Bin Zhang

On the coefficients of a class of ternary cyclotomic polynomials

Accepted manuscript

ON THE COEFFICIENTS OF A CLASS OF TERNARY CYCLOTOMIC POLYNOMIALS

BIN ZHANG

Qufu Normal University, P. R. China

ABSTRACT. A cyclotomic polynomial $\Phi_n(x)$ is said to be flat if its nonzero coefficients involve only ± 1. In this paper, for odd primes $p < q < r$ with $q \equiv 1 \pmod{p}$ and $9r \equiv \pm 1 \pmod{pq}$, we prove that $\Phi_{pqr}(x)$ is flat if and only if $p = 5$, $q \geq 41$, and $q \equiv 1 \pmod{5}$.

1. INTRODUCTION

Let
$$\Phi_n(x) = \prod_{\substack{(m,n)=1 \\ 1 \leq m \leq n}} (x - \zeta_n^m),$$

where $\zeta_n = e^{2\pi i/n}$. This polynomial is called the nth cyclotomic polynomial. It is a classical and neoteric problem in number theory to investigate the arithmetic properties of cyclotomic polynomials. Since $\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n) = \deg \Phi_n(x)$, it follows that $\Phi_n(x)$ is the irreducible polynomial for ζ_n. Also, $\Phi_n(x) \in \mathbb{Z}[x]$ since the coefficients are rational and also are algebraic integers.

The first few cyclotomic polynomials are

$$\Phi_1(x) = x - 1, \qquad \Phi_2(x) = x + 1,$$
$$\Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1.$$

All these have coefficients ± 1 and 0; however, this is not true in general. By choosing n with many prime factors one can obtain arbitrarily large coefficients.

Let $a(n, j)$ denote the coefficient of x^j in the nth cyclotomic polynomial $\Phi_n(x)$ and $A(n) = \max\{|a(n, j)| : 0 \le j \le \phi(n)\}$ be the height of $\Phi_n(x)$. Cyclotomic polynomials of unit height are called *flat*. Since

$$\Phi_n(x) = \Phi_{\mathrm{radical}(n)}(x^{n/\mathrm{radical}(n)}) \text{ and } \Phi_{2n}(x) = \pm\Phi_n(-x),$$

we can restrict the study of $A(n)$ to the case $n = pqr\cdots$, where $3 \le p < q < r < \cdots$ are primes. It is clear that

$$a(p, j) = \begin{cases} 1 & \text{if } 0 \le j \le p - 1; \\ 0 & \text{otherwise,} \end{cases}$$

(1.1)

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

where s and t are unique positive integers $1 \le s < q$, $1 \le t < p$ such that $pq + 1 = ps + qt$, see e.g. Lam and Leung [8] or Thangadurai [10]. Thus all the prime cyclotomic polynomials $\Phi_p(x)$ and binary cyclotomic polynomials $\Phi_{pq}(x)$ are flat.

The problem of flat ternary cyclotomic polynomials—flat polynomials of the form $\Phi_{pqr}(x)$, where p, q, and r are distinct odd primes—seems tantalizingly accessible but remains open. In 2009, Broadhurst proposed some conjectures about flat ternary cyclotomic polynomials, see [7, Conjecture] or [4, Conjecture 4.4.3]. Let $p < q < r$ be odd primes such that $zr \equiv \pm 1 \pmod{pq}$, where z is a positive integer. At present, the flatness of $\Phi_{pqr}(x)$ in special cases $1 \le z \le 8$ has been considered, see [1, 2, 3, 5, 6, 9, 11, 12, 13, 14, 15, 16]. In this paper, we study the flatness of $\Phi_{pqr}(x)$ in the special case when $q \equiv 1 \pmod{p}$ and $z = 9$, and establish the following result.

THEOREM 1.1. *Let $p < q < r$ be odd primes such that $q \equiv 1 \pmod{p}$ and $9r \equiv \pm 1 \pmod{pq}$. Then $\Phi_{pqr}(x)$ is flat if and only if $p = 5$, $q \ge 41$, and $q \equiv 1 \pmod{5}$.*

2. Preliminaries

Before starting our proof of the theorem, the following lemmas will be useful. Let $p < q$ be odd primes such that $q = kp+1$. Then, for $pq+1 = ps+qt$, we have $s = q - k$, $t = 1$. Hence it follows immediately from (1.1) that

LEMMA 2.1. *Let $p < q$ be odd prime such that $q = kp + 1$. Then*

$$a(pq, j) = \begin{cases} 1 & \text{if } j = up \text{ for some } 0 \leq u \leq q - k - 1; \\ -1 & \text{if } j = up + vq + 1 \text{ for some } 0 \leq u \leq k - 1, 0 \leq v \leq p - 2; \\ 0 & \text{otherwise.} \end{cases}$$

Our main tool is the following technical lemma due to Kaplan [6, Lemma 1], which reduces the computing of the ternary cyclotomic coefficients to the binary cyclotomic coefficients.

LEMMA 2.2. *Let $p < q < r$ be odd primes. Let $n \geq 0$ be an integer and $f(i)$ be the unique value $0 \leq f(i) \leq pq - 1$ such that*

(2.2) $$r f(i) + i \equiv n \pmod{pq}.$$

(1) Then

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

(2) Put

(2.3) $$a^*(pq, f(i)) = \begin{cases} a(pq, f(i)) & \text{if } f(i) \leq \frac{n}{r}; \\ 0 & \text{otherwise.} \end{cases}$$

Then

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

We also need the periodicity of $A(pqr)$, which implies that the height $A(pqr)$ is determined by $\pm r \pmod{pq}$, see [6].

LEMMA 2.3. *Let $3 \leq p < q < r$ be primes. Then for any prime $s > q$ such that $s \equiv \pm r \pmod{pq}$, $A(pqr) = A(pqs)$.*

3. PROOF OF THEOREM 1.1

Note that $9r \equiv \pm 1 \pmod{pq}$ implies that $p \neq 3$. In view of Lemma 2.3, it is enough to consider primes $p < q < r$ such that

$$p \geq 5, \ q \equiv 1 \pmod{p}, \text{ and } 9r \equiv 1 \pmod{pq}.$$

The proof will be split into the following three parts according to the value of p.

