Values of coefficients of cyclotomic polynomials II

Chun-Gang Ji, Wei-Ping Li and Pieter Moree

Abstract

Let $a(n,k)$ be the $k$th coefficient of the $n$th cyclotomic polynomial. In part I it was proved that $\{a(mn,k) \mid n \geq 1, \ k \geq 0\} = \mathbb{Z}$, in case $m$ is a prime power. In this paper we show that the result also holds true in case $m$ is an arbitrary positive integer.

1 Introduction

Let $\Phi_n(x) = \sum_{k=0}^{\phi(n)} a(n,k)x^k$ be the $n$th cyclotomic polynomial. The rational function $1/\Phi_n(x)$ has a Taylor series around $x = 0$ given by

$$\frac{1}{\Phi_n(x)} = \sum_{k=0}^{\infty} c(n,k)x^k,$$

where it can be shown that the $c(n,k)$ are also integers. It turns out that usually the coefficients $a(n,k)$ and $c(n,k)$ are quite small in absolute value, for example for $n < 10^5$ it is well-known that $|a(n,k)| \leq 1$ and for $n < 561$ we have $|c(n,k)| \leq 1$ (by [3, Lemma 12]).

The purpose of this note is to show that although so often the coefficients $a(n,k)$ and $c(n,k)$ are small, they assume every integer value, even when we require $n$ to be a multiple of an arbitrary natural number $m$.

Theorem 1 Let $m \geq 1$ be an integer. Put $S(m) = \{a(mn,k) \mid n \geq 1, \ k \geq 0\}$ and $R(m) = \{c(mn,k) \mid n \geq 1, \ k \geq 0\}$. Then $S(m) = \mathbb{Z}$ and $R(m) = \mathbb{Z}$.

Schur proved in 1931 (in a letter to E. Landau) that $S(1)$ is not a finite set. In 1987 Suzuki [4] proved that $S(1) = \mathbb{Z}$. Recently the first two authors [2] proved that $S(p^e) = \mathbb{Z}$ with $p^e$ a prime power.

The fact that every integer already occurs as a coefficient of $\Phi_{pqr}(x)$ with $p, q$ and $r$ odd primes is implicit in Bachman [1]. The third author established this result for the reciprocal cyclotomic polynomials $1/\Phi_{pqr}(x)$, see Moree [3]. This result implies that $R(1) = \mathbb{Z}$.

Mathematics Subject Classification (2000). 11B83, 11C08

The first author is partially supported by the Grant No.10771103 from NNSF of China.
2 Some lemmas

Since
\[ x^n - 1 = \prod_{d \mid n} \Phi_d(x), \quad (1) \]
we have by the Möbius inversion formula, \( \Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(\frac{n}{d})} \), where \( \mu \) denotes the Möbius function.

On using that \( \sum_{d \mid n} \mu(d) = 0 \) if \( n > 1 \), it is seen that, for \( n > 1 \),
\[ \Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(\frac{n}{d})} = \prod_{d \mid n} (1 - x^d)^{\mu(\frac{n}{d})} = \prod_{d \mid n} (1 - x^d)^{\mu(\frac{n}{d})}. \]
(Thus for \( n > 1 \), the polynomial \( \Phi_n(x) \) is self-reciprocal.)

**Lemma 1** The coefficient \( c(n, k) \) is an integer whose values only depends on the congruence class of \( k \) modulo \( n \).

**Proof.** Let us first consider \( \Psi_n(x) := x^n - 1/\Phi_n(x) \).

By (1) we have that \( \Psi_n(x) = \prod_{d<n, d \mid n} \Phi_d(x) \) and thus its coefficients are integers. The degree of \( \Psi_n(x) \) is \( n - \varphi(n) \), with \( \varphi \) Euler’s totient function. We infer that, for \( |x| < 1 \),
\[ \frac{1}{\Phi_n(x)} = -\Psi_n(x)(1 + x^n + x^{2n} + \cdots) \]
Since \( n > n - \varphi(n) \), the proof is completed. \( \square \)

Let \( \kappa(m) = \prod_{p \mid m} p \) denote the squarefree kernel of \( m \), that is the largest squarefree divisor of \( m \).

