Bull. Math. Soc. Sci. Math. Roumanie
Tome 66 (114), No. 1, 2023, 89–95

A family of non-flat ternary cyclotomic polynomials

by

Bin Zhang

Abstract

Let $\Phi_n(x)$ be the n-th cyclotomic polynomial, $p < q < r$ be odd primes, and z be an integer such that $zr \equiv \pm 1 \pmod{pq}$. There have been extensive studies about the flatness of ternary cyclotomic polynomials $\Phi_{pqr}(x)$ for special cases of z. We present some classes of non-flat ternary cyclotomic polynomials for the general cases of z.

Key Words: Coefficients of cyclotomic polynomial, ternary cyclotomic polynomial, non-flat cyclotomic polynomial.
2010 Mathematics Subject Classification: Primary 11B83; Secondary 11C08.

1 Introduction

Let

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

be the n-th cyclotomic polynomial, where ϕ is Euler's function. The coefficients $a(n,m)$ are known to be integral. We define the height of $\Phi_n(x)$ to be

$$A(n) := \max\{|a(n,m)| : 0 \le m \le \phi(n)\}.$$

If $A(n) = 1$, then we say that $\Phi_n(x)$ is flat. By using basic properties of cyclotomic polynomials, it is easy to see that in the investigation about the coefficients of $\Phi_n(x)$ we can reduce our enquiry to the case when n is odd and square-free.

Throughout the paper, the letters p, q and r will always mean odd primes with $p < q < r$. It follows from $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ and the following proposition that if n has at most two distinct odd prime factors, then $\Phi_n(x)$ is flat.

Proposition 1. ([6, 10]) *Let s and t be the unique positive integers such that $pq+1 = sp+tq$. Then*

$$\Phi_{pq}(x) = \sum_{u=0}^{s-1}\sum_{v=0}^{t-1} x^{up+vq} - \sum_{u=0}^{q-s-1}\sum_{v=0}^{p-t-1} x^{up+vq+1}.$$

Also, for $0 \le m \le (p-1)(q-1)$, we have

(1) $a(pq,m) = 1$ *if and only if* $m = up + vq$ *with* $0 \le u \le s-1$ *and* $0 \le v \le t-1$;

(2) $a(pq,m) = -1$ *if and only if* $m = up + vq + 1$ *with* $0 \le u \le q-s-1$ *and* $0 \le v \le p-t-1$;

(3) $a(pq,m) = 0$ *otherwise.*

In 1883, Migotti [8] noted that $a(3 \cdot 5 \cdot 7, 7) = -2$. Thus the easiest case where we can expect non-trivial behavior of the coefficients of $\Phi_n(x)$ is the ternary case $n = pqr$. In 2006, Bachman [1] established the existence of an infinite family of flat ternary cyclotomic polynomials by showing that $A(pqr) = 1$ when $p \geq 5$, $q \equiv -1 \pmod{p}$ and $r \equiv 1 \pmod{pq}$. In 2007, Kaplan [5] proved the following technical proposition, relating coefficients of $\Phi_{pqr}(x)$ to the coefficients of $\Phi_{pq}(x)$.

Proposition 2. *Let $m \geq 0$ be an integer and $f(i)$ the unique value $0 \leq f(i) \leq pq - 1$ such that*

$$rf(i) + i \equiv m \pmod{pq}. \tag{1.1}$$

Set $a^*(pq, j) = a(pq, j)$, if $rj \leq m$; and 0 otherwise. Then

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

The investigation of the coefficients of $\Phi_{pqr}(x)$ has a long history, see Sanna [9] for a recent survey on this topic. Nevertheless, it is still an open problem to give a complete classification of flat ternary cyclotomic polynomials. Broadhurst once proposed the following conjecture about flat ternary cyclotoic polynomials.

Conjecture 1. *Let $p < q < r$ be odd primes with w the unique integer $0 \leq w \leq \frac{pq-1}{2}$ satisfying $r \equiv \pm w \pmod{pq}$.*

If $w = 1$, then we say that $[p, q, r]$ is of Type 1.

If $w > 1$, $q \equiv 1 \pmod{pw}$ and $p \equiv 1 \pmod{w}$, then we say that $[p, q, r]$ is of Type 2.

If $w > p$, $q > p(p - 1)$, $q \equiv \pm 1 \pmod{p}$ and $w \equiv \pm 1 \pmod{p}$, and in the case where $w \equiv 1 \pmod{p}$ we have $wp \nmid q + 1$ and $wp \nmid q - 1$, then we say that $[p, q, r]$ is of Type 3.