3.1 The case when $p = 5$.

(i) By using the PARI/GP system, we have $A(5 \cdot 11 \cdot 269) = A(5 \cdot 31 \cdot 379) = 2$. On noting that $9 \cdot 269 \equiv 1 \pmod{5 \cdot 11}$ and $9 \cdot 379 \equiv 1 \pmod{5 \cdot 31}$, we obtain from Lemma 2.3 that

$$A(5qr) = 2 \text{ if } q = 11, 31, \text{ and } 9r \equiv 1 \pmod{5q}.$$

(ii) Next we will show that

$$A(5qr) = 1 \text{ if } q \geq 41, \ q \equiv 1 \ (\text{mod } 5), \text{ and } 9r \equiv 1 \ (\text{mod } 5q).$$

Let $q = 5k + 1$. Then k is even and $k \geq 8$. For $5q + 1 = 5s + qt$, we have $s = 4k+1$, $t = 1$. Thus in this case, we may rewrite the conclusion of Lemma 2.1 in the following form

$$(3.5) \qquad a(5q, j) = \begin{cases} 1 & \text{if } j \equiv 0 \quad (\text{mod } 5) \text{ and } 0 \leq j \leq 20k; \\ -1 & \text{if } j \equiv 1 \quad (\text{mod } 5) \text{ and } 1 \leq j \leq 5k - 4; \\ -1 & \text{if } j \equiv 2 \quad (\text{mod } 5) \text{ and } 5k + 2 \leq j \leq 10k - 3; \\ -1 & \text{if } j \equiv 3 \quad (\text{mod } 5) \text{ and } 10k + 3 \leq j \leq 15k - 2; \\ -1 & \text{if } j \equiv 4 \quad (\text{mod } 5) \text{ and } 15k + 4 \leq j \leq 20k - 1; \\ 0 & \text{otherwise.} \end{cases}$$

For any given $n \in [0, \phi(5qr)]$, it follows from $rf(i) + i \equiv n \ (\text{mod } 5q)$ that

$$(3.6) \qquad\qquad f(i + 1) + 9 \equiv f(i) \quad (\text{mod } 5q).$$

Therefore, the quantity $f(i)$ can be regarded as uniquely determined by $f(0)$, where $1 \leq i \leq 4$ and $q \leq i \leq q+4$. Now we give the following tables according to the value of $f(0)$. For simplicity, we may put

$$a_{f(i)} = a(5q, f(i))$$

in the rest of this section. The second row in each table is the inequality about $f(i)$ for $i \in [0, 4] \cup [q, q + 4]$. The values of $a_{f(i)}$ in the following tables are obtained by using (3.5) and (3.6). We will let $\overline{f(0)}$ denote the unique integer satisfying $\overline{f(0)} \equiv f(0) \ (\text{mod } 5)$ and $0 \leq \overline{f(0)} \leq 4$ in Tables 5, 7, 9, 11, and 16 below.

Table 1. $0 \leq f(0) \leq 8$

$f(0)$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$
					$f(1) > f(2) > f(3) > f(4) > f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0)$					
0	0	0	0	0	0	0	0	0	-1	1
1	0	0	0	0	1	0	0	-1	1	-1
2	0	0	0	0	0	0	-1	1	0	0
3	0	0	0	0	0	-1	1	0	0	0
4	0	0	0	0	-1	1	0	0	0	0
5	0	0	0	0	0	0	0	0	-1	1
6	0	0	0	0	1	0	0	-1	1	-1
7	0	0	0	0	0	0	-1	1	0	0
8	0	0	0	0	0	-1	1	0	0	0

Table 2. $9 \leq f(0) \leq 17$

$f(0)$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$
				$f(2) > f(3) > f(4) > f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1)$						
9	0	0	0	-1	0	0	0	0	0	1
10	0	0	0	0	1	0	0	-1	1	-1
11	0	0	0	1	0	0	-1	1	-1	0
12	0	0	0	0	0	-1	1	0	0	0
13	0	0	0	0	-1	1	0	0	0	0
14	0	0	0	-1	0	0	0	0	0	1
15	0	0	0	0	1	0	0	-1	1	-1
16	0	0	0	1	0	0	-1	1	-1	0
17	0	0	0	0	0	-1	1	0	0	0

Table 3. $18 \le f(0) \le 26$

$f(0)$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$
	$f(3) > f(4) > f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2)$									
18	0	0	0	-1	0	0	0	0	0	1
19	0	0	-1	0	1	0	0	0	1	-1
20	0	0	0	1	0	0	-1	1	-1	0
21	0	0	1	0	0	-1	1	-1	0	0
22	0	0	0	0	-1	1	0	0	0	0
23	0	0	0	-1	0	0	0	0	0	1
24	0	0	-1	0	1	0	0	0	1	-1
25	0	0	0	1	0	0	-1	1	-1	0
26	0	0	1	0	0	-1	1	-1	0	0

Table 4. $27 \le f(0) \le 35$

$f(0)$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$
	$f(4) > f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3)$									
27	0	0	0	-1	0	0	0	0	0	1
28	0	0	-1	0	1	0	0	0	1	-1
29	0	-1	0	1	0	0	0	1	-1	0
30	0	0	1	0	0	-1	1	-1	0	0
31	0	1	0	0	-1	1	-1	0	0	0
32	0	0	0	-1	0	0	0	0	0	1
33	0	0	-1	0	1	0	0	0	1	-1
34	0	-1	0	1	0	0	0	1	-1	0
35	0	0	1	0	0	-1	1	-1	0	0

Table 5. $36 \le f(0) \le q - 1$

$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
	$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$									
0	0	1	0	0	-1	1	-1	0	0	0
1	1	0	0	-1	0	-1	0	0	0	1
2	0	0	-1	0	1	0	0	0	1	-1
3	0	-1	0	1	0	0	0	1	-1	0
4	-1	0	1	0	0	0	1	-1	0	0

