The flatness of a class of ternary cyclotomic polynomials

By BIN ZHANG (Qufu)

Abstract. Recently, there has been much progress in our understanding of the flatness of ternary cyclotomic polynomials, but a complete classification is not known. Let \( p < q < r \) be odd primes such that \( q \equiv \pm 1 \pmod{p} \) and \( zr \equiv \pm 1 \pmod{pq} \). The cases \( 1 \leq z \leq 6 \) have been thoroughly investigated. In this paper, we concentrate on the case \( z = 7 \), giving a classification of the cases for which \( A(pqr) = 1 \). We also present some results about the coefficients of \( \Phi_{pqr}(x) \) for the general cases of \( z \).

1. Introduction

Let

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

denote the \( n \)-th cyclotomic polynomial, and let \( A(n) \) be the maximum absolute value of the coefficients of \( \Phi_n(x) \). We say that a cyclotomic polynomial is flat if \( A(n) = 1 \). In fact, if \( n \) has no more than two distinct prime factors, then \( A(n) = 1 \). It was discovered long ago, however, that one can have \( A(n) > 1 \), for instance, \( A(3 \cdot 5 \cdot 7) = 2 \) with \( a(105,7) = -2 \).

Mathematics Subject Classification: 11B83, 11C08, 11N56.
Key words and phrases: flat cyclotomic polynomial, ternary cyclotomic polynomial, coefficients of cyclotomic polynomial.
This work was supported by the National Natural Science Foundation of China (Grant No. 11801303), by Project ZR2019QA016 of Shandong Provincial Natural Science Foundation, by China Postdoctoral Science Foundation (Grant No. 2018M640617), and by the Young Talents Invitation Program of Shandong Province.
The polynomial $\Phi_n(x)$ is said to be ternary, or of order three, if $n$ is divisible by exactly three distinct odd primes. As is well known, to study the coefficients of $\Phi_n(x)$, it suffices to consider only odd, square-free integers $n$, therefore in the case of ternary polynomials we consider $\Phi_{pqr}(x)$, with odd primes $p < q < r$. In 1978, Beiter [2] classified all flat cyclotomic polynomials of the form $\Phi_{3qr}(x)$ by proving the following result.

**Proposition 1.1** (Beiter). Let $3 < q < r$ be primes such that $r = (wq \pm 1)/h$, $1 < h \leq (q - 1)/2$. Then $A(3qr) = 1$ if and only if one of these conditions holds:

1. $w \equiv 0$ and $h + q \equiv 0 \pmod{3}$, or
2. $h \equiv 0$ and $w + r \equiv 0 \pmod{3}$.

It would be a very interesting and difficult problem to classify all flat ternary cyclotomic polynomials. Nothing further was done on this until 2006, when Bachman established the existence of an infinite family of flat ternary cyclotomic polynomials. Since then, there has been a surge of interest in the coefficients of cyclotomic polynomials, but a complete classification of flat ternary cyclotomic polynomials is still unknown. In particular, Elder [3] proposed the following conjecture in 2012.

**Conjecture 1.2** (Elder). If $p < q < r$ are odd primes, then $A(pqr) = 1$ implies either $q \equiv \pm 1 \pmod{p}$ or $r \equiv \pm 1 \pmod{pq}$.

Let $zr \equiv \pm 1 \pmod{pq}$. In 2007, Kaplan [6] showed that if $z = 1$, then $A(pqr) = 1$. On the other hand, by Elder’s conjecture, one is led to think that if $z \neq 1$ and $A(pqr) = 1$, then $q \equiv \pm 1 \pmod{mp}$. At present, the cases $1 \leq z \leq 6$ have been studied by [1], [3]–[6] and [10]–[13], and the results are as follows:

- If $z = 1$, then $A(pqr) = 1$.
- If $z = 2$, then $A(pqr) = 1$ if and only if $p = 3$ and $q \equiv 1 \pmod{3}$.
- If $z = 3$, then $A(pqr) > 1$.
- If $z = 4$, then $A(pqr) = 1$ if and only if (i) $p = 3, q \geq 11$ and $q \equiv -1 \pmod{3}$ or (ii) $p = 5, q \geq 13$ and $q \equiv 1 \pmod{5}$.
- If $z = 5$, then $A(pqr) = 1$ if and only if $p = 3, q \geq 13$ and $q \equiv 1 \pmod{3}$.
- If $z = 6$ and $q \equiv \pm 1 \pmod{p}$, then $A(pqr) = 1$ if and only if (i) $p = 5, q \geq 29$ and $q \equiv -1 \pmod{5}$ or (ii) $p = 7, q \geq 43$ and $q \equiv 1 \pmod{7}$.

In this paper, we mainly consider the coefficients of ternary cyclotomic polynomials in the case $z = 7$, and prove the following result.
Theorem 1.3. Let \( p < q < r \) be odd primes such that \( q \equiv \pm 1 \pmod{p} \) and \( 7r \equiv \pm 1 \pmod{pq} \). Then \( A(pqr) = 1 \) if and only if \( p = 3, \ q \geq 17 \) and \( q \equiv -1 \pmod{3} \).

