CURIOS CONGRUENCES ON CYCLOTOMIC POLYNOMIALS

SHIGEKI AKIYAMA AND HAJIME KANEKO

Abstract. Let \( \Phi_n^{(k)}(x) \) be the \( k \)-th derivative of \( n \)-th cyclotomic polynomial. Extending a work of D. H. Lehmer [4], we show some curious congruences: 
\[
2\Phi_n^{(3)}(1) \text{ is divisible by } \phi(n) - 2 \text{ and } \Phi_n^{(2k+1)}(1) \text{ is divisible by } \phi(n) - 2k \text{ for } k \geq 2.
\]

1. Introduction

The \( n \)-th cyclotomic polynomial
\[
\Phi_n(x) = \prod_{0 < d < n, (d,n) = 1} \left( x - \exp \left( \frac{2\pi d\sqrt{-1}}{n} \right) \right)
\]
is the minimum polynomial of the \( n \)-th primitive roots of unity over \( \mathbb{Q} \). It is an irreducible polynomial in \( \mathbb{Z}[x] \) of degree \( \phi(n) \) where \( \phi \) is the Euler totient function. From the trivial relation \( x^n - 1 = \prod_{d|n} \Phi_d(x) \), the well known formula
\[
\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}
\]
is derived by Möbius inversion. Here \( \mu \) is the Möbius function. In [5] [6], it is surmised that \( \Phi_n(x) \) is an increasing function for \( x > 1 \). We start with a simple proof of this fact.

Theorem 1.

\[
\Phi_n^{(j)}(1) > 0
\]
for \( j = 1, \ldots, \phi(n) \). In particular, \( \Phi_n^{(k)}(x) \) is strictly increasing for \( x \geq 1 \) and \( k = 0, 1, \ldots, \phi(n) - 1 \).

Proof. Since \( \Phi_1(x) = x - 1 \) and \( \Phi_2(x) = x + 1 \) are increasing, we may assume that \( n \geq 3 \). Then we have
\[
\Phi_n(x) = \prod_{0 < d < n/2, (d,n) = 1} \left( x - \exp \left( \frac{2\pi d\sqrt{-1}}{n} \right) \right) \left( x - \exp \left( \frac{2\pi (n-d)\sqrt{-1}}{n} \right) \right)
\]
\[
= \prod_{0 < d < n/2, (d,n) = 1} \left( x^2 - 2 \cos \left( \frac{2\pi d}{n} \right) x + 1 \right)
\]
Since all coefficients of
\[
(x + 1)^2 + b(x + 1) + 1 = x^2 + (b + 2)x + b + 2
\]
Key words and phrases. Cyclotomic polynomials, Jordan totient function.
with \( b \in (-2, 2) \) are positive, the expansion \( \Phi_n(x + 1) = \sum_{i=0}^{d} c_i x^i \) at \( x = 0 \) have positive coefficients \( c_i \) for \( i \leq d = \phi(n) \). This proves the theorem. \( \square \)

We give several remarks. First: the inequality \( x \geq 1 \) in Theorem 1 is sharp. If \( p \) is an odd prime, then

\[
\Phi_{2p}(x) = \frac{1 - (-x)^p}{1 + x}.
\]

It is easy to confirm

\[
\Phi'_{2p} \left( 1 - \frac{1}{\sqrt{p}} \right) = \frac{\left( 2p - \sqrt{p} + \frac{1}{\sqrt{p}} - 1 \right) \left( 1 - \frac{1}{\sqrt{p}} \right)^{p-1} - 1}{\left( 2 - \frac{1}{\sqrt{p}} \right)^2} < 0. \tag{3}
\]

Thus there exists no \( \varepsilon > 0 \) that \( \Phi_n(x) \) is increasing on \( [1 - \varepsilon, \infty) \) for any \( n \geq 1 \).

Second: there is an alternative proof only works for \( k = 0 \), giving a starting point of this paper. Since \( \Phi_1(x) = x - 1 \), we may assume that \( n \geq 2 \). From (2), we see

\[
\Phi_n(1) = \prod_{d|n} d^{\mu(n/d)} \geq 1.
\]