Table 6. $q \le f(0) \le q + 32$

$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
	$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$									
q	0	0	0	-1	0	0	0	0	0	1
$q+1$	1	0	-1	0	1	-1	0	0	1	-1
$q+2$	0	-1	0	1	0	0	0	1	-1	0
$q+3$	-1	0	1	0	0	0	1	-1	0	0
$q+4$	0	1	0	0	-1	1	-1	0	0	0
$q+5$	0	0	0	-1	0	0	0	0	0	1
$q+6$	1	0	-1	0	1	-1	0	0	1	-1
$q+7$	0	-1	0	1	0	0	0	1	-1	0
$q+8$	-1	0	1	0	0	0	1	-1	0	0
$q+9$	0	0	0	0	-1	1	0	0	0	0
$q+10$	0	1	0	-1	0	0	-1	0	0	1
$q+11$	1	0	-1	0	1	-1	0	0	1	-1
$q+12$	0	-1	0	1	0	0	0	1	-1	0
$q+13$	-1	0	1	0	0	0	1	-1	0	0
$q+14$	0	0	0	0	-1	1	0	0	0	0
$q+15$	0	1	0	-1	0	0	-1	0	0	1
$q+16$	1	0	-1	0	1	-1	0	0	1	-1
$q+17$	0	-1	0	1	0	0	0	1	-1	0
$q+18$	-1	0	0	0	0	0	1	0	0	0
$q+19$	0	0	1	0	-1	1	0	-1	0	0
$q+20$	0	1	0	-1	0	0	-1	0	0	1
$q+21$	1	0	-1	0	1	-1	0	0	1	-1
$q+22$	0	-1	0	1	0	0	0	1	-1	0
$q+23$	-1	0	0	0	0	0	1	0	0	0
$q+24$	0	0	1	0	-1	1	0	-1	0	0
$q+25$	0	1	0	-1	0	0	-1	0	0	1
$q+26$	1	0	-1	0	1	-1	0	0	1	-1

$q+27$	0	-1	0	0	0	0	0	1	0	0
$q+28$	-1	0	0	1	0	0	1	0	-1	0
$q+29$	0	0	1	0	-1	1	0	-1	0	0
$q+30$	0	1	0	-1	0	0	-1	0	0	1
$q+31$	1	0	-1	0	1	-1	0	0	1	-1
$q+32$	0	-1	0	0	0	0	0	1	0	0

Table 7. $q + 33 \leq f(0) \leq 2q - 1$										
	$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$									
$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
0	0	0	1	0	-1	1	0	-1	0	0
1	0	1	0	-1	0	0	-1	0	0	1
2	1	0	-1	0	0	-1	0	0	1	0
3	0	-1	0	0	1	0	0	1	0	-1
4	-1	0	0	1	0	0	1	0	-1	0

Table 8. $2q \leq f(0) \leq 2q + 32$										
	$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$									
$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
$2q$	0	0	-1	0	0	0	0	0	1	0
$2q+1$	1	-1	0	0	1	-1	0	1	0	-1
$2q+2$	-1	0	0	1	0	0	1	0	-1	0
$2q+3$	0	0	1	0	-1	1	0	-1	0	0
$2q+4$	0	1	0	-1	0	0	-1	0	0	1
$2q+5$	0	0	-1	0	0	0	0	0	1	0
$2q+6$	1	-1	0	0	1	-1	0	1	0	-1
$2q+7$	-1	0	0	1	0	0	1	0	-1	0
$2q+8$	0	0	1	0	-1	1	0	-1	0	0
$2q+9$	0	0	0	-1	0	0	0	0	0	1
$2q+10$	0	1	-1	0	0	0	-1	0	1	0
$2q+11$	1	-1	0	0	1	-1	0	1	0	-1
$2q+12$	1	0	0	-1	0	0	-1	0	1	0
$2q+13$	0	0	1	0	-1	1	0	-1	0	0
$2q+14$	0	0	0	-1	0	0	0	0	0	1
$2q+15$	0	1	-1	0	0	0	-1	0	1	0
$2q+16$	1	-1	0	0	1	-1	0	1	0	-1
$2q+17$	-1	0	0	1	0	0	1	0	-1	0
$2q+18$	0	0	0	0	-1	1	0	0	0	0
$2q+19$	0	0	1	-1	0	0	0	-1	0	1
$2q+20$	0	1	-1	0	0	0	-1	0	1	0
$2q+21$	1	-1	0	0	1	-1	0	1	0	-1
$2q+22$	-1	0	0	1	0	0	1	0	-1	0
$2q+23$	0	0	0	0	-1	1	0	0	0	0
$2q+24$	0	0	1	-1	0	0	0	-1	0	1
$2q+25$	0	1	-1	0	0	0	-1	0	1	0
$2q+26$	1	-1	0	0	1	-1	0	1	0	-1
$2q+27$	-1	0	0	0	0	0	1	0	0	0
$2q+28$	0	0	0	1	-1	1	0	0	-1	0
$2q+29$	0	0	1	-1	0	0	0	-1	0	1
$2q+30$	0	1	-1	0	0	0	-1	0	1	0
$2q+31$	1	-1	0	0	1	-1	0	1	0	-1
$2q+32$	-1	0	0	0	0	0	1	0	0	0

Table 9. $2q + 33 \leq f(0) \leq 3q - 1$										
	$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$									
$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
0	0	0	0	1	-1	1	0	0	-1	0
1	0	0	1	-1	0	0	0	-1	0	1
2	0	1	-1	0	0	0	-1	0	1	0
3	1	-1	0	0	0	-1	0	1	0	0
4	-1	0	0	0	1	0	1	0	0	-1