The methods used in the proof of the above theorem can likely be applied with the condition \( 7r \equiv \pm 1 \pmod{pq} \) replaced by \( zr \equiv \pm 1 \pmod{pq} \) where \( z \) is allowed to be more than just 7. We would eventually like to classify all flat ternary cyclotomic polynomials \( \Phi_{pqr}(x) \) for all \( z \). However, there are too many cases to consider and this appears rather difficult. We have just obtained the following result for the general cases of \( z \).

Theorem 1.4. Let \( p < q < r \) be odd primes such that \( q \equiv \ell \pmod{p} \) and \( zr \equiv \pm 1 \pmod{pq} \), where \( 2 \leq \ell \leq p - 2 \) and \( z \geq 2 \). If \( p > 2z + 1 \) and \( \ell \equiv 0 \pmod{z} \), then \( A(pqr) \geq 2 \).

2. Preliminaries

In this section, we present some lemmas which are useful to prove our theorems. First recall that the coefficients of \( \Phi_{pqr}(x) \) and \( \Phi_{pq}(x) \) could be computed explicitly by the following two lemmas, respectively.

Lemma 2.1 ([6]). Let \( p < q < r \) be odd primes. Let \( n \geq 0 \) be an integer, and \( f(i) \) the unique value \( 0 \leq f(i) \leq pq - 1 \) such that
\[
rf(i) + i \equiv n \pmod{pq}.
\]

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

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

Lemma 2.2 ([7] or [9]). Let \( p < q \) be odd primes. Let \( s \) and \( t \) be positive integers such that \( pq + 1 = sp + tq \) is written uniquely. Then
\[
a(pq,j) = \begin{cases} 
1 & \text{if } j = up + vq \text{ with } 0 \leq u \leq s - 1, 0 \leq v \leq t - 1; \\
-1 & \text{if } j = up + vq + 1 \text{ with } 0 \leq u \leq q - s - 1, 0 \leq v \leq p - t - 1; \\
0 & \text{otherwise.} \end{cases}
\]
We will use Lemma 2.2 in the cases \( q \equiv \pm 1 \pmod{p} \), and we write these two cases as lemmas as follows.

**Lemma 2.3.** Let \( p < q \) be odd primes satisfying \( q = kp + 1 \). Then

\[
a(pq, j) = \begin{cases} 
1 & \text{if } j = up \text{ with } 0 \leq u \leq s - 1; \\
-1 & \text{if } j = up + vq + 1 \text{ with } 0 \leq u \leq k - 1, 0 \leq v \leq p - 2; \\
0 & \text{otherwise}. 
\end{cases}
\]

**Lemma 2.4.** Let \( p < q \) be odd primes satisfying \( q = kp - 1 \). Then

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

We now provide bounds for the values of \( s, t \) used in the proof of Theorem 1.4.

**Lemma 2.5.** Let \( p < q \) be odd primes with \( q = kp + \ell \) for some \( 2 \leq \ell \leq p - 2 \). Let \( s, t \) be the unique integers \( 1 \leq s \leq q - 1, 1 \leq t \leq p - 1 \), such that \( pq + 1 = ps + qt \). Then (i) \( 2 \leq t \leq p - 1 \); (ii) \( s \leq q - k - 2 \).

**Proof.** (i) Since \( t = 1 \) if and only if \( q \equiv 1 \pmod{p} \), we have \( 2 \leq t \leq p - 1 \).

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

\[
ps = pq + 1 - qt = pq - (tkp + \ell t - 1),
\]

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

We also need the next periodicity result for \( A(pqr) \) due to Kaplan [6].

**Lemma 2.6** ([6]). Let \( p < q < r \) be odd primes. Then for any prime \( s > q \) such that \( s \equiv \pm r \pmod{pq} \), \( A(pqr) = A(pqs) \).

3. Proof of Theorem 1.3 when \( p = 3 \)

By using Proposition 1.1 with \( h = 7 \) and \( w = 3 \), we have

**Corollary 3.1.** Let \( q \geq 17 \) and \( 7r \equiv \pm 1 \pmod{3q} \), then \( A(3qr) = 1 \) if and only if \( q \equiv -1 \pmod{3} \).
By using the PARI/GP system, we obtain \( A(3 \cdot 5 \cdot 13) = A(3 \cdot 11 \cdot 19) = A(3 \cdot 13 \cdot 67) = 2 \). Then it follows from Lemma 2.6 that \( A(3 \cdot q \cdot r) = 2 \) for \( q = 5, 11, 13 \) and \( 7r \equiv \pm 1 \pmod{3q} \). Combining this with Corollary 3.1 gives the following result.

**Proposition 3.2.** Let \( 3 < q < r \) be primes such that \( 7r \equiv \pm 1 \pmod{3q} \). Then \( A(3qr) = 1 \) if and only if \( q \geq 17 \) and \( q \equiv -1 \pmod{3} \).

4. Proof of Theorem 1.3 when \( p = 5 \)

In view of Lemma 2.6, Theorem 1.3 will be proved in the case \( p = 5 \) by showing the following two propositions.

**Proposition 4.1.** Let \( 5 < q < r \) be primes such that \( q \equiv 1 \pmod{5} \) and \( 7r \equiv 1 \pmod{5q} \).
1. If \( q = 11 \), then \( A(55r) = 2 \).
2. If \( q > 11 \), then \( a(5qr, 2qr + 16r + q + 1) = 2 \).