Then $A(pqr) = 1$ if and only if $[p, q, r]$ is of Type 1 or 2, or $[p, q, r]$ is of Type 3 and $\Phi_{pq}(x^s)/\Phi_{pq}(x)$ is flat, where s is the smallest positive integer such that $s \equiv 1 \pmod{p}$ and $s \equiv \pm r \pmod{pq}$.

Let $p < q < r$ be odd primes such that

$$zr \equiv \pm 1 \pmod{pq},$$

where z is a positive integer. For some fixed values of z, such as $1 \leq z \leq 8$, the flatness of $\Phi_{pqr}(x)$ has been studied in literature [1, 2, 3, 4, 5, 7, 9, 11, 12, 13, 15, 14, 16]. In this paper, we study the flatness of $\Phi_{pqr}(x)$ and establish the following result, without fixing z.

Theorem 1. *Let $p < q < r$ be odd primes such that $q \equiv \ell \pmod{p}$ and $zr \equiv 1 \pmod{pq}$, where $1 < \ell < p - 1$ and $4 < 2z < p$ are integers.*

(1) *If $p \equiv \ell \pmod{z}$, then $a(pqr, pr + qr - \ell r + p + q + r - 1 - \frac{p-\ell}{z}) \geq 2$.*

(2) *If $p \equiv -\ell \pmod{z}$ and $\ell \equiv -1 \pmod{z}$, then $a(pqr, qr + p + q - 1 - \frac{p+\ell}{z}) \leq -2$.*

(3) *If $p \equiv -\ell \pmod{z}$ and $\ell \not\equiv -1 \pmod{z}$, then $a(pqr, qr + p + q + r - 1 - \frac{p+\ell}{z}) \geq 2$.*

Recall that Kaplan [5] showed that for any prime $s > q$ such that $s \equiv \pm r \pmod{pq}$, $A(pqr) = A(pqs)$. Then, as an immediately consequence of Theorem 1, we obtain

Corollary 1. *Let $p < q < r$ be odd primes such that $q \equiv \ell \pmod{p}$ and $zr \equiv \pm 1 \pmod{pq}$, where $1 < \ell < p - 1$ and $4 < 2z < p$ are integers. If $p \equiv \pm \ell \pmod{z}$, then $\Phi_{pqr}(x)$ is non-flat.*

2 Preliminaries

We now provide bounds for the values s and t in the equation $pq+1 = sp+tq$ used in the proof of Theorem 1.

Lemma 1. *Let $p < q$ be odd primes with $q = kp + \ell$ for some $k \geq 1$ and $1 < \ell < p-1$. Let s, t be unique integers $0 < s < q$, $0 < t < p$ such that $pq + 1 = sp + tq$. Then*

(1) $2 \leq t \leq p-2$;

(2) $k+1 < s \leq q-k-2$.

Proof. (1) Note that $t = 1$ if and only if $q \equiv 1 \pmod p$, and $t = p-1$ if and only if $q \equiv -1 \pmod p$. Then, we have $2 \leq t \leq p-2$.

(2) It follows from $t \geq 2$ and $k \geq 1$ that

$$\begin{aligned} p(q-k-2) - ps &= tkp + \ell t - kp - 2p - 1 \\ &\geq kp - p + \ell t - (p+1) \\ &\geq \ell t - (p+1). \end{aligned}$$

On noting that $\ell t \equiv 1 \pmod p$, we obtain from $\ell > 1$ that $\ell t \geq p+1$, implying that $s \leq q-k-2$.

Since $t \leq p-2$, we deduce that $sp = (p-t)q + 1 \geq 2q + 1 > kp + p$. So $s > k+1$. This completes the proof of Lemma 1. □

3 Proof of Theorem 1

Put $q = kp + \ell$, where k is a positive integer.

(1) Let $p' = \frac{p-\ell}{z}$ and $m = pr + qr - \ell r + p + q + r - 1 - p'$. By substituting the value of m into congruence $rf(i) + i \equiv m \pmod{pq}$, we have

$$f(i) \equiv zp + (z+1)q - z + 1 - zi \pmod{pq}.$$

It follows from $4 < 2z < p$ that

$$0 < f(q+p-1) < f(0) < pq.$$

So $f(i) = zp + (z+1)q - z + 1 - zi$, where $i \in [0, p-1] \cup [q, q+p-1]$. Then one readily verifies that

$$\begin{aligned} m &< rf(q+p-2-p') < \cdots < rf(q) < rf(p-1) < \cdots < rf(0); \\ m &> rf(q+p-1-p') > \cdots > rf(q+p-1). \end{aligned}$$