Table 10. $3q \le f(0) \le 3q + 32$										
$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$										
$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
$3q$	0	-1	0	0	0	0	0	1	0	0
$3q+1$	0	0	0	0	1	-1	1	0	0	-1
$3q+2$	0	0	0	1	-1	1	0	0	-1	0
$3q+3$	0	0	1	-1	0	0	0	-1	0	1
$3q+4$	0	1	-1	0	0	0	-1	0	1	0
$3q+5$	0	-1	0	0	0	0	0	1	0	0
$3q+6$	0	0	0	0	1	-1	1	0	0	-1
$3q+7$	0	0	0	1	-1	1	0	0	-1	0
$3q+8$	0	0	1	-1	0	0	0	-1	0	1
$3q+9$	0	0	-1	0	0	0	0	0	1	0
$3q+10$	0	0	0	0	0	0	-1	1	0	0
$3q+11$	0	0	0	0	1	-1	1	0	0	-1
$3q+12$	0	0	0	1	-1	1	0	0	-1	0
$3q+13$	0	0	1	-1	0	0	0	-1	0	1
$3q+14$	0	0	-1	0	0	0	0	0	1	0
$3q+15$	0	0	0	0	0	0	-1	1	0	0
$3q+16$	0	0	0	0	1	-1	1	0	0	-1
$3q+17$	0	0	0	1	-1	1	0	0	-1	0
$3q+18$	0	0	0	-1	0	0	0	0	0	1
$3q+19$	0	0	0	0	0	0	0	-1	1	0
$3q+20$	0	0	0	0	0	0	-1	1	0	0
$3q+21$	0	0	0	0	1	-1	1	0	0	-1
$3q+22$	0	0	0	1	-1	1	0	0	-1	0
$3q+23$	0	0	0	-1	0	0	0	0	0	1
$3q+24$	0	0	0	0	0	0	0	-1	1	0
$3q+25$	0	0	0	0	0	0	0	-1	1	0
$3q+26$	0	0	0	0	1	-1	1	0	0	-1
$3q+27$	0	0	0	0	-1	1	0	0	0	0
$3q+28$	0	0	0	0	0	0	0	0	-1	1
$3q+29$	0	0	0	0	0	0	0	-1	1	0
$3q+30$	0	0	0	0	0	0	-1	1	0	0
$3q+31$	0	0	0	0	1	-1	1	0	0	-1
$3q+32$	0	0	0	0	-1	1	0	0	0	0

Table 11. $3q + 33 \le f(0) \le 4q - 1$										
$f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4)$										
$f(0)$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$
0	0	0	0	0	0	1	0	0	0	-1
1	0	0	0	0	0	0	0	0	-1	1
2	0	0	0	0	0	0	0	-1	1	0
3	0	0	0	0	0	0	-1	1	0	0
4	0	0	0	0	0	-1	1	0	0	0

Table 12. $4q \le f(0) \le 4q + 8$										
$f(q+1) > f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4) > f(q)$										
$f(0)$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$
$4q$	0	0	0	0	0	1	0	0	0	-1
$4q+1$	0	0	0	0	0	0	0	0	-1	1
$4q+2$	0	0	0	0	0	0	0	-1	1	0
$4q+3$	0	0	0	0	0	0	-1	1	0	0
$4q+4$	0	0	0	0	0	-1	1	0	0	0
$4q+5$	0	0	0	0	0	1	0	0	0	-1
$4q+6$	0	0	0	0	0	0	0	0	-1	1
$4q+7$	0	0	0	0	0	0	0	-1	1	0
$4q+8$	0	0	0	0	0	0	-1	1	0	0

Table 13. $4q + 9 \le f(0) \le 4q + 17$

$f(0)$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$
	$f(q+2) > f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4) > f(q) > f(q+1)$									
$4q+9$	0	0	0	0	0	1	0	0	0	-1
$4q+10$	0	0	0	0	0	0	0	0	-1	1
$4q+11$	0	0	0	0	0	0	0	-1	1	0
$4q+12$	0	0	0	0	0	0	-1	1	0	0
$4q+13$	0	0	0	0	0	-1	1	0	0	0
$4q+14$	0	0	0	0	0	1	0	0	0	-1
$4q+15$	0	0	0	0	0	0	0	0	-1	1
$4q+16$	0	0	0	0	0	0	0	-1	1	0
$4q+17$	0	0	0	0	0	0	-1	1	0	0

Table 14. $4q + 18 \le f(0) \le 4q + 26$

$f(0)$	$-a_{f(q+3)}$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$
	$f(q+3) > f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4) > f(q) > f(q+1) > f(q+2)$									
$4q+18$	0	0	0	0	0	1	0	0	0	-1
$4q+19$	0	0	0	0	0	0	0	0	-1	1
$4q+20$	0	0	0	0	0	0	0	-1	1	0
$4q+21$	0	0	0	0	0	0	-1	1	0	0
$4q+22$	0	0	0	0	0	-1	1	0	0	0
$4q+23$	0	0	0	0	0	1	0	0	0	-1
$4q+24$	0	0	0	0	0	0	0	0	-1	1
$4q+25$	0	0	0	0	0	0	0	-1	1	0
$4q+26$	0	0	0	0	0	0	-1	1	0	0

Table 15. $4q + 27 \le f(0) \le 4q + 35$

$f(0)$	$-a_{f(q+4)}$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$
	$f(q+4) > f(0) > f(1) > f(2) > f(3) > f(4) > f(q) > f(q+1) > f(q+2) > f(q+3)$									
$4q+27$	0	0	0	0	0	1	0	0	0	-1
$4q+28$	0	0	0	0	0	0	0	0	-1	1
$4q+29$	0	0	0	0	0	0	0	-1	1	0
$4q+30$	0	0	0	0	0	0	-1	1	0	0
$4q+31$	0	0	0	0	0	-1	1	0	0	0
$4q+32$	0	0	0	0	0	1	0	0	0	-1
$4q+33$	0	0	0	0	0	0	0	0	-1	1
$4q+34$	0	0	0	0	0	0	0	-1	1	0
$4q+35$	0	0	0	0	0	0	-1	1	0	0

Table 16. $4q + 36 \le f(0) \le 5q - 1$

$f(0)$	$a_{f(0)}$	$a_{f(1)}$	$a_{f(2)}$	$a_{f(3)}$	$a_{f(4)}$	$-a_{f(q)}$	$-a_{f(q+1)}$	$-a_{f(q+2)}$	$-a_{f(q+3)}$	$-a_{f(q+4)}$
	$f(0) > f(1) > f(2) > f(3) > f(4) > f(q) > f(q+1) > f(q+2) > f(q+3) > f(q+4)$									
0	0	0	0	0	0	1	0	0	0	-1
1	0	0	0	0	0	0	0	0	-1	1
2	0	0	0	0	0	0	0	-1	1	0
3	0	0	0	0	0	0	1	-1	0	0
4	0	0	0	0	0	-1	1	0	0	0

Recall that n is a fixed integer in the range $0 \le n \le \phi(5qr)$ and we have, by Lemma 2.2 (2),

$$a(5qr, n) = \sum_{i=0}^{4} a^*(5q, f(i)) + \sum_{i=q}^{q+4} \Big(- a^*\big(5q, f(i)\big) \Big),$$

where

$$a^*(5q, f(i)) = \begin{cases} a_{f(i)} & \text{if } f(i) \le \frac{n}{r}; \\ 0 & \text{otherwise.} \end{cases}$$

Let

$$I = \{0, 1, 2, 3, 4, q, q+1, q+2, q+3, q+4\}.$$

If $f(i) > \frac{n}{r}$ holds for all $i \in I$, then $a^*(pq, f(i)) = 0$. So $a(5qr, n) = 0$.