**Lemma 2** Let \( p \) be a prime. For \( l, m \geq 1 \) we have \( S(p^lm) = S(pm) \) and \( R(p^lm) = R(pm) \).

**Corollary 1** We have \( S(m) = S(\kappa(m)) \) and \( R(m) = R(\kappa(m)) \).

**Proof of Lemma 2** It is easy to prove, see e.g. Thangadurai [5], that if \( p \) is prime and \( p \mid n \), then
\[ \Phi_{pn}(x) = \Phi_n(x^p). \quad (2) \]
Using this we deduce that \( \Phi_{p^2m}(x) = \Phi_{pm}(x^p) \) and thus \( a(pm, 1) = 0 \) and hence \( 0 \in S(pm) \). On repeatedly applying (2) we can easily infer that \( \Phi_{p^lmn}(x) = \Phi_{pmn}(x^{pl^{-1}}) \) for any \( l \geq 1 \), so
\[ a(p^lmn, k) = \begin{cases} a(pm, k) & \text{if } pl^{-1} \mid k; \\ 0 & \text{otherwise.} \end{cases} \]
This together with \( 0 \in S(pm) \) and the trivial inclusion \( S(p^lm) \subseteq S(pm) \) shows that \( S(p^lm) = S(pm) \).

The proof that \( R(p^lm) = R(pm) \) is completely analogous. Here we use that if \( p \mid n \), then \( \Psi_{pn}(x) = \Psi_n(x^p) \), which is immediate from (2) and the definition of \( \Psi_n(x) \). \( \square \)
Lemma 3 (Quantitative form of Dirichlet’s theorem.) Let \( a \) and \( m \) be coprime natural numbers and let \( \pi(x; m, a) \) denote the number of primes \( p \leq x \) that satisfy \( p \equiv a(\mod m) \). Then, as \( x \) tends to infinity,

\[
\pi(x; m, a) \sim \frac{x}{\varphi(m) \log x}.
\]

Corollary 2 Given \( m, t \geq 1 \) and any real number \( r > 1 \), there exists a constant \( N_0(t, m, r) \) such that for every \( n > N_0(t, m, r) \) the interval \((n, rn)\) contains at least \( t \) primes \( p \equiv 1(\mod m) \).

3 The proof of Theorem 1

We first prove that \( S(m) = \mathbb{Z} \). Since \( S(m) = S(\kappa(m)) \), we may assume that \( m \) is squarefree. We may also assume that \( m > 1 \). Suppose that \( n > N_0(t, m, \frac{15}{8}) \).

Then there exist primes \( p_1, p_2, \ldots, p_t \) such that

\[
n < p_1 < p_2 < \ldots < p_t < \frac{15}{8}n \quad \text{and} \quad p_j \equiv 1(\mod m), \quad j = 1, 2, \ldots, t.
\]

Hence \( p_t < 2p_1 \).

Let \( q \) be any prime exceeding \( 2p_1 \) and put

\[
m_1 = \begin{cases} p_1p_2\cdots p_tq & \text{if } t \text{ is even;} \\ p_1p_2\cdots p_t & \text{otherwise.} \end{cases}
\]

Note that \( m \) and \( m_1 \) are coprime and that \( \mu(m_1) = -1 \). Using these observations we conclude that

\[
\Phi_{m_1,m}(x) \equiv \prod_{d|m_1m, \; d<2p_1} (1 - x^d)^{\mu(m_1m/d)} \quad (\mod x^{2p_1})
\]

\[
\equiv \prod_{d|m} (1 - x^d)^{\mu(m_1)\mu(m_1m)} \prod_{j=1}^t (1 - x^{p_j})^{-\mu(m_1m/p_j)} \quad (\mod x^{2p_1})
\]

\[
\equiv \Phi_m(x)^{\mu(m_1)} \prod_{j=1}^t (1 - x^{p_j})^{-\mu(m_1m)} \quad (\mod x^{2p_1}).
\]

\[
\equiv \frac{1}{\Phi_m(x)} \prod_{j=1}^t (1 - x^{p_j})^{\mu(m)} \quad (\mod x^{2p_1}).
\]

\[
\equiv \frac{1}{\Phi_m(x)} \left(1 - \mu(m)(x^{p_1} + \ldots + x^{p_t})\right) \quad (\mod x^{2p_1}). \tag{3}
\]

From (3) it follows that, if \( p_t \leq k < 2p_1 \),

\[
a(m_1m, k) = c(m, k) - \mu(m) \sum_{j=1}^t c(m, k - p_j).
\]

By Lemma 1 we have \( c(m, k - p_j) = c(m, k - 1) \). Thus we find that

\[
a(m_1m, k) = c(m, k) - \mu(m) tc(m, k - 1) \quad \text{with } p_t \leq k < 2p_1. \tag{4}
\]
We consider two cases ($\mu(m) = 1$, respectively $\mu(m) = -1$).

