On the Cyclotomic Polynomials with +1 or −1 Coefficients

by

Shabnam Akhtari
B.Sc., Sharif University of Technology, 2002.

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
July 2004

APPROVAL

Name: Shabnam Akhtari

Degree: Master of Science

Title of Thesis: On the Cyclotomic Polynomials with +1 or −1 Coefficients

Examining Committee: Ralf Wittenberg
Chair

Dr. S. Choi
Senior Supervisor

Dr. P. Borwein
Supervisory Committee

Dr. J. Jedwab
Supervisory Committee

Dr. F. Littmann
Internal Examiner

Date of Defense: July 7th, 2004

Abstract

In this thesis, we study the cyclotomic polynomials of degree $N-1$ with coefficients restricted to the set $\{+1,-1\}$. By a cyclotomic polynomial we mean any monic polynomial with integer coefficients and all roots of modulus 1.

By a careful analysis of the effect of Graeffe's root squaring algorithm on cyclotomic polynomials, P. Borwein and K.K. Choi give a complete characterization of all cyclotomic polynomials with odd coefficients. They also prove that a polynomial $p(x)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if

$$p(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\ldots\Phi_{p_r}(\pm x^{p_1p_2\cdots p_{r-1}}),$$

where $N = p_1p_2\ldots p_r$ and the p_i are primes, not necessarily distinct. Here $\Phi_p(x) := \frac{x^p-1}{x-1}$ is the pth cyclotomic polynomial. Based on substantial computation, they also conjecture that this characterization also holds for polynomials of odd degree with ± 1 coefficients.

We consider the conjecture for odd degree here. Using Ramanujan's sums, we solve the problem for some special cases. We prove that the conjecture is true for polynomials of degree 2^tp^r-1 with odd prime p or separable polynomials of any odd degree. We also give a simpler proof of Borwein and Choi's result.

Acknowledgments

I am very much grateful to Dr. Stephen Kwok-Kwong Choi for his great supervising, support and kindness.

A constant source of appreciation and respect is my family: My Dad, whose memory is still encouraging, my very suffering mom, my caring husband and my lovely sisters.

Contents

Chapter 1

Introduction and Preliminaries

1.1 Introduction

We are interested in studying polynomials with coefficients restricted to the set $\{+1, -1\}$. This particular set of polynomials has drawn much attention and there are a number of difficult old questions concerning it. Littlewood raised a number of these questions and so we call these polynomials **Littlewood polynomials**. A Littlewood polynomial of degree n has L_2 norm on the unit circle equal to $\sqrt{n+1}$. Many of the questions raised concern comparing the behavior of these polynomials in other norms to the L_2 norm. One of the older and more intriguing of these asks whether such polynomials can be "flat". Specifically, do there exist two positive constants C_1 and C_2 so that for each n there is Littlewood polynomial of degree n with

$$C_1\sqrt{n+1} < |p(z)| < C_2\sqrt{n+1}$$

for each z of modulus 1.

The size of the L_p norm of Littlewood polynomials has been studied from a number of points of view. The problem of minimizing the L_4 norm has also attracted a lot of attention.

Mahler raised the question of maximizing the Mahler measure of Littlewood polynomials. The Mahler measure is just the L_0 norm on the circle and one would expect this to be closely related to the minimizing problem for the L_4 norm above.

In [2] P. Borwein and K.K