If $f(i) \leq \frac{n}{r}$ holds for all $i \in I$, then $a^*(pq, f(i)) = a_{f(i)}$. So

$$a(5qr, n) = \sum_{i=0}^{4} a_{f(i)} + \sum_{i=q}^{q+4} (-a_{f(i)}).$$

Then it follows from Lemma 2.2 (1) that $a(5qr, n) = 0$.

If otherwise, then there certainly exist two neighboring symbols $f(i_1)$ and $f(i_2)$ in the second row of the corresponding Table such that

$$f(i_1) > \frac{n}{r} \geq f(i_2).$$

If $0 \leq i_2 \leq 4$ (or $q \leq i_2 \leq q + 4$), the value of $a(5qr, n)$ is given by computing the sum of values from $a_{f(i_2)}$ (or $-a_{f(i_2)}$) to the end of the relevant row.

It is a routine matter to see that the sums of values about $\pm a_{f(i)}$, from anywhere to the end in all tables, is equal to ± 1 or 0. That is to say, $a(5qr, n) \in \{\pm 1, 0\}$ for $0 \leq n \leq \phi(5qr)$.

Therefore, $A(5qr) = 1$ if $q \geq 41$, $q \equiv 1 \pmod{5}$, and $9r \equiv 1 \pmod{5q}$, as desired.

3.2 The case when $p = 7$.

For primes $7 < q < r$ with $q \equiv 1 \pmod 7$ and $9r \equiv 1 \pmod{7q}$, our goal here is to use Lemma 2.2 to show that

$$a(7qr, 2qr + 22r + q + 2) = 2.$$

Let $n = 2qr + 22r + q + 2$. By substituting the value of n into congruence (2.2), we infer that $f(i) \equiv 11q + 40 - 9i \pmod{7q}$. On noting $0 \leq f(i) \leq 7q - 1$, we obtain that $f(i) = 11q + 40 - 9i$ for $0 \leq i \leq 6$ and $q \leq i \leq q + 6$. Then $rf(i) \leq n$ if $i \in \{q+2, q+3, q+4, q+5, q+6\}$ and $rf(i) > n$ if $i \in \{0, 1, \cdots, 6\} \cup \{q, q+1\}$. From (2.3), we have

$$a^*(7q, f(i)) = \begin{cases} a(7q, f(i)) & \text{if } i \in \{q+2, q+3, q+4, q+5, q+6\}; \\ 0 & \text{if } i \in \{0, 1, \cdots, 6\} \cup \{q, q+1\} \end{cases}$$

It follows from Lemma 2.2 that

(3.7) $$a(7qr, n) = -\sum_{i=q+2}^{q+6} a(7q, f(i)).$$

On rewriting $f(q+2)$, $f(q+6)$ as $f(q+2) = 3*7 + 2q + 1$ and $f(q+6) = \frac{q-15}{7} \cdot 7 + q + 1$, we deduce, by Lemma 2.1, $a(pq, f(q+2)) = a(pq, f(q+6)) = -1$. Applying this to (3.7) yields

$$a(7qr, n) = 2 - \sum_{i=q+3}^{q+5} a(7q, f(i)).$$

Let $q + 3 \leq i \leq q + 5$. On one hand, it follows from $f(i) \not\equiv 0 \pmod{7}$ and Lemma 2.1 that $a(7q, f(i)) \neq 1$; on the other hand, it follows from $f(i) \neq 7u + vp + 14$ with $0 \leq u \leq \frac{q-8}{7}$, $0 \leq v \leq 5$ that $a(7q, f(i)) \neq -1$. Hence $a(7q, f(i)) = 0$, and thus $a(7qr, n) = 2$.

3.3 The case when $p > 7$.

In this part, we will prove the following proposition to complete the proof of Theorem 1.1.

PROPOSITION 3.1. *Let $7 < p < q < r$ be odd primes such that $q = kp + 1$ and $9r \equiv 1 \pmod{pq}$.*

(1) If $p \equiv 1 \pmod{9}$, then

$$2 \leq \begin{cases} a(pqr, pr + 10qr + q + r + \frac{2p-11}{9}) & \text{if } k = 4; \\ a(pqr, 3pr + 9qr + q + r + \frac{p-10}{9}) & \text{if } k \geq 6. \end{cases}$$

(2) If $p \equiv 2 \pmod{9}$, then

$$2 \begin{cases} = A(pqr) & \text{if } k = 2 \text{ and } p = 11; \\ \leq a(pqr, 10qr + q + r + \frac{2p-13}{9}) & \text{if } k = 2 \text{ and } p > 11; \\ \leq a(pqr, qr + q + r + \frac{5p-10}{9}) & \text{if } k \geq 6. \end{cases}$$

(3) If $p \equiv 4 \pmod{9}$, then $a(pqr, 3qr + r + \frac{7p-10}{9}) \leq -2$.
(4) If $p \equiv 5 \pmod{9}$, then

$$2 \leq \begin{cases} a(pqr, -pr + 10qr + q + \frac{4p-11}{9}) & \text{if } k = 2; \\ a(pqr, 5pr + 9qr + r + q + \frac{2p-10}{9}) & \text{if } k \geq 6. \end{cases}$$

(5) If $p \equiv 7 \pmod{9}$, then $a(pqr, 3pr + 9qr + q + r + \frac{4p-10}{9}) \geq 2$.
(6) If $p \equiv 8 \pmod{9}$, then $a(pqr, 3qr + q + r + \frac{8p-10}{9}) \geq 2$.