**Case 1.** $\mu(m) = 1$. In this case $m$ has at least two prime divisors. Let $q_1 < q_2$ be the smallest two prime divisors of $m$. Here we also require that $n \geq 8q_2$. This ensures that $p_t + q_2 < 2p_1$. Note that

$$
\frac{1}{\Phi_m(x)} \equiv \frac{(1 - x^{q_1})(1 - x^{q_2})}{1 - x} \mod x^{q_2 + 2}
$$

$$
\equiv 1 + x + x^2 + \ldots + x^{q_1 - 1} - x^{q_2} - x^{q_2 + 1} \mod x^{q_2 + 2}.
$$

Thus $c(m, k) = 1$ if $k \equiv \beta \mod m$ with $\beta \in \{1, 2\}$ and $c(m, k) = -1$ if $k \equiv \beta \mod m$ with $\beta \in \{q_2, q_2 + 1\}$. This in combination with (4) shows that $a(m_1m, p_t + 1) = 1 - t$ and $a(m_1m, p_t + q_2) = t - 1$. Since $\{1 - t, t - 1 \mid t \geq 1\} = \mathbb{Z}$, the result follows in this case.

**Case 2.** $\mu(m) = -1$. Here we notice that

$$
\frac{1}{\Phi_m(x)} \equiv \begin{cases} 
1 - x \mod x^3 & \text{if } 2 \nmid m; \\
1 - x + x^2 \mod x^3 & \text{otherwise.}
\end{cases}
$$

Using this we find that $a(m_1m, p_t) = -1 + t$. Furthermore, $a(m_1m, p_t + 1) = -t$ in case $m$ is odd and $a(m_1m, p_t + 1) = 1 - t$ otherwise. Since $\{-1 + t, -t \mid t \geq 1\} = \mathbb{Z}$ and $\{-1 + t, 1 - t \mid t \geq 1\} = \mathbb{Z}$, it follows that also $S(m) = \mathbb{Z}$ in this case.

It remains to show that $R(m) = \mathbb{Z}$. As before we may assume that $m$ is squarefree (by Corollary 1) and that $m > 1$ (by Theorem 8 of Moree [3]).

Let $q$ be any prime exceeding $2p_1$ and put

$$
\overline{m_1} = \begin{cases} 
(p_1p_2 \cdots p_t & \text{if } t \text{ is even}; \\
p_1p_2 \cdots p_tq & \text{otherwise.}
\end{cases}
$$

Note that $\mu(\overline{m_1}) = 1$. Reasoning as in the derivation of (3) we obtain

$$
\frac{1}{\Phi_{\overline{m_1}m}(x)} \equiv \frac{1}{\Phi_m(x)} \left(1 - \mu(m)(x^{p_1} + \ldots + x^{p_t})\right) \mod x^{2p_1}
$$

and from this $c(\overline{m_1}m, k) = a(m_1m, k)$ for $k < 2p_1$. Reasoning as in the proof of $S(m) = \mathbb{Z}$, the proof is then completed.

**Remark 1.** If one specializes the above proof to the case $m = p^k$, a proof a little easier than that given in part I [2] is obtained, since it does not involve a case distinction between $m$ is odd and $m$ is even as made in part I. This is a consequence of working modulo $x^{2p_1}$, rather than modulo $x^{2p_1 + 1}$.

**Remark 2.** The fraction 15/8 in the proof can be replaced by $2 - \epsilon$, with $0 < \epsilon < 1$ arbitrary. One then requires that $n > N_0(t, m, 2 - \epsilon)$ and in case $\mu(m) = 1$ in addition that $n \geq q_2/\epsilon$. 

\[ \Box \]
References

[1] Gennady Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, *Proc. Amer. Math. Soc.* **132** (2004), 1943–1950.

[2] Chun-Gang Ji and Wei-Ping Li, Values of coefficients of cyclotomic polynomials, to appear in Discrete Mathematics.

[3] Pieter Moree, Reciprocal cyclotomic polynomials, [arXiv:0709.1570](http://arxiv.org/abs/0709.1570), submitted for publication.

[4] Jiro Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* **63** (1987), 279–280.

[5] Ravindranathan Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), 311–322, Bhaskaracharya Pratishtana, Pune, 2000.

Department of Mathematics,
Nanjing Normal University
Nanjing 210097, P.R. China
e-mail: cgji@njnu.edu.cn

Rugao Normal College,
Rugao 226500, Jiangsu, P.R. China
e-mail: lwpeace@sina.com

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany.
e-mail: moree@mpim-bonn.mpg.de