This is rewritten as \( \Phi_n(1) = \exp(\Lambda(n)) \) with the von Mangoldt function

\[
\Lambda(n) := \begin{cases} 
\log p & n = p^e \ (p \text{ prime}) \\
1 & \text{otherwise},
\end{cases}
\]

which plays a crucial role in analytic number theory. The fact above was proved by Lebesque [3]. We also have

\[
\log \Phi_n(x) = \sum_{d|n} \mu \left( \frac{n}{d} \right) \log \left( \frac{x^d - 1}{x - 1} \right)
\]

\[
\frac{\Phi_n'(x)}{\Phi_n(x)} = \sum_{d|n} \mu \left( \frac{n}{d} \right) \left( \frac{(d-1)x^{d-2} + (d-2)x^{d-3} + \cdots + 1}{x^{d-1} + x^{d-2} \cdots + 1} \right). \tag{4}
\]

Letting \( x \to 1 \), we obtain

\[
\frac{\Phi_n'(1)}{\Phi_n(1)} = \sum_{d|n} \mu \left( \frac{n}{d} \right) \frac{d - 1}{2} = \frac{1}{2} \sum_{d|n} \mu \left( \frac{n}{d} \right) d = \frac{\phi(n)}{2}
\]

Thus we see that

\[
\Phi_n'(1) = \frac{1}{2} \phi(n) \Phi_n(1) \geq 1 > 0, \tag{5}
\]

which was proved by Hölder [2]. Now we consider \( \Phi_n(z) \) as a polynomial of complex variable \( z \in \mathbb{C} \). Recalling Gauss-Lucas theorem, any root of \( \Phi_n'(z) \) lies in the convex hull of the roots of \( \Phi_n(z) \) in the complex plane. Therefore from (1) and \( n \geq 2 \), the real function \( \Phi_n'(x) \) has no root in \( x \geq 1 \). This implies \( \Phi_n'(x) > 0 \) for \( x \geq 1 \) since \( \Phi_n'(x) \) is continuous.

Third: let \( p \) be an odd prime again. (3) and (5) imply that there exists a real root of \( \Phi_{2p}'(x) \) in the interval \((1 - 1/\sqrt{p}, 1)\).
Proof. Applying Leibniz formula to (4),

\[ J_k(n) = n^k \prod_{p \mid n} \left(1 - \frac{1}{p^k}\right) \]

where \( p \) runs over prime divisors of \( n \). Clearly \( J_k(n) \) is a generalization of the Euler totient function \( \phi(n) = J_1(n) \). The name came from C. Jordan who studied linear groups over \( \mathbb{Z}/n\mathbb{Z} \) and deduced, e.g.,

\[ \text{Card}(GL_k(\mathbb{Z}/n\mathbb{Z})) = n \sum_{j=1}^{k} J_j(n). \]

As we observed in the second remark, the special values \( \Phi_n^{(k)}(1) \) give important arithmetic functions such as von Mangoldt function and Euler totient function. Lehmer [4] gave an explicit formula of \( \Phi_n^{(k)}(1)/\Phi_n(1) \) as a polynomial of \( \phi(n) \) and \( J_{2i}(n) \) over \( \mathbb{Q} \), using Stirling numbers and Bernoulli numbers, see [1] for further developments. Here we give a quick proof of this fact but without its explicit form.

**Theorem 2.** For \( n \geq 2 \), \( \Phi_n^{(\ell)}(1)/\Phi_n(1) \) is expressed as a polynomial of \( \phi(n) \) and \( J_{2i}(n) (1 \leq i \leq (\ell + 1)/2) \) over \( \mathbb{Q} \), and its value is a positive integer \( \Phi_n^{(\ell)}(1)/\Phi_n(1) \) for \( \phi(n) \geq \ell \).

**Proof.** Applying Leibniz formula to [4],

\[ \frac{\Phi_n^{(k)}}{\Phi_n(x)} = \sum_{\ell=0}^{k} \binom{k}{\ell} \frac{\Phi_n^{(\ell)}(x)}{\Phi_n(x)} \sum_{d \mid n} \mu \left(\frac{n}{d}\right) \left(1 - dx^{d-1} + dx^d - x^d\right) \frac{(x-1)(x^d-1)}{(x-1)(x^d-1)}^{(k-\ell)}. \]

Substituting \( x \) by \( 1 + t \), we get the Taylor expansion at \( t = 0 \):

\[ \frac{((d-1)t-1)(t+1)^{d-1} + 1}{t((t+1)^d-1)} = \frac{d-1}{2} + \frac{d^2 - 6d + 5}{12} t + \frac{-d^2 + 4d - 3}{8} t^2 + O(t^3). \]