PROOF. (1) *Case 1. $k = 4$.*

On noting that $p \equiv 1 \pmod{9}$ and $q = 4p + 1$, we get $p \geq 37$. Let $n = pr + 10qr + q + r + \frac{2p-11}{9}$. In order to use Lemma 2.2, we first obtain, by substituting the value of l into congruence $rf(i) + i \equiv l \pmod{pq}$,

$$f(i) \equiv 12p + 17q - 8 - 9i \pmod{pq}.$$

Since $p \geq 37$ and $0 \leq f(i) \leq pq - 1$, we have

(3.8) $f(i) = 12p + 17q - 8 - 9i$,

where $0 \leq i \leq p - 1$ or $q \leq i \leq q + p - 1$. Then it follows that $rf(i) > n$ whenever $i \in \{0, 1, \cdots, p-1\} \cup \{q, q+1, \cdots, q+\frac{2p-20}{9}\}$ and $rf(i) \leq n$ whenever $i \in \{q + \frac{2p-11}{9}, q + \frac{2p-2}{9}, \cdots, q + p - 1\}$. Thus, by (2.3),

$$a^*(pq, f(i)) = \begin{cases} 0 & \text{if } i \in [0, p-1] \cup [q, q + \frac{2p-20}{9}]; \\ a(pq, f(i)) & \text{if } i \in [q + \frac{2p-11}{9}, q + p - 1]. \end{cases}$$

Hence

(3.9)
$$a(pqr, n) = - \sum_{j=\frac{2p-11}{9}}^{p-1} a(pq, f(q+j)).$$

On noticing that $f(q + \frac{2p-11}{9}) = p+10q+1$, $f(q+p-1) = 3p+8q+1$, we deduce from Lemma 2.1 that $a(pq, f(q + \frac{2p-11}{9})) = a(pq, f(q + p - 1)) = -1$. Applying this into (3.9) gives

$$a(pqr, n) = 2 - \sum_{j=\frac{2p-2}{9}}^{p-2} a(pq, f(q+j)).$$

Let $\frac{2p-2}{9} \leq j \leq p-2$. It is clear that the binary coefficient $a(pq, f(q+j))$ takes on one of three values: -1, 0, or 1. To show $a(pqr, n) \geq 2$, it suffices to prove that $a(pq, f(q+j)) \neq 1$. If the assertion would not hold, then, by Lemma 2.1, we obtain

$$f(q+j) \equiv 0 \pmod{p}.$$

Combing with (3.8) yields $9j \equiv 0 \pmod{p}$. This leads to a contradiction, and therefore $a(pqr, n) \geq 2$.

Case 2. $k \geq 6$.

Let $n = 3pr + 9qr + q + r + \frac{p-10}{9}$. Then by using the congruence (2.2) we have $f(i) = 4p + 18q - 9 - 9i$ for $0 \leq i \leq p-1$ and $q \leq i \leq q+p-1$. So $f(i) > \frac{n}{r}$ if $i \in [0, p-1] \cup [q, q+\frac{p-19}{9}]$, and $f(i) \leq \frac{n}{r}$ if $i \in [q+\frac{p-10}{9}, q+p-1]$. On invoking Lemma 2.2, we have

$$a^*(pq, f(i)) = \begin{cases} 0 & \text{if } i \in [0, p-1] \cup [q, q+\frac{p-19}{9}]; \\ a(pq, f(i)) & \text{if } i \in [q+\frac{p-10}{9}, q+p-1]. \end{cases}$$

Hence

(3.10)
$$a(pqr, n) = - \sum_{j=\frac{p-10}{9}}^{p-1} a(pq, f(q+j)).$$

On noting that $f(q+\frac{p-10}{9}) = 3p+9q+1$, $f(q+p-1) = (k-5)p+8q+1$, and $k \geq 6$, we deduce from Lemma 2.1 that $a(pq, f(q + \frac{p-10}{9})) = a(pq, f(q + p-1)) = -1$. Combing this with (3.10) gives

$$a(pqr, n) = 2 - \sum_{j=\frac{p-1}{9}}^{p-2} a(pq, f(q+j)).$$

Next we claim that $a(pq, f(q+j)) \neq 1$ for $\frac{p-1}{9} \leq j \leq p-2$. If the assertion would not hold, then, by Lemma 2.1, we obtain

$$f(q+j) = 4p + 9q - 9 - 9j \equiv 0 \pmod{p}.$$

So $p \mid 9j$, a contradiction to $\frac{p-1}{9} \leq j \leq p-2$.

Hence we infer that $a(pq, f(q+j)) \in \{-1, 0\}$ for $\frac{p-1}{9} \leq j \leq p-2$, and then $a(pqr, n) \geq 2$.

(2) *Case 1.* $k = 2$ and $p = 11$.

By using PARI/GP, we have $A(11 \cdot 23 \cdot 1237) = 2$. Then it follows from $9 \cdot 1237 \equiv 1 \pmod{11 \cdot 23}$ and Lemma 2.3 that $A(pqr) = 2$ in the case $p = 11$, $q = 23$, and $9r \equiv 1 \pmod{pq}$.

Case 2. $k = 2$ and $p > 11$.

Let $n = 10qr + q + r + \frac{2p-13}{9}$. By substituting the value of n into congruence $rf(i) + i \equiv n \pmod{pq}$ and noting that $0 \leq f(i) \leq pq - 1$, we have

$$(3.11) \qquad f(i) = 2p + 19q - 12 - 9i,$$

where $0 \leq i \leq p - 1$ or $q \leq i \leq q + p - 1$. So

$$\frac{n}{r} \begin{cases} > f(i) & \text{if } q + \frac{2p-13}{9} \leq i \leq q + p - 1; \\ < f(i) & \text{if } 0 \leq i \leq p - 1 \text{ or } q \leq i \leq q + \frac{2p-22}{9}. \end{cases}$$

It follows from Lemma 2.2 that

$$a(pqr, n) = -\sum_{j=\frac{2p-13}{9}}^{p-1} a(pq, f(q+j)).$$

On noting that $f(q + \frac{2p-13}{9}) = 10q + 1$ and $f(q + p - 1) = p + 6q + 1$, we infer from Lemma 2.1 that $a(pq, f(q + \frac{2p-13}{9})) = a(pq, f(q+p-1)) = -1$, and thus

$$a(pqr, n) = 2 - \sum_{j=\frac{2p-4}{9}}^{p-2} a(pq, f(q+j)).$$

Let $\frac{2p-4}{9} \leq j \leq p - 2$. Our task now is to show that $a(pq, f(q+j)) \neq 1$. If otherwise, then we have

$$f(q+j) \equiv 0 \pmod{p}$$

in view of Lemma 2.1. Applying (3.11) to the above congruence yields $9j + 2 \equiv 0 \pmod{p}$. Hence we deduce that $9j + 2 \in \{wp : 2 \leq w \leq 8\}$, a contradiction to $p \equiv 2 \pmod 9$. According to Lemma 2.1, we have $a(pq, f(q+j)) \in \{0, -1\}$, and thus $a(pqr, n) \geq 2$.