In view of Proposition 2, we infer that

$$a^*(pq, f(i)) = \begin{cases} 0 & \text{if } i \in [0, p-1] \cup [q, q+p-2-p']; \\ a(pq, f(i)) & \text{if } i \in [q+p-1-p', q+p-1], \end{cases}$$

and thus

$$a(pqr,m) = -\sum_{j=p-1-p'}^{p-1} a(pq, f(q+j)). \tag{3.1}$$

On noting that $f(q+p-1) = q+1$ and $f(q+p-1-p') = (k+1)p+1$, we obtain from Lemma 1 and Proposition 1 that $a(pq, f(q+p-1)) = a(pq, f(q+p-1-p')) = -1$. Therefore we can write (3.1) as

$$a(pqr,m) = 2 - \sum_{j=p-p'}^{p-2} a(pq, f(q+j)).$$

Set $p-p' \le j \le p-2$. It follows from Proposition 1 that the quantity $a(pq, f(q+j))$ takes on one of three values: -1, 0 or 1. We will now show that

$$a(pq, f(q+j)) \ne 1. \tag{3.2}$$

According to Proposition 1, we only have to prove that $f(q+j)$ can not be written in the form $up+vq$ for some $0 \le u \le s-1$ and $0 \le v \le t-1$, where s and t are the unique positive integers such that $pq+1 = sp+tq$. Let us suppose that

$$f(q+j) = zp+q+1-(1+j)z = up+vq. \tag{3.3}$$

Since

$$q < f(q+p-1) < f(q+j) < f(q+p-1-p') < 2q,$$

we have $v = 0, 1$.

If $v=0$, then, by taking (3.3) modulo p,

$$(1+j)z - \ell - 1 \equiv 0 \pmod p.$$

On noting that $(z-1)p < (z-1)p + z - 1 \le (1+j)z - \ell - 1 \le zp - z - \ell - 1 < zp$, we derive a contradiction.

If $v=1$, we similarly infer that $(1+j)z-1 \equiv 0 \pmod p$. This contradicts the fact that $(z-1)p < (1+j)z - 1 < zp$ and proves our claim (3.2). Hence $a(pqr,m) \ge 2$.

(2) Our argument here proceeds along the same lines. Let $p'' = \frac{p+\ell}{z}$ and $m = qr+p+q-1-p''$. On noting $4 < 2z < p$ and $0 \le f(i) \le pq-1$, it follows from congruence (1.1) that

$$f(i) = (z-1)p + (z+1)q - \ell - z - zi,$$

where $i \in [0, p-1] \cup [q, q+p-1]$. Then $rf(i) > m$ whenever $i \in [0,p-1] \cup [q, q+p-2-p'']$, and $rf(i) \le m$ whenever $i \in [q+p-1-p'', q+p-1]$. According to Proposition 2, we deduce that

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

In particular, we have $f(q+p-1) = (k-1)p$ and $f(q+p-1-p'') = q$. By using Proposition 1 and Lemma 1, we derive that $a(pq, f(q+p-1)) = a(pq, q+p-1-p'') = 1$, and then

$$a(pqr,m) = -2 - \sum_{j=p-p''}^{p-2} a(pq, f(q+j)).$$

In light of Proposition 1, for the purpose of proving $a(pqr, m) \le -2$, it suffices to show that

$$a(pq, f(q+j)) \neq -1 \text{ for } p - p'' \le j \le p - 2. \tag{3.4}$$

If $a(pq, f(q+j)) = -1$, then, by Proposition 1 once again, there exist non-negative integers u, v such that

$$f(q+j) = (z-1)p + q - \ell - z - zj = up + vq + 1. \tag{3.5}$$

Since $(k-1)p < f(q+j) < q$, we obtain that $v = 0$. Then by taking (3.5) modulo p, we have $zj + z + 1 \equiv 0 \pmod p$. It follows from $(z-2)p < zj + z + 1 < zp$ that

$$zj + z + 1 = (z-1)p.$$

On taking the above equation modulo z, we derive a contradiction to $p \equiv 1 \pmod z$ and establish the validity of (3.4).