The \( \ell \)-th Taylor coefficient is a polynomial of \( d \) whose degree does not exceed \( \ell + 1 \). Using these Taylor coefficients, we recursively obtain the explicit formula for \( \Phi_n^{(\ell)}(1)/\Phi_n(1) \). Thus \( \Phi_n^{(\ell)}(1)/\Phi_n(1) \) is a polynomial on \( J_1(n), J_2(n), \ldots, J_{\ell+1}(n) \) over \( \mathbb{Q} \). Moreover since

\[ \frac{((d-1)t-1)(t+1)^{d-1} + 1}{t((t+1)^d-1)} = \frac{d}{2(t+1)} (t+1)^d + 1 \]

is an even function on \( d \), the terms \( d^{2k+1} \) with \( k = 1, 2, \ldots \) do not show, i.e., \( J_{2k+1}(n) (k = 1, 2, \ldots) \) never appear. By Theorem [4] \( \Phi_n^{(\ell)}(1)/\Phi_n(1) > 0 \) for \( \phi(n) \geq \ell \). Since

\[ \Phi_n(1) = \exp(\Lambda(n)) = \begin{cases} p & n = p^e \ (p \text{ prime}) \\ 1 & \text{otherwise}, \end{cases} \]

it suffices to show \( \Phi_n^{(\ell)}(1) \equiv 0 \ (\text{mod} \ p) \). By

\[ \Phi_n^{(\ell)}(x) = \frac{x^{p^\ell} - 1}{x^{p^\ell-1} - 1} = \Phi_p(x^{p^\ell-1}), \]

\[ \Phi_n^{(\ell)}(x) = 0 \text{ for } \phi(n) < \ell. \]
the case $e > 1$ is plain and the case $e = 1$ remains. Indeed we have,

$$
\Phi_p^{(1)}(1) = \frac{\prod_{i=0}^{p-1} i(i-1) \cdots (i-\ell + 1)}{\ell + 1} = \frac{p(p-1) \cdots (p-\ell)}{\ell + 1} \equiv 0 \pmod{p}.
$$

□

For example, we have

**Corollary 1.**

\[
\begin{align*}
\frac{\Phi_n^{(2)}(1)}{\Phi_n(1)} &= \frac{J_2(n)}{12} + \frac{\phi(n)^2}{4} - \frac{\phi(n)}{2}, \\
\frac{\Phi_n^{(3)}(1)}{\Phi_n(1)} &= \frac{(\phi(n) - 2)(J_2(n) + \phi(n)(\phi(n) - 4))}{8}, \\
\frac{\Phi_n^{(4)}(1)}{\Phi_n(1)} &= \frac{1}{240} \left(30J_2(n)\phi(n)^2 - 180J_2(n)\phi(n) + 5J_2(n)^2 + 220J_2(n) - 2J_4(n) + 15\phi(n)^4 - 180\phi(n)^3 + 660\phi(n)^2 - 720\phi(n) \right), \\
\frac{\Phi_n^{(5)}(1)}{\Phi_n(1)(\phi(n) - 4)} &= \frac{1}{96} \left(3\phi(n)^4 - 48\phi(n)^3 + 10J_2(n)\phi(n)^2 + 228\phi(n)^2 - 80J_2(n)\phi(n) - 288\phi(n) + 5J_2(n)^2 + 100J_2(n) - 2J_4(n) \right).
\end{align*}
\]

Let

$$
\Phi_n(x + 1) = \sum_{h=0}^{\phi(n)} c_n(h)x^h \quad \text{with} \quad c_n(h) = \frac{1}{h!}\Phi_n^{(h)}(1) \in \mathbb{Z}.
$$

Lehmer [4] further stated an interesting observation on the coefficients $c_n(h)$. For a real $R$, set $R^{[\ell]} := R(R - 1) \cdots (R - \ell + 1)$. For a positive integer $r$, let $t_r := J_r(n)/(2r)$. We define Bernoulli numbers $B_m$ ($m \geq 0$) by

$$
t_r = \frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.
$$

Under the setting above, he claimed that

$$
c_n(h) = \frac{\phi(n)}{\Phi_n(1)} = t_1^{[h]} + 2 \sum_{\ell=1}^{\infty} B_{2\ell} \left( \frac{h}{2\ell} \right) (t_1 - \ell)^{[h-2\ell]} \Omega_{\ell},
$$

but the general form of $\Omega_{\ell}$ is not given. He only wrote the first few terms:

\[
\begin{align*}
\Omega_1 &= t_2, \\
\Omega_2 &= t_4 - 5t_2^{[2]}, \\
\Omega_3 &= t_6 - 7t_4(t_2 - 1) + \frac{35}{3}t_2^{[3]} + \frac{14}{3}t_2, \\
\Omega_4 &= t_8 - \frac{20}{3}t_6(t_2 - 1) - \frac{7}{3}t_4^{[2]} + \frac{70}{3}t_4(t_2 - 1)^{[2]} \\
&\quad - \frac{175}{9}t_2^{[4]} + \frac{10}{3}t_6 - \frac{280}{9}t_2^{[2]} + \frac{290}{9}t_2.
\end{align*}
\]