Case 3. $k \geq 6$.

Let $n = qr + q + r + \frac{5p-10}{9}$. Then we have $f(i) = 5p + 10q - 9 - 9i$ for $0 \leq i \leq p - 1$ and $q \leq i \leq q + p - 1$. Hence $\frac{n}{r} > f(i)$ whenever $i \in \{q + \frac{5p-10}{9}, q + \frac{5p-1}{9}, \cdots, q + p - 1\}$ and $\frac{n}{r} < f(i)$ whenever $i \in \{0, 1, \cdots, p - 1\} \cup \{q, q + 1, \cdots, q + \frac{5p-19}{9}\}$. So we infer

$$(3.12) \qquad a(pqr, n) = -\sum_{j=\frac{5p-10}{9}}^{p-1} a(pq, f(q+j)).$$

On noting that $f(q + \frac{5p-10}{9}) = q + 1$ and $f(q + p - 1) = (k - 4)p + 1$, we deduce $a(pq, f(q + \frac{5p-10}{9})) = a(pq, f(q + p - 1)) = -1$ from Lemma 2.1. Then (3.12) becomes

$$a(pqr, n) = 2 - \sum_{j=\frac{5p-1}{9}}^{p-2} a(pq, f(q + j)).$$

Recall that the coefficients of binary cyclotomic polynomials $\Phi_{pq}(x)$ can only take on one of three values: ± 1 or 0. For the purpose of proving $a(pqr, n) \geq 2$, it suffices to show $a(pq, f(q + j)) \neq 1$ for $\frac{5p-1}{9} \leq j \leq p - 2$. In view of Lemma 2.1, if $a(pq, f(q + j)) = 1$, then $f(q + j) \equiv 0 \pmod p$. This yields

$$9j + 8 \equiv 0 \pmod p.$$

It follows from $5p + 7 \leq 9j + 8 \leq 9p - 10$ that $9j + 8 \in \{wp : 6 \leq w \leq 8\}$. This is contrary to $p \equiv 2 \pmod 9$, completing the proof.

(3) Let $n = 3qr + r + \frac{7p-10}{9}$. Then $f(i) = 7p + 3q - 9 - 9i$ for $0 \leq i \leq p - 1$ and $f(q + j) = pq + 7p - 6q - 9j$ for $0 \leq j \leq p - 1$. So $\frac{l}{r} > f(i)$ whenever $i \in [\frac{7p-10}{9}, p - 1]$ and $\frac{l}{r} < f(i)$ whenever $i \in [0, \frac{7p-19}{9}] \cup [q, q + p - 1]$. So

$$(3.13) \qquad\qquad a(pqr, n) = \sum_{j=\frac{7p-10}{9}}^{p-1} a(pq, f(j)).$$

Since $f(\frac{7p-10}{9}) = 3q + 1$ and $f(p - 1) = (k - 2)p + 2q + 1$, then, by Lemma 2.1, $a(pq, f(\frac{7p-10}{9})) = a(pq, f(p - 1)) = -1$. By substituting this into (3.13), we obtain

$$a(pqr, n) = -2 + \sum_{j=\frac{7p-1}{9}}^{p-2} a(pq, f(j)).$$

Our next destination is to show that $a(pq, f(j)) \neq 1$ for $\frac{7p-1}{9} < j < p - 2$. If $a(pq, f(j)) = 1$, according to Lemma 2.1, then

$$f(j) = 7p + 3q - 9 - 9j \equiv 0 \pmod p,$$

and thus $9j + 6 \equiv 0 \pmod p$. It follows from $7p + 5 \leq 9j + 6 \leq 9p - 12$ that $9j + 6 = 8p$, a contradiction to $p \equiv 4 \pmod 9$. Taking Lemma 2.1 into consideration, we derive $a(pq, f(j)) \in \{-1, 0\}$, and thus $a(pqr, n) \leq -2$.

(4) *Case 1.* $k = 2$.

Let $n = -pr + 10qr + q + \frac{4p-11}{9}$. Then $f(i) = 3p + 19q - 11 - 9i$ for $i \in [0, p - 1] \cup [q, q + p - 1]$. So

$$\frac{n}{r} \begin{cases} > f(i) & \text{if } q + \frac{4p-11}{9} \leq i \leq q + p - 1; \\ < f(i) & \text{if } 0 \leq i \leq p - 1 \text{ or } q \leq i \leq q + \frac{4p-20}{9}. \end{cases}$$

On invoking Lemma 2.2, we have

$$a^*(pq, f(i)) = \begin{cases} a(pq, f(i)) & \text{if } i \in [q + \frac{4p-11}{9}, q + p - 1]; \\ 0 & \text{if } i \in [0, p - 1] \cup [q, q + \frac{4p-20}{9}]. \end{cases}$$

In particular, we have $f(q + \frac{4p-11}{9}) = p + 9q + 1$ and $f(q + p - 1) = 7q + 1$. It follows from Lemma 2.1 that $a(pq, f(q + \frac{4p-11}{9})) = a(pq, f(q + p - 1)) = -1$, and thus

$$a(pqr, n) = 2 - \sum_{j=\frac{4p-2}{9}}^{p-2} a(pq, f(q + j)).$$

Next we will show that $a(pq, f(q + j)) \neq 1$ for $\frac{4p-2}{9} \leq j \leq p - 2$. If not, by Lemma 2.1, we have $f(q + j) = 3p + 10q - 11 - 9j \equiv 0 \pmod{p}$. This yields $9j + 1 \equiv 0 \pmod{p}$. Since $4p - 1 \leq 9j + 1 \leq 9p - 17$, we obtain that $9j + 1 \in \{wp : 4 \leq w \leq 8\}$, a contradiction to $p \equiv 5 \pmod{9}$. So, by Lemma 2.1, $a(pq, f(q + j)) = -1$ or 0, and then $a(pqr, n) \geq 2$.