**Proof.** (1) By using the PARI/GP system, we have \( A(5 \cdot 11 \cdot 173) = 2 \). Thus, by Lemma 2.6, we have \( A(55r) = 2 \) for primes \( r \) with \( 7r \equiv 7 \cdot 173 \equiv 1 \pmod{55} \).

(2) Let \( n = 2qr + 16r + q + 1 \). In order to use Lemma 2.1, we need to determine for which \( i \) the inequality \( rf(i) > n \) is satisfied. By using the congruence

\[ rf(i) + i \equiv n \pmod{5q} \]

and noting that \( 0 \leq f(i) \leq 5q - 1 \), we infer

\[ f(i) = 4q + 23 - 7i \quad \text{and} \quad f(q + i) = 2q + 23 - 7i, \]

where \( 0 \leq i \leq 4 \). So

\[ rf(0) > rf(1) > \cdots > rf(4) > rf(q) > n > rf(q + 1) > \cdots > rf(q + 4). \]

Then it follows from Lemma 2.1 that

\[ a(5qr, n) = -\sum_{i=1}^{4} a(pq, f(q + i)). \]

Let \( q = 5k + 1 \). Then \( k \geq 4 \). Note that \( f(q+1) = 3 \cdot 5 + 2 \cdot q + 1 \) and \( f(q+4) = (k-1) \cdot 5 + 1 \cdot q + 1 \). By Lemma 2.3, we have \( a(pq, f(q+1)) = a(pq, f(q+4)) = -1 \).
It follows from \( f(q+2) = 2q+9 \equiv 1 \pmod{5} \) and Lemma 2.3 that \( a(pq, f(q+2)) \neq 1 \). If \( a(pq, f(q+2)) = -1 \), then
\[
f(q+2) = u \cdot 5 + v \cdot q + 1 \tag{4.1}
\]
for \( 0 \leq u \leq k-1 \) and \( 0 \leq v \leq p-2 \). Since \( 0 < f(q+2) < 3q \), we obtain \( v = 0, 1 \) or \( 2 \). On the other hand, taking equality (4.1) modulo 5 gives
\[
v \equiv 0 \pmod{5}.
\]
Then we have \( v = 0 \), and thus \( u = 2k + 2 \), a contradiction to \( 0 \leq u \leq k-1 \). Consequently, we infer that \( a(pq, f(q+2)) = 0 \) by Lemma 2.3. Similarly, we can show that \( a(pq, f(q+3)) = 0 \).

Hence
\[
a(5qr, n) = -(-1 + 0 + 0 - 1) = 2.
\]
This completes the proof of Proposition 4.1.

**Proposition 4.2.** Let \( 5 < q < r \) be primes such that \( q \equiv 1 \pmod{5} \) and \( 7r \equiv 1 \pmod{q} \).

1. If \( q = 19 \), then \( A(95r) = 2 \).
2. If \( q > 19 \), then \( a(5qr, qr + 10r + 2) = 2 \).

**Proof.** (1) By using the PARI/GP system, we have \( A(5 \cdot 19 \cdot 163) = 2 \). Thus, by Lemma 2.6, we have \( A(95r) = 2 \) for primes \( r \) with \( 7r \equiv 7 \cdot 163 \equiv 1 \pmod{95} \).

(2) Let \( n = qr + 10r + 2 \). By using the congruence (2.1) and \( 0 \leq f(i) \leq 5q-1 \), we infer
\[
f(i) = q + 24 - 7i \quad \text{and} \quad f(q + i) = 4q + 24 - 7i,
\]
where \( 0 \leq i \leq 4 \). So \( rf(i) > n \) whenever \( i \in \{0, 1, q, q + 1, \ldots, q + 4\} \), and \( rf(i) \leq n \) whenever \( i \in \{2, 3, 4\} \). Then, by Lemma 2.1,
\[
a(5qr, n) = a(5q, f(2)) + a(5q, f(3)) + a(5q, f(4)).
\]
Let \( q = 5k - 1 \). Then \( k > 4 \). Note that \( f(2) = 2 \cdot 5 + 1 \cdot q \) and \( f(4) = (k-1) \cdot 5 \). It follows from Lemma 2.4 that \( a(5q, f(2)) = a(5q, f(4)) = 1 \).

On invoking \( f(3) = q + 3 \equiv 2 \pmod{5} \) and Lemma 2.4, we obtain that \( a(5q, f(3)) \neq -1 \). If \( a(pq, f(3)) = 1 \), then
\[
f(3) = u \cdot 5 + v \cdot q,
\]
where \( 0 \leq u \leq k-1 \) and \( 0 \leq v \leq p-2 \). Taking this equality modulo 5 gives
\[
v \equiv 3 \pmod{5}.
\]
This contradicts the fact \( 0 < f(3) < 2q \). So, by Lemma 2.4, \( a(5q, f(3)) = 0 \). Therefore, we infer that \( a(5qr, n) = 1 + 0 + 1 = 2 \).
5. Proof of Theorem 1.3 when \( p > 7 \)

Note that the congruence \( 7r \equiv \pm 1 \pmod{pq} \) yields \( p \neq 7 \). In this section, we prove the following two propositions to finish the proof of Theorem 1.3.

**Proposition 5.1.** Let \( 7 < p < q < r \) be odd primes such that \( q \equiv 1 \pmod{p} \) and \( 7r \equiv 1 \pmod{pq} \).

