic polynomials*, Bull. Korean Math. Soc. **52** (2015), no. 6, 1911–1924.

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

Bin Zhang
School of Mathematical Sciences
Qufu Normal University
Qufu 273165, P. R. China
*E-mail address*: zhangbin100902025@163.com