(3) By applying $m = qr + p + q + r - 1 - p''$ into congruence (1.1), we have

$$f(i) = (z-1)p + (z+1)q - \ell - z + 1 - zi,$$

where $i \in [0, p-1] \cup [q, q+p-1]$. Then

$$m \begin{cases} < rf(i) & \text{if } 0 \le i \le p-1 \text{ or } q \le i \le q+p-2-p''; \\ \ge rf(i) & \text{if } q+p-1-p'' \le i \le q+p-1. \end{cases}$$

So

$$a(pqr, m) = -\sum_{j=p-1-p''}^{p-1} a(pq, f(q+j)). \tag{3.6}$$

On observing that $f(q+p-1) = (k-1)p+1$ and $f(q+p-1-p'') = q+1$, we obtain from Lemma 1 and Proposition 1 that $a(pq, f(q+p-1)) = a(pq, f(q+p-1-p'')) = -1$. This allows us rewrite (3.6) as

$$a(pqr, m) = 2 - \sum_{j=p-p''}^{p-2} a(pq, f(q+j)).$$

Set $p - p'' \le j \le p-2$. It is clear that $a(pq, f(q+j)) \in \{-1, 0, 1\}$. In order to show $a(pqr, m) \ge 2$, it remains to prove that $a(pq, f(q+j)) \neq 1$. If the assertion would not hold, then, by Proposition 1, there exist non-negative integers u, v such that

$$f(q+j) = (z-1)p + q - \ell - z + 1 - zj = up + vq. \tag{3.7}$$

Since $0 < f(q+j) < q$, we infer that $v = 0$. Taking (3.7) modulo p yields $zj + z - 1 \equiv 0 \pmod p$. It follows from $(z-2)p < zj + z - 1 < zp$ that $zj + z - 1 = (z-1)p$. Then we can derive that $p \equiv 1 \pmod z$. This leads to a contradiction and completes the proof of Theorem 1.

Acknowledgements. *I would like to express my sincere gratitude to the referees and editors for careful reading of the manuscript and giving valuable comments. This work was supported by Taishan Scholar Project of Shandong Province (Grant No. tsqn202103060), the Young Talents Invitation Program of Shandong Province, project ZR2019QA016 supported by Shandong Provincial Natural Science Foundation, and National Natural Science Foundation of China (Grant Nos. 12071247,11801303).*

References

[1] G. Bachman, Flat cyclotomic polynomials of order three, *Bull. Lond. Math. Soc.*, **38**, 53-60 (2006).

[2] S. Elder, Flat cyclotomic polynomials: A new approach, arXiv:1207.5811v1 (2012).

[3] T. J. Flanagan, On the coefficients of ternary cyclotomic polynomials, Master's thesis, University of Nevada, Las Vegas (2007).

[4] C. G. Ji, A special family of cyclotomic polynomials of order three, *Science China Math.*, **53**, 2268-2274 (2010).

[5] N. Kaplan, Flat cyclotomic polynomials of order three, *J. Number Theory*, **127**, 118-126 (2007).

[6] T. Y. Lam, K. H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly*, **103**, 562-564 (1996).

[7] F. Luca, P. Moree, R. Osburn, S. S. Eddin, A. Sedunova, Constrained ternary integers, *Int. J. Number Theory*, **15**, 407-431 (2019).

[8] A. Migotti, Zur Theorie der Kreisteilungsgleichung, Sitzber. Math.-Naturwiss. Classe der Kaiser, *Akad. der Wiss.*, **87**, 7-14 (1883).

[9] C. Sanna, A survey on coefficients of cyclotomic polynomials, *Expo. Math.*, **40**, 469-494 (2022).

[10] R. Thangadurai, On the coefficients of cyclotomic polynomials, in *Cyclotomic Fields and Related Topics, Pune, 1999, Bhaskaracharya Pratishthana, Pune*, 311-322 (2000).

[11] B. Zhang, Y. Zhou, On a class of ternary cyclotomic polynomials, *Bull. Korean Math. Soc.*, **52**, 1911-1924 (2015).

[12] B. Zhang, Remarks on the flatness of ternary cyclotomic polynomials, *Int. J. Number Theory*, **13**, 529-547 (2017).

[13] B. Zhang, The flatness of a class of ternary cyclotomic polynomials, *Publ. Math. Debrecen*, **97**, 201-216 (2020).

[14] B. Zhang, The flatness of ternary cyclotomic polynomials, *Rend. Sem. Mat. Univ. Padova*, **145**, 1-42 (2021).

[15] B. Zhang, A remark on flat ternary cyclotomic polynomials, *Glasnik Matematicki*, **56**, 241-261 (2021).

[16] J. Zhao, X. K. Zhang, Coefficients of ternary cyclotomic polynomials, *J. Number Theory*, **130**, 2223-2237 (2010).

Received: 11.09.2022
Revised: 17.10.2022
Accepted: 01.11.2022

School of Mathematical Sciences, Qufu Normal University,
Qufu, Shandong, 273165, P. R. China
E-mail: zhangb2015@qfnu.edu.cn