(1) If \( p \equiv 1 \pmod{14} \), \( q = 2p + 1 \), then \( a(pqr, 5pr + 5qr + 3r + q + \frac{2p-9}{7}) \geq 2 \).

(2) If \( p \equiv 1 \pmod{14} \), \( q = 4p + 1 \), then \( a(pqr, 8pr + 5qr + 3r + q + \frac{2p-9}{7}) \geq 2 \).

(3) If \( p \equiv 1 \pmod{14} \), \( q \geq 6p + 1 \), then \( a(pqr, 4pr + 7qr + q + r + \frac{2p-9}{7}) \geq 2 \).

(4) If \( p \equiv 3 \pmod{14} \), then \( a(pqr, pq + pr - 10qr + r + q + \frac{5p-9}{7}) \geq 2 \).

(5) If \( p \equiv 5 \pmod{14} \), then \( a(pqr, pq + 3pr - 10qr + r + q + \frac{3p-9}{7}) \geq 2 \).

(6) If \( p \equiv 9 \pmod{14} \), then \( a(pqr, pq + pr - 11qr + r + q + \frac{4p-8}{7}) \geq 2 \).

(7) If \( p \equiv 11 \pmod{14} \), \( q = 2p + 1 \), then \( a(pqr, 4pr + qr + q + 3r + \frac{4p-9}{7}) \geq 2 \).

(8) If \( p \equiv 11 \pmod{14} \), \( q = 4p + 1 \), then \( a(pqr, 7pr + 6qr + q + 2r + \frac{2p-8}{7}) \geq 2 \).

(9) If \( p \equiv 11 \pmod{14} \), \( q \geq 6p + 1 \), then \( a(pqr, pq + pr - 8qr + q + r + \frac{2p-8}{7}) \geq 2 \).

(10) If \( p \equiv 13 \pmod{14} \), then \( a(pqr, pq + pr - 10qr + q + r + \frac{6p-5}{7}) \geq 2 \).

**Proof.** (1) Let \( n = 5qr + 5pr + 3r + q + \frac{2p-9}{7} \). By substituting \( n \) into congruence (2.1) and using \( 0 \leq f(i) \leq pq - 1 \), we have

\[
f(i) = 7p + 12q - 6 - 7i, \quad (5.1)
\]

where \( i \in [0, p - 1] \cup [q, q + p - 1] \). Then one readily verifies that \( rf(i) > n \) when \( i \in [0, p - 1] \cup [q, q + \frac{2p-10}{7}] \), and \( rf(i) \leq n \) when \( i \in [q + \frac{2p-9}{7}, q + p - 1] \). It follows from Lemma 2.1 that

\[
a(pqr, n) = - \sum_{i=\frac{2p-9}{7}}^{p-1} a(pq, f(q + i)). \quad (5.2)
\]

Note that \( f(q + \frac{2p-9}{7}) = 1 \cdot p + 7 \cdot q + 1 \) and \( f(q + p - 1) = 5 \cdot q + 1 \). Therefore, by \( q = 2p + 1 \) and Lemma 2.3, we get \( a(pq, f(q + \frac{2p-9}{7})) = a(pq, f(q + p - 1)) = -1 \). So equality (5.2) becomes

\[
a(pqr, n) = 2 - \sum_{i=\frac{2p-9}{7}}^{p-2} a(pq, f(q + i)).
\]

Recall that as a coefficient of binary cyclotomic polynomial \( \Phi_{pq}(x) \), the quantity \( a(pq, f(q + i)) \) takes on one of three values: \(-1, 0, 1\). Our task now is to show that

\[
a(pq, f(q + i)) \neq 1 \quad \text{for} \quad \frac{2p-2}{7} \leq i \leq p - 2.
\]
If not, then, by Lemma 2.3, we get \( f(q+i) \equiv 0 \pmod{p} \). Combining this with (5.1) gives
\[
7i + 1 \equiv 0 \pmod{p}.
\]
Since \( 2p - 1 \leq 7i + 1 \leq 7p - 13 \), we have \( 7i + 1 = 2p, 3p, 4p, 5p \) or \( 6p \). This contradicts the fact that \( p \equiv 1 \pmod{14} \). Thus we conclude that \( a(pqr, n) \geq 2 \).

(2) Let \( n = 8pr + 5qr + 3r + q + \frac{2p - 9}{7} \). Proceeding as in the proof of (1), we obtain
\[
f(i) = 10p + 12q - 6 - 7i,
\]
where \( i \in [0, p-1] \cup [q, q+p-1] \). Then one readily verifies that \( r f(i) > n \) when \( i \in [0, p-1] \cup [q, q+p-1] \), and \( r f(i) \leq n \) when \( i \in [q + \frac{2p - 9}{7}, q + p - 1] \). It follows from Lemma 2.1 that
\[
a(pqr, n) = - \sum_{i=\frac{2p - 9}{7}}^{p-1} a(pq, f(q+i)).
\]
Note that \( f(q + 2p - 9) = 7 \cdot q + 1 \) and \( f(q + p - 1) = 3 \cdot p + 5 \cdot q + 1 \). Therefore, by \( q = 4p + 1 \) and Lemma 2.3, we have \( a(pq, f(q + 2p - 9)) = a(pq, f(q + p - 1)) = -1 \).