Case 2. $k \geq 6$.

Proceeding as above, let $n = 5pr + 9qr + q + r + \frac{2p-10}{9}$. Then $f(i) = 7p + 18q - 9 - 9i$ for $i \in [0, p-1] \cup [q, q+p-1]$. It is easy to show that $f(i) \leq \frac{n}{r}$ if $q + \frac{2p-10}{9} \leq i \leq q + p - 1$ and $f(i) > \frac{n}{r}$ if $0 \leq i \leq p - 1$ or $q \leq i \leq q + \frac{2p-19}{9}$.

Owing to Lemma 2.2, we have

$$a^*(pq, f(i)) = \begin{cases} a(pq, f(i)) & \text{if } i \in [q + \frac{2p-10}{9}, q + p - 1]; \\ 0 & \text{if } i \in [0, p - 1] \cup [q, q + \frac{2p-19}{9}]. \end{cases}$$

On noting that $f(q + \frac{2p-10}{9}) = 5p + 9q + 1$ and $f(q + p - 1) = (k - 2)p + 8q + 1$, we infer from Lemma 2.1 that $a(pq, f(q + \frac{2p-10}{9})) = a(pq, f(q + p - 1)) = -1$. According to Lemma 2.2, we then find that

$$a(pqr, n) = 2 - \sum_{j=\frac{2p-1}{9}}^{p-2} a(pq, f(q + j)).$$

In order to prove $a(pqr, n) \geq 2$, it remains to show that $a(pq, f(q+j)) \neq 1$ for $\frac{2p-1}{9} \leq j \leq p - 2$. If not, by Lemma 2.1, we have

$$f(q + j) = 7p + 9q - 9 - 9j \equiv 0 \pmod{p}.$$

This gives $9j \equiv 0 \pmod{p}$, a contradiction to $\frac{2p-1}{9} \leq j \leq p - 2$.

(5) Applying $n = 3pr + 9qr + q + r + \frac{4p-10}{9}$ to congruence (2.2), we infer that $f(i) = 7p + 18q - 9 - 9i$, where $0 \leq i \leq p - 1$ and $q \leq i \leq q + p - 1$. It is easy to see that $f(i) \leq \frac{n}{r}$ when $q + \frac{4p-10}{9} \leq i \leq q + p - 1$, and $f(i) > \frac{n}{r}$ when $0 \leq i \leq p - 1$ and $q \leq i \leq q + \frac{4p-19}{9}$. It follows from (2.3) and (2.4) that

$$a(pqr, n) = - \sum_{j=\frac{4p-10}{9}}^{p-1} a(pq, f(q + j)).$$

On noting $f(q + \frac{4p-10}{9}) = 3p + 9q + 1$ and $f(q+p-1) = (k-2)p + 8q + 1$, we obtain from Lemma 2.1 that $a(pq, f(q + \frac{4p-10}{9})) = a(pq, f(q+p-1)) = -1$. So

$$a(pqr, n) = 2 - \sum_{j=\frac{4p-1}{9}}^{p-2} a(pq, f(q+j)).$$

Let $\frac{4p-1}{9} \leq j \leq p-2$. If $a(pq, f(q+j)) = 1$, then, by Lemma 2.1,

$$f(q+j) = 7p + 9q - 9 - 9j \equiv 0 \pmod{p}.$$

This yields $9j \equiv 0 \pmod{p}$, a contradiction to the range of j. So $a(pq, f(q+j)) = -1$ or 0. Therefore $a(pqr, n) \geq 2$.

(6) By substituting $n = 3qr + q + r + \frac{8p-10}{9}$ into (2.2), we deduce that $f(i) = 8p + 12q - 9 - 9i$ for $i \in [0, p-1] \cup [q, q+p-1]$. It is straightforward to verify that $f(i) \leq \frac{n}{r}$ when $i \in [q + \frac{8p-10}{9}, q+p-1]$, and $f(i) > \frac{n}{r}$ when $i \in [0, p-1] \cup [q, q + \frac{8p-19}{9}]$. Then it follows from Lemma 2.2 that

$$(3.14) \qquad\qquad a(pqr, n) = - \sum_{j=\frac{8p-10}{9}}^{p-1} a(pq, f(q+j)).$$

On noting $f(q + \frac{8p-10}{9}) = 3q + 1$ and $f(q+p-1) = (k-1)p + 2q + 1$, we obtain from Lemma 2.1 that $a(pq, f(q + \frac{8p-10}{9})) = a(pq, f(q+p-1)) = -1$. Combing this with (3.14) gives

$$a(pqr, n) = 2 - \sum_{j=\frac{8p-1}{9}}^{p-2} a(pq, f(q+j)).$$

Our task now is to show that $a(pq, f(q+j)) \neq 1$ for $\frac{8p-1}{9} \leq j \leq p-2$. If the assertion would not hold, then, by Lemma 2.1,

$$f(q+j) = 8p + 3q - 9 - 9j \equiv 0 \pmod{p}.$$

Consequently, we infer that $9j + 6 \equiv 0 \pmod{p}$. This contradicts the fact that $8p + 5 \leq 9j + 6 \leq 9p - 12$. Hence the binary coefficient $a(pq, f(q+j))$ takes on one of two values: -1 or 0. Finally, we have $a(pqr, n) \geq 2$. This completes the proof of Proposition 3.1. □

REFERENCES

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

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

[3] T.J. Flanagan, *On the coefficients of ternary cyclotomic polynomials*, MS Thesis, University of Nevada, Las Vegas (2007).

[4] G.B. Imhoff, *On the coefficients of cyclotomic polynomials,* MS Thesis, California State University (2013).

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

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

[7] N. Kaplan, *Flat cyclotomic polynomials of order four and higher,* Integers **10** (2010), 357-363.

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

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

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

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

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

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

[14] B. Zhang, *The flatness of ternary cyclotomic polynomials,* Rend. Sem. Mat. Univ. Padova **145** (2021), 1-48.

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

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

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