Both Corollary [4] and this observation suggest a
The goal of this paper is to prove intimately related divisibility:

\[ \Phi_n^{(2k+1)}(1)/\Phi_n(1) \text{ is divisible by } \phi(n) - 2k \text{ in } \mathbb{Z}, \]

for \( k \geq 1 \), see Theorem[3] and Corollary[2]. (The dividend should be doubled for the case \( k = 1 \).) We did not find yet a special meaning of this divisibility. For a fixed \( n \), such divisibility is confirmed using Theorem[2]. Before closing this section, we give a property of the Jordan totient function, which is used to show this divisibility for a fixed \( n \). This property is not used in the later sections but of independent interest.

Let \( \mathbb{E}(m) \) be the exponent of \( (\mathbb{Z}/m\mathbb{Z})^* \), the unit group of the ring \( \mathbb{Z}/m\mathbb{Z} \). For an odd prime \( p \), \( \mathbb{E}(p^e) = \phi(p^e) \) holds since \( (\mathbb{Z}/p^e\mathbb{Z})^* \) is cyclic. From

\[ (\mathbb{Z}/2^e\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-2}\mathbb{Z} \]

for \( e \geq 2 \), we have

\[ \mathbb{E}(2^e) = \begin{cases} 1 & e = 1 \\ 2 & e = 2 \\ 2^{e-2} & e \geq 3. \end{cases} \]

For a prime \( p \) and a positive integer \( e \), we write \( \mathbb{E}(p^e) \parallel k \) if both \( \mathbb{E}(p^e) \mid k \) and \( \mathbb{E}(p^{e+1}) \nmid k \) hold.

**Proposition 1 (Trivial congruence).** For \( k \geq 3 \), we have

\[ J_k(n) \equiv 0 \pmod{\prod_{\mathbb{E}(p^e)\parallel k} p^e} \]

for \( n \geq k + 2 \). For \( M > \prod_{\mathbb{E}(p^e)\parallel k} p^e \) and any \( n_0 \in \mathbb{N} \), there exists \( n \geq n_0 \) such that \( J_k(n) \not\equiv 0 \pmod{M} \).

**Proof:** Clearly there are only finitely many prime \( p \) such that \( \mathbb{E}(p^e) \mid k \). For a prime factor \( q \) of \( n \), \( q^k - 1 \) is a factor of \( J_k(n) \). The condition \( \mathbb{E}(p^e) \mid k \) implies \( q^k - 1 \equiv 0 \pmod{p^e} \) for all \( q \) which is coprime with \( p \). Assume that

\[ n > \max\{ p : \mathbb{E}(p^e) \mid k \}. \]  

(6)

If \( n \) has two distinct prime factors \( p_1 \) and \( p_2 \), then \( J_k(n) \) is divisible by \((p_1^k - 1)(p_2^k - 1)\). We see \( p_1^k - 1 \) is divisible by \( p_2^e \) with \( p \neq p_i \) if \( \mathbb{E}(p^e) \mid k \). This implies that \((p_1^k - 1)(p_2^k - 1)\) is divisible by \( \prod_{\mathbb{E}(p^e)\parallel k} p^e \). Thus we may assume that \( n \) is a power of a prime \( q \) and \( \mathbb{E}(q^e) \mid k \), i.e., \( n = q^\ell \) and \( \ell \geq 2 \). In this case, \( J_k(n) \) is divisible by \( q^{\ell k} - q^{(\ell-1)k} = q^{(\ell-1)k}(q^k - 1) \). We see

\[ \prod_{\mathbb{E}(p^e)\parallel k} p^e \mid q^k - 1. \]