So
\[
a(pqr, n) = 2 - \sum_{i=\frac{2p - 9}{7}}^{p-2} a(pq, f(q+i)).
\]
Owing to Lemma 2.3, it remains to show that
\[
a(pq, f(q+i)) \neq 1 \quad \text{for} \quad \frac{2p - 2}{7} \leq i \leq p - 2.
\]

If otherwise, then \( f(q+i) \equiv 0 \pmod{p} \). Applying equation (5.3) to this yields
\[
7i + 1 \equiv 0 \pmod{p}.
\]
Since \( 2p - 1 \leq 7i + 1 \leq 7p - 13 \), we have \( 7i + 1 = 2p, 3p, 4p, 5p \) or \( 6p \), a contradiction to the fact that \( p \equiv 1 \pmod{14} \). Thus we conclude that \( a(pqr, n) \geq 2 \).

(3) Let \( n = 4pr + 7qr + q + r + \frac{p - 9}{7} \). By using congruence (2.1), we obtain
\[
f(i) = 5p + 14q - 7 - 7i, \quad \text{where} \quad i \in [0, p-1] \cup [q, q+p-1].
\]
Then \( r f(i) > n \) when \( i \in [0, p-1] \cup [q, q + \frac{p - 12}{7}] \), and \( r f(i) \leq n \) when \( i \in [q + \frac{p - 9}{7}, q + p - 1] \). It follows from Lemma 2.1 that
\[
a(pqr, n) = - \sum_{i=\frac{p - 9}{7}}^{p-1} a(pq, f(q+i)).
\]
Since $f(q + \frac{p-8}{7}) = 4 \cdot p + 7 \cdot q + 1$ and $f(q + p - 1) = \frac{q-2p-1}{p} \cdot p + 6 \cdot q + 1$, we have $a(pq, f(q + \frac{p-8}{7})) = a(pq, f(q + p - 1)) = -1$, and then

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

We claim that

$$a(pq, f(q+i)) \neq 1 \quad \text{for} \quad \frac{p-1}{7} \leq i \leq p-2.$$ 

If the assertion did not hold, then $f(q+i) \equiv 0 \pmod{p}$. Therefore

$$7i \equiv 0 \pmod{p}.$$ 

Since $p-1 \leq 7i \leq 7p-14$, we have $7i+1 = p, 2p, 3p, 4p, 5p$ or $6p$, a contradiction to the fact that $p \equiv 1 \pmod{14}$. Thus we conclude that $a(pqr, n) \geq 2.$

(4) Let $n = pqr + pr - 10qr + r + q + \frac{5p-8}{7}$. Then $f(i) = pq + 6p - 3q - 7 - 7i$, where $i \in [0, p-1] \cup [q, q+p-1]$. So

$$rf(i) \begin{cases} > n, & \text{if} \ i \in [0, p-1] \cup [q, q + \frac{5p-15}{7}], \\ \leq n, & \text{if} \ i \in [q + \frac{5p-8}{7}, q + p - 1]. \end{cases}$$

It follows from Lemma 2.1 that

$$a(pqr, n) = - \sum_{i=\frac{5p-8}{7}}^{\frac{p-1}{7}} a(pq, f(q+i)).$$

Noting that $f(q + \frac{5p-8}{7}) = 1 \cdot p + (p-10) \cdot q + 1$ and $f(q + p - 1) = \frac{2p-1}{p} \cdot p + (p-11) \cdot q + 1$, we have $a(pq, f(q + \frac{5p-8}{7})) = a(pq, f(q + p - 1)) = -1$, and thus

$$a(pqr, n) = 2 - \sum_{i=\frac{5p-8}{7}}^{\frac{p-1}{7}} a(pq, f(q+i)).$$

We claim that

$$a(pq, f(q+i)) \neq 1 \quad \text{for} \quad \frac{5p-1}{7} \leq i \leq p-2.$$ 

If the statement was false, then $f(q+i) \equiv 0 \pmod{p}$. Hence

$$7i + 17 \equiv 0 \pmod{p}.$$
On account of $5p + 16 \leq 7i + 17 \leq 7p + 3$, we have $7i + 17 = 6p$ or $7p$, a contradiction to the fact that $p \equiv 3 \pmod{14}$. It follows from Lemma 2.3 that $a(pqr, n) \geq 2$.

(5) Let $n = pq + 3pr - 10qr + q + r + \frac{3p-8}{7}$. Then $f(i) = pq + 6p - 3q - 7 - 7i$, where $i \in [0, p - 1] \cup [q, q + p - 1]$. So

$$rf(i) \begin{cases} > n, & \text{if } i \in [0, p - 1] \cup [q, q + \frac{3p-15}{7}], \\ \leq n, & \text{if } i \in [q + \frac{3p-8}{7}, q + p - 1]. \end{cases}$$

Thus, by Lemma 2.1,

$$a(pqr, n) = - \sum_{i=\frac{3p-8}{7}}^{p-1} a(pq, f(q+i)).$$

It follows from $f(q + \frac{3p-8}{7}) = 3 \cdot p + (p - 10) \cdot q + 1$ and $f(q + p - 1) = \frac{q-p-1}{p} \cdot p + (p - 11) \cdot q + 1$ that $a(pq, f(q + \frac{3p-8}{7})) = a(pq, f(q + p - 1)) = -1$, and then

$$a(pqr, n) = 2 - \sum_{i=\frac{3p-15}{7}}^{p-2} a(pq, f(q+i)). \quad (5.4)$$

We claim that

$$a(pq, f(q+i)) \neq 1 \quad \text{for } \frac{3p-1}{7} \leq i \leq p-2.$$ 

If the statement was not true, then $f(q+i) \equiv 0 \pmod{p}$. Hence $7i + 17 \equiv 0 \pmod{p}$. In view of $3p + 16 \leq 7i + 17 \leq 7p + 3$, we have $7i + 17 = 4p, 5p, 6p$ or $7p$, a contradiction to the fact that $p \equiv 5 \pmod{14}$. Combining this with Lemma 2.3 and (5.4) gives $a(pqr, n) \geq 2$.

(6) Let $n = pq + pr - 11qr + q + r + \frac{3p-8}{7}$. Then $f(i) = pq + 5p - 4q - 7 - 7i$, where $i \in [0, p - 1] \cup [q, q + p - 1]$. It is clear that

$$rf(i) \begin{cases} > n, & \text{if } i \in [0, p - 1] \cup [q, q + \frac{4p-15}{7}], \\ \leq n, & \text{if } i \in [q + \frac{3p-8}{7}, q + p - 1]. \end{cases}$$

So, by Lemma 2.1,

$$a(pqr, n) = - \sum_{i=\frac{4p-8}{7}}^{p-1} a(pq, f(q+i)).$$
Observing that \( f(q + 4p - 8) = 1 \cdot p + (p - 12) \cdot q + 1 \) and \( f(q + p - 1) = \frac{q - 2p - 1}{p} \cdot p + (p - 12) \cdot q + 1 \), we have \( a(pq, f(q + 4p - 8)) = a(pq, f(q + p - 1)) = -1 \), and then
\[
a(pqr, n) = 2 - \sum_{i=\frac{4p-1}{7}}^{p-2} a(pq, f(q + i)). \tag{5.5}
\]

Next we will show that
\[ a(pq, f(q + i)) \neq 1 \text{ for } \frac{4p-1}{7} \leq i \leq p - 2. \]

In fact, if the assertion was not true, then \( f(q + i) \equiv 0 \pmod{p} \). So \( 7i + 18 \equiv 0 \pmod{p} \). On noting that \( 4p + 17 \leq 7i + 18 \leq 7p + 4 \), we have \( 7i + 18 = 5p, 6p \) or \( 7p \), a contradiction to the fact that \( p \equiv 9 \pmod{14} \). Combining this with Lemma 2.3 and (5.5) gives \( a(pqr, n) \geq 2 \).

(7) Let \( n = 4pr + qr + q + 3r + \frac{4p-9}{7} \). Then \( f(i) = 8p + 8q - 6 - 7i, \) where \( i \in [0, p - 1] \cup [q, q + p - 1] \). It is clear that
\[
r(f(i)) \begin{cases} > n, & \text{if } i \in [0, p - 1] \cup [q, q + \frac{4p-16}{7}], \\ \leq n, & \text{if } i \in [q + \frac{4p-9}{7}, q + p - 1]. \end{cases}
\]

So, by Lemma 2.1,
\[
a(pqr, n) = - \sum_{i=\frac{4p-9}{7}}^{p-2} a(pq, f(q + i)).
\]

Observing that \( f(q + 4p - 9) = 3 \cdot q + 1 \) and \( f(q + p - 1) = p + q + 1 \), we have \( a(pq, f(q + 4p - 9)) = a(pq, f(q + p - 1)) = -1 \), and then
\[
a(pqr, n) = 2 - \sum_{i=\frac{4p-9}{7}}^{p-2} a(pq, f(q + i)). \tag{5.6}
\]

Next we will show that
\[ a(pq, f(q + i)) \neq 1 \text{ for } \frac{4p-2}{7} \leq i \leq p - 2. \]

In fact, if the assertion was not true, then \( f(q + i) \equiv 0 \pmod{p} \). So \( 7i + 5 \equiv 0 \pmod{p} \). On noting that \( 4p + 3 \leq 7i + 18 \leq 7p - 9 \), we have \( 7i + 18 = 5p \) or \( 6p \), a contradiction to the fact that \( p \equiv 11 \pmod{14} \). Taking this, Lemma 2.3 and (5.6) into consideration, we have \( a(pqr, n) \geq 2 \).
(8) Let \( n = 7pr + 6qr + q + 2r + \frac{2p - 8}{7} \). Then
\[
f(i) = 9p + 13q - 6 - 7i,
\]
where \( i \in [0, p - 1] \cup [q, q + p - 1] \). So
\[
rf(i) \begin{cases} 
> n, & \text{if } i \in [0, p - 1] \cup [q, q + \frac{2p - 15}{7}], \\
\leq n, & \text{if } i \in [q + \frac{2p - 8}{7}, q + p - 1].
\end{cases}
\]
Thus, by Lemma 2.1,
\[
a(pqr, n) = - \sum_{i=2}^{p-1} a(pq, f(q + i)).
\]
It follows from \( f(q + \frac{2p - 8}{7}) = 3 \cdot p + 7 \cdot q + 1 \) and \( f(q + p - 1) = 2p + 6q + 1 \) that \( a(pq, f(q + \frac{2p - 8}{7})) = a(pq, f(q + p - 1)) = -1 \), and then
\[
a(pqr, n) = 2 - \sum_{i=\frac{2p - 8}{7}}^{p-2} a(pq, f(q + i)). \quad (5.8)
\]
Next we will show that
\[
a(pq, f(q + i)) \neq 1 \text{ for } \frac{2p - 1}{7} \leq i \leq p - 2.
\]
In fact, if the assertion was not true, then \( f(q + i) \equiv 0 \pmod{p} \). Substituting (5.7) into this congruence yields \( 7i \equiv 0 \pmod{p} \). Since \( p > 7 \), we infer that \( p|i \), a contradiction to the fact that \( \frac{2p - 1}{7} \leq i \leq p - 2 \). In view of Lemma 2.3 and (5.8), we obtain \( a(pqr, n) \geq 2 \).