When \( q \neq 2 \), since \( e \leq \mathbb{E}(q^e) \leq k \), we see \( q^e \) divides \( q^{(\ell-1)k} \) and the required congruence holds. For \( q = 2 \) we only have \( e - 1 \leq \mathbb{E}(2^e) \leq k \) and hence \( e \leq 2k \). So additionally if \( \ell > 2 \), then \( q^e \mid q^{(\ell-1)k} \) holds. Therefore our discussion fails only when \( n = 2^{2k}, \mathbb{E}(2^e) \mid k \) and \( e > k \). This happens when \( 2^{k-1} < k \), that is, \( k \leq 2 \). Summing up if \( k \geq 3 \), (6) implies our congruence. Moreover (6) holds if \( n > k + 1 \), because the worst case happens when \( k + 1 \) is an odd prime.
Take $M > \prod \Xi(p^e)k^e$ and any $n_0 \in \mathbb{N}$. There exists a prime power factor $p^{e+1}$ of $M$ that $\Xi(p^{e+1})$ does not divide $k$. From the definition of the exponent, there exists $t \in \mathbb{N}$ which is coprime to $p$ that $t^k \not\equiv 1 \mod p^{e+1}$. By Dirichlet’s theorem, there exists a prime $q \geq n_0$ that $q \equiv t \mod p^{e+1}$.

Then $J_k(q) = q^k - 1 \not\equiv 0 \mod M$. □

Here is a table of the first several values of Prop 1.

| $k$ | odd | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 |
|-----|-----|---|---|---|---|----|----|----|----|----|----|
| $\prod \Xi(p^e)k^e$ | 2 | 24 | 240 | 480 | 264 | 65520 | 24 | 16320 | 28728 | 13200 |

2. Main results

Throughout this section, let $n$ be an integer greater than 2. In particular, $\phi(n)$ is even. In this section we introduce a new relation for $c_n(h)$. We denote the primitive $n$-th root of one by $\zeta_1, \zeta_2, \ldots, \zeta_{\phi(n)}$. We may assume that $\zeta_{j+\phi(n)/2} = \overline{\zeta_j}$ for $j = 1, \ldots, \phi(n)/2$. Then we have

$$\sum_{h=0}^{\phi(n)} c_n(h)x^h = \prod_{j=1}^{\phi(n)/2} (x + 1 - \zeta_j). \quad (7)$$

Let

$$\prod_{j=1}^{\phi(n)/2} (x + 2 - \zeta_j - \overline{\zeta_j}) =: \sum_{\ell=0}^{\phi(n)/2} a_n(\ell)x^\ell. \quad (8)$$

Our key is a special equality between $c_n(h)$ and $a_n(\ell)$, which does not appear to be reduced to a simple relation of generating functions.

Theorem 3. For any $h$ with $0 \leq h \leq \phi(n)$, we have

$$c_n(h) = \sum_{\ell=\max(0,h-\phi(n)/2)}^{\lfloor h/2 \rfloor} \binom{\phi(n)/2 - \ell}{h - 2\ell} a_n(\ell). \quad (9)$$

Theorem 3 leads to our curious congruences.

Corollary 2. (i) $2\Phi''_n(1)$ is divisible by $\phi(n) - 2$.

(ii) Suppose that $k \geq 2$. Then $\Phi_n(2k+1)(1)$ is divisible by $\phi(n) - 2k$.

Proof. For the proof of (i), we may assume that $\phi(n) \geq 3$. Since $2\Phi_n''(1) = 12c_n(3)$, (i) follows from (9) and

$$12\left(\frac{\phi(n)/2}{3}\right) = (\phi(n) - 2) \cdot \frac{\phi(n)}{2} \cdot \frac{\phi(n) - 4}{2}.$$

For the proof of (ii), we may assume that $\phi(n) \geq 2k + 1$. Then (ii) follows from $\Phi_n(2k+1)(1) = (2k + 1)!c_n(2k + 1)$ and (9). In fact, Set

$$\overline{c(\ell)} := (2k + 1)!\left(\frac{\phi(n)/2 - \ell}{2k + 1 - 2\ell}\right).$$
Note that \((\phi(n) - 4k + 2)/2 \cdot (\phi(n) - 4k)/2\) is even. If \(\ell = 0\), then we see by \(k \geq 2\) that
\[
\overline{c(0)} = \frac{\phi(n)}{2} \cdot \frac{\phi(n) - 2}{2} \cdot \frac{\phi(n) - 2k}{2} \cdots \frac{\phi(n) - 4k + 2}{2} \cdot \frac{\phi(n) - 4k}{2}
\]
is divisible by \(\phi(n) - 2k\). Moreover, if \(1 \leq \ell \leq k\), then
\[
\overline{c(\ell)} = \frac{(2k + 1)!}{(2k + 1 - 2\ell)!} \cdot \frac{\phi(n) - 2\ell}{2} \cdot \frac{\phi(n) - 2k}{2} \cdots \frac{\phi(n) - 4k + 2\ell}{2}
\]
is divisible by \(\phi(n) - 2k\) because \((2k + 1)!/(2k + 1 - 2\ell)!\) is even. \(\Box\)