(9) Let \( n = pqr + 4pr - 8qr + q + r + \frac{2p - 8}{7} \). Then
\[
f(i) = pq + 6p - q - 7i,
\]
where \( i \in [0, p - 1] \cup [q, q + p - 1] \). So
\[
rf(i) \begin{cases} 
> n, & \text{if } i \in [0, p - 1] \cup [q, q + \frac{2p - 15}{7}], \\
\leq n, & \text{if } i \in [q + \frac{2p - 8}{7}, q + p - 1].
\end{cases}
\]
Thus, by Lemma 2.1,
\[
a(pqr, n) = - \sum_{i=\frac{2p - 8}{7}}^{p-1} a(pq, f(q + i)).
\]
It follows from \( f(q + \frac{2p-8}{7}) = 4 \cdot p + (p - 8) \cdot q + 1 \) and \( f(q + p - 1) = \frac{2p-1}{p} \cdot p + (p - 9) \cdot q + 1 \) that \( a(pq, f(q + \frac{2p-8}{7})) = a(pq, f(q + p - 1)) = -1 \), and then

\[
a(pqr, n) = 2 - \sum_{i=\frac{2p-1}{7}}^{p-2} a(pq, f(q + i)).
\]

Next we will show that

\[
a(pq, f(q + i)) \neq 1 \quad \text{for } \frac{2p-1}{7} \leq i \leq p - 2.
\]

In fact, if the assertion was not true, then \( f(q + i) \equiv 0 \pmod{p} \). Substituting (5.9) into this congruence yields \( 7i + 15 \equiv 0 \pmod{p} \). On noting that \( 2p + 14 \leq 7i + 15 \leq 7p + 1 \), we infer \( 7i + 15 = 7p, 4p, 5p, 6p \) or \( 7p \). This is a contradiction, which completes the proof of Proposition 5.1.

□

(10) Let \( n = pqr - 10qr + q + r + \frac{6p-8}{7} \). Then

\[
f(i) = pq + 6p - 3q - 7 - 7i,
\]

where \( i \in [0, p - 1] \cup [q, q + p - 1] \). So

\[
rf(i) \begin{cases} > n, & \text{if } i \in [0, p - 1] \cup [q, q + \frac{6p-15}{7}], \\ \leq n, & \text{if } i \in [q + \frac{6p-8}{7}, q + p - 1]. \\
\end{cases}
\]

Thus, by Lemma 2.1,

\[
a(pqr, n) = - \sum_{i=\frac{6p-8}{7}}^{p-1} a(pq, f(q + i)).
\]

It follows from \( f(q + \frac{6p-8}{7}) = (p - 10) \cdot q + 1 \) and \( f(q + p - 1) = \frac{2p-1}{p} \cdot p + (p - 11)q + 1 \) that \( a(pq, f(q + \frac{6p-8}{7})) = a(pq, f(q + p - 1)) = -1 \), and then

\[
a(pqr, n) = 2 - \sum_{i=\frac{6p-1}{7}}^{p-2} a(pq, f(q + i)).
\]

Next we will show that

\[
a(pq, f(q + i)) \neq 1 \quad \text{for } \frac{6p-1}{7} \leq i \leq p - 2.
\]

In fact, if the assertion was not true, then \( f(q + i) \equiv 0 \pmod{p} \). Substituting (5.10) into this congruence yields \( 7i + 17 \equiv 0 \pmod{p} \). On noting that \( 6p + 16 \leq 7i + 17 \leq 7p + 3 \), we infer \( 7i + 15 = 7p \). This is a contradiction, which completes the proof of Proposition 5.1.
Proposition 5.2. Let 7 < p < q < r be primes such that q \equiv -1 \pmod{p} and 7r \equiv 1 \pmod{pq}.

(1) If \( p \equiv 1 \pmod{14} \), then \( a(pqr, pqr - 11q + q + \frac{6p-6}{7}) \leq -2 \).

(2) If \( p \equiv 3 \pmod{14} \), \( q > 2p - 1 \), then \( a(pqr, pqr - 10q + q + \frac{4p-5}{7}) \leq -2 \).

(3) If \( p \equiv 3 \pmod{14} \), \( q \geq 4p - 1 \), then \( a(pqr, pqr + 3pr - 11q + q + \frac{2p-6}{7}) \leq -2 \).

(4) If \( p \equiv 5 \pmod{14} \), then \( a(pqr, pqr + pr - 11q + q + \frac{3p-4}{7}) \leq -2 \).

(5) If \( p \equiv 9 \pmod{14} \), \( q = 2p - 1 \), then \( a(pqr, 6pr + 8qr - 3r + q + \frac{2p-4}{7}) \leq -2 \).

(6) If \( p \equiv 9 \pmod{14} \), \( q \geq 4p - 1 \), then \( a(pqr, 3pr + 6q + q + \frac{3p-6}{7}) \leq -2 \).

(7) If \( p \equiv 11 \pmod{14} \), then \( a(pqr, pqr + pr - 10q + q + \frac{5p-6}{7}) \leq -2 \).

(8) If \( p = 13 \), then \( a(13qr, 6qr + 52r + 1) \geq 2 \).

(9) If \( p > 13 \), \( p \equiv 13 \pmod{14} \), \( q = 2p - 1 \), then \( a(pqr, 5pr + 5qr - 2r + q + \frac{2p-5}{7}) \leq -2 \).

(10) If \( p > 13 \), \( p \equiv 13 \pmod{14} \), \( q = 4p - 1 \), then \( a(pqr, 7pr + 5qr - r + q + \frac{p-6}{7}) \leq -2 \).

(11) If \( p > 13 \), \( p \equiv 13 \pmod{14} \), \( q \geq 6p - 1 \), then \( a(pqr, 4pr + 6qr + q + \frac{p-6}{7}) \leq -2 \).

**Proof.** The proof of this proposition can be completed by the method analogous to that used above. We omit the straight-forward details. \(\square\)

6. Proof of Theorem 1.4

In view of Lemma 2.6, the theorem will be proved by showing that

\[ a \left( pqr, qr + p + q + r - 1 - \frac{\ell}{z} \right) \geq 2, \]

where \( q \equiv \ell \pmod{p} \) and \( zr \equiv 1 \pmod{pq} \).

Let \( q = kp + \ell \) and \( n = qr + p + q + r - 1 - \frac{\ell}{z} \). By using \( rf(i) + i \equiv n \pmod{pq} \), we have

\[ f(i) \equiv zp + (z + 1)q - \ell - z + 1 - zi \pmod{pq}, \quad (6.1) \]

where \( i \in [0, p - 1] \cup [q, q + p - 1] \). The condition \( 2z + 1 < p \) ensures that

\[ zp + (z + 1)q - \ell - z + 1 - z \cdot 0 < (2z + 1)p < pq. \quad (6.2) \]

Obviously,

\[ 0 < kp + 1 < zp + (z + 1)q - \ell - z + 1 - z \cdot (q + p - 1). \quad (6.3) \]
Hence, by (6.2) and (6.3), congruence (6.1) becomes \( f(i) = zp + (z+1)q - \ell - z + 1 - zi \). Then one readily verifies that
\[
\begin{align*}
    n < rf \left( q + p - 2 - \frac{\ell}{z} \right) < \cdots < rf(q) < rf(p-1) < \cdots < rf(0);  \\
    n > rf \left( q + p - 1 - \frac{\ell}{z} \right) > \cdots > rf(q+p-1).
\end{align*}
\] (6.4) (6.5)

Let \( pq + 1 = ps + qt \). Then \( f(q+p-1 - \frac{\ell}{z}) = q + 1 \). By Lemma 2.5 (i), we have \( 2 \leq t \leq p - 2 \). Thus \( 1 \leq p - t - 1 \), and so by Lemma 2.2, we get \( a(pq, f(q+p-1 - \frac{\ell}{z})) = -1 \). Clearly, \( f(q+p-1) = kp + 1 \). Lemma 2.5 (ii) gives \( k \leq q - s - 2 \). So by Lemma 2.2 once again, we have \( a(pq, f(q+p-1)) = -1 \).

Therefore, by (6.4), (6.5) and Lemma 2.1, we obtain
\[
a(pqr, n) = - \sum_{i=p-1-\frac{\ell}{z}}^{p-1} a(pq, f(q+i)) = 2 - \sum_{i=p-1-\frac{\ell}{z}}^{p-2} a(pq, f(q+i)).
\] (6.6)

We will now show that \( a(pq, f(q+i)) \neq 1 \), where \( p - \frac{\ell}{z} \leq i \leq p - 2 \). (6.7)

To this end, according to Lemma 2.2, we only have to prove that \( f(q+i) \) cannot be written in the form \( up + vq \) for some \( 0 \leq u \leq s - 1 \) and \( 0 \leq v \leq t - 1 \).

Suppose that \( f(q+i) = zp + q - \ell + 1 - (1+i)z = up + vq \).

Since
\[
0 < f(q+p-1) < f(q+i) \leq f \left( q + p - \frac{\ell}{z} \right) = 2q + 1 - z < q,
\]
we have \( v = 0 \). Then we obtain that
\[
f(q+i) = zp + q - \ell + 1 - (1+i)z = up.
\]

Taking this equality modulo \( p \) gives
\[
(1+i)z - 1 \equiv 0 \pmod{p}.
\]

Note that \( (z-1)p < pz - \ell + z - 1 < (1+i)z - 1 < pz - z - 1 < zp \). Therefore, we derive a contradiction and prove our claim (6.7).

So, by Lemma 2.2, \( a(pq, f(q+i)) = 0 \) or \(-1 \), where \( p - \frac{\ell}{z} \leq i \leq p - 2 \). Finally, it follows from this and (6.6) that \( a(pqr, n) \geq 2 \).

Acknowledgements. I would like to express my sincere gratitude to the referee and the editor for carefully reading the manuscript and giving valuable comments.
References