3. Proof of Theorem 3

3.1. Preliminaries. Let \(n\) be an integer greater than 2. We use the same notation as Section 2. Set
\[
S := \{1, 2, \ldots, \phi(n)\}, \quad T := \{1, 2, \ldots, \phi(n)/2\}.
\]
For any \(I \subseteq S\), put
\[
f(I) := \prod_{j \in S \setminus I} (1 - \zeta_j).
\]
From (7), we have
\[
c_n(h) = \sum_{I \subseteq S \atop |I| = h} f(I), \quad (10)
\]
where \(|I|\) denotes the cardinality of \(I\). Similarly, for any \(A \subseteq T\), we set
\[
g(A) := \prod_{j \in T \setminus A} (2 - \zeta_j - \overline{\zeta_j}).
\]
Then (8) implies that
\[
a_n(\ell) = \sum_{A \subseteq T \atop |A| = \ell} g(A). \quad (11)
\]
The main idea in the proof of Theorem 3 is to find many same valued subsums in (10), by using the relation
\[
(x + 1 - \zeta_j)(x + 1 - \overline{\zeta_j}) = x^2 + (2 - \zeta_j - \overline{\zeta_j})x + (1 - \zeta_j)(1 - \overline{\zeta_j})
\]
\[
= x^2 + (2 - \zeta_j - \overline{\zeta_j})x + (2 - \zeta_j - \overline{\zeta_j}).
\]
See Lemma 1 for details. For any \(I \subseteq S\), let
\[
m(I) := \bigcup \left\{ j, j + \frac{\phi(n)}{2} \bigg| 1 \leq j \leq \frac{\phi(n)}{2}, \ j \in I \text{ and } j + \frac{\phi(n)}{2} \in I \right\},
\]
\[
s(I) := \bigcup \left\{ j, j + \frac{\phi(n)}{2} \bigg| 1 \leq j \leq \frac{\phi(n)}{2}, \ j \in I \text{ or } j + \frac{\phi(n)}{2} \in I \right\}
\]
It is easily seen that \(m(I) \subseteq s(I)\). Note that \(m(\emptyset) = \emptyset\) and \(s(\emptyset) = \emptyset\).

Example 1. Consider the case where \(n = 16\). Note that \(\phi(16) = 8\). Let \(I := \{1, 5, 2\}\). Then we have \(m(I) = \{1, 5\}\) and \(s(I) = \{1, 5, 2, 6\}\).
Lemma 1. Let $I_0$ be a subset of $S$. Then we have
\[
\sum_{\substack{I \subset S \ni \phi \ni (1, \ldots, n) \ni \bigcup \{1, \ldots, n\} \ni m(I) = m(I_0) \ni s(I) = s(I_0)}} f(I) = f(m(I_0)). \tag{12}
\]

We denote the left-hand side of (12) by $F(I_0)$.

Remark 1. Let $I_0$ be a fixed subset of $S$. If $I \subset S$ satisfies $m(I) = m(I_0)$ and $s(I) = s(I_0)$, then $|I| = |I_0|$.

Example 2. Before proving Lemma 4, we give an example of (12). Key idea is the equality
\[
(1 - \zeta_j)(1 - \zeta_j) = (1 - \zeta_j) + (1 - \zeta_j)
\]
for any $j \in S$. We consider the case where $n = 16$ and $I_0 = \{1, 5, 2\}$ (see also Example 7). We list $I \subset S$ satisfying $m(I) = m(I_0) = \{1, 5\}$ and $s(I) = s(I_0) = \{1, 5, 2, 6\}$ as follows: $I = \{1, 5, 2\}, \{1, 5, 6\}$. Thus, we see
\[
F(I_0) = (1 - \zeta_6)(1 - \zeta_6)(1 - \zeta_7)(1 - \zeta_7)(1 - \zeta_6)(1 - \zeta_6)
+ (1 - \zeta_2)(1 - \zeta_4)(1 - \zeta_4)(1 - \zeta_4)(1 - \zeta_4)
= (1 - \zeta_2)f(s(I_0)) + (1 - \zeta_2)f(s(I_0))
= (1 - \zeta_2)(1 - \zeta_2)f(s(I_0)) = f(m(I_0)).
\]

Proof of Lemma 7. We use induction on $|s(I_0) \ni m(I_0)|$. First, consider the case of $s(I_0) = m(I_0)$. Then we see $s(I_0) = m(I_0) = I_0$, and so
\[
F(I_0) = f(I_0) = f(m(I_0)),
\]
which implies (12). Next, we suppose that $|s(I_0) \ni m(I_0)| > 0$. Without loss of generality, we may assume that $1 + \phi(n)/2 \in s(I_0) \ni m(I_0)$. Put $I_0 := I_0 \cup \{1 + \phi(n)/2\}$. Note that $m(I_0) = m(I_0) \cup \{1, 1 + \phi(n)/2\}$ and $s(I_0) = s(I_0)$. We take $I \subset S$ with $m(I) = m(I_0)$ and $s(I) = s(I_0)$. Set $\tilde{I} := I \cup \{1, 1 + \phi(n)/2\}$. Note that $1 \in I$ or $1 + \phi(n)/2 \in \tilde{I}$. We get
\[
f(I) = \begin{cases} 
(1 - \zeta_1)f(\tilde{I}) & \text{if } 1 \in I, \\
(1 - \zeta_1)f(\tilde{I}) & \text{if } 1 + \phi(n)/2 \in \tilde{I}.
\end{cases}
\]
Moreover, observe that $m(\tilde{I}) = m(I_0)$, $s(\tilde{I}) = s(I_0)$. Hence, we obtain
\[
F(I_0) = (1 - \zeta_1) \sum_{\substack{\tilde{I} \subset S \ni \phi \ni (1, \ldots, n) \ni (1 + \phi(n))/2 \ni m(\tilde{I}) = m(I_0) \ni s(\tilde{I}) = s(I_0)}} f(\tilde{I}) + (1 - \zeta_1) \sum_{\substack{\tilde{I} \subset S \ni \phi \ni (1, \ldots, n) \ni (1 + \phi(n))/2 \ni m(\tilde{I}) = m(I_0) \ni s(\tilde{I}) = s(I_0)}} f(\tilde{I})
= (1 - \zeta_1)F(I_0) + (1 - \zeta_1)F(I_0).
\]
Since $|s(I_0) \ni m(I_0)| = |s(I) \ni m(I)| - 2$, the inductive hypothesis implies that
\[
F(I_0) = (1 - \zeta_1)f(m(I_0)) + (1 - \zeta_1)f(m(I_0))
= (1 - \zeta_1)(1 - \zeta_1)f(m(I_0)) = f(m(I_0)),
\]
which implies (12).
3.2. Completion of the proof. In what follows, we apply Lemma 1 to (10). We now introduce some definition. Recall that \( S = \{1,2,\ldots,\phi(n)\} \) and \( T = \{1,2,\ldots,\phi(n)/2\} \).

**Definition 1.** Let \( J \subset S \).

- \( J \) is called full if \( J = \{x \mid x \in J\} \).
- \( \pi(J) := J \cap T \).

**Remark 2.** If \( J \subset S \) is full, then we have

\[
f(J) = \prod_{j \in S \setminus J} (1 - \zeta_j) = \prod_{j \in T \setminus \pi(J)} (1 - \zeta_j)(1 - \overline{\zeta_j}) = g(\pi(J)).
\]

**Definition 2.** Let \( h \) be an integer with \( 0 \leq h \leq \phi(n) \).

- For \( J \subset S \), we write \( h \ni J \) if there exists \( I_0 \subset S \) such that \( |I_0| = h \) and \( m(I_0) = J \).
- Suppose that \( h \ni J \) and \( J' \subset S \). We write \( h \ni (J,J') \) if there exists \( I_0 \subset S \) such that \( |I_0| = h \), \( m(I_0) = J \), and \( s(I_0) = J' \).

**Lemma 2.** Let \( h \) be an integer with \( 0 \leq h \leq \phi(n) \).

(i) Let \( J \subset S \). Then \( h \ni J \) if and only if \( J \) is full and

\[
2h - \phi(n) \leq |J| \leq h.
\]

(ii) Suppose that \( h \ni J \), \( |J| = 2\ell \) and \( J' \subset S \). Then \( h \ni (J,J') \) if and only if \( J' \) is full, \( J \subset J' \), and \( |\pi(J' - J)| = h - 2\ell \). In particular, the number of \( J' \) with \( h \ni (J,J') \) is

\[
\left( \frac{\phi(n)/2 - \ell}{h - 2\ell} \right).
\]

**Proof.** Let us show (i). It is clear that if \( h \ni J \), then \( J \) is full. When \( J \) is full, we derive a necessary and sufficient condition for \( h \ni J \) in terms of \( |J| \). Suppose that \( h \ni J \). There exists \( I_0 \subset S \) such that \( m(I_0) = J \) and \( h = |I_0| \). Let \( 2\ell := |m(I_0)| \) and \( a := |I_0\setminus m(I_0)| \). Then we have \( 2\ell \leq h \) and \( h = 2\ell + a \). Moreover, since

\[
|\pi(s(I_0))| = \ell + a \leq \frac{\phi(n)}{2},
\]

we get

\[
h \leq \ell + \frac{\phi(n)}{2},
\]

which implies (14). Conversely, if (13) holds for a full \( J \), then putting \( 2\ell := |J| \), \( a := h - 2\ell \), we have \( 0 \leq a \leq \phi(n)/2 - \ell \). Thus we can find an \( I_0 \subset S \) with \( m(I_0) = J \) and \( |I_0| = h \), i.e. \( h \ni J \).

Next we prove (ii). It is obvious that if \( h \ni (J,J') \), then \( J' \) is full and \( J \subset J' \). When \( J' \) is full and \( J \subset J' \), we deduce a necessary and sufficient condition for \( h \ni (J,J') \) in terms of \( |J'| \). Suppose that \( h \ni (J,J') \). There exists \( I_0 \subset S \) such that \( |I_0| = h \), \( m(I_0) = J \), and \( s(I_0) = J' \). Putting again \( a := |I_0\setminus m(I_0)| \), we see \( |\pi(J' - J)| = a = h - 2\ell \). Conversely, if \( a := |\pi(J' - J)| = h - 2\ell \), then \( h \ni (J,J') \) is similarly shown. Since we choose \( a \) elements in \( T \setminus \pi(J) \) of cardinality \( \phi(n)/2 - \ell \), the latter part of (ii) immediately follows. \( \square \)

**Remark 3.** Let \( 0 \leq h \leq \phi(n) \). Let \( J \subset S \) with \( h \ni J \). Let \( J' \subset S \) with \( h \ni (J,J') \). Then Remark 4 implies that if \( I \subset S \) satisfies \( m(I) = J \) and \( s(I) = J' \), then \( |I| = h \).
Let $h$ be an integer with $0 \leq h \leq \phi(n)$. Applying (10) and Lemma 1, we obtain
\[
c_n(h) = \sum_{I \subseteq S, |I| = h} f(I) = \sum_{J \subseteq S, h \gg J \gg (J,J')} \sum_{J' \subseteq S, h \gg J} f(J) \sum_{J' \subseteq S, h \gg (J,J')} f(J) \sum_{J' \subseteq S, h \gg (J,J')} 1.
\]
Lemma 2 (i) implies that
\[
c_n(h) = \sum_{\ell = \max\{0, h - \phi(n)/2\}}^{[h/2]} \sum_{J \subseteq S, J: \text{full}, |J| = 2\ell} f(J) \sum_{J' \subseteq S, h \gg (J,J')} 1.
\]
Hence, Lemma 2 (ii) implies that
\[
c_n(h) = \sum_{\ell = \max\{0, h - \phi(n)/2\}}^{[h/2]} \left( \frac{\phi(n)/2 - \ell}{h - 2\ell} \right) \sum_{J \subseteq S, J: \text{full}, |J| = 2\ell} g(A).
\]
Using Remark 2 and (11), we deduce that
\[
c_n(h) = \sum_{\ell = \max\{0, h - \phi(n)/2\}}^{[h/2]} \left( \frac{\phi(n)/2 - \ell}{h - 2\ell} \right) a_n(\ell),
\]
which completes the proof of Theorem 3.

REFERENCES
[1] A. Herrera-Poyatos, P. Moree, Coefficients and higher order derivatives of cyclotomic polynomials: Old and new. Expo. Math. 39 (2021), no. 3, 309–343.
[2] O. Hölder, Zur theorie der Kreisteilungsgleichung $k_m(x) = 0$, Prace Mat. Fiz 43 (1936), 13–23.
[3] V. A. Lebesque, Dimostrazione Dell’irreduuttibilità Dell’equazione formata con le radici primitive dell’unità, Ann. Mat. 2 (1859), 232–237.
[4] D. H. Lehmer, Some properties of the cyclotomic polynomial. J. Math. Anal. Appl. 15 (1966), 105–117.
[5] K. Motose, Ramanujan’s sums and cyclotomic polynomials. Math. J. Okayama Univ. 47 (2005), 65–74.
[6] K. Motose, On values of cyclotomic polynomials. VII. Bull. Fac. Sci. Technol. Hirosaki Univ. 7 (2004), no. 1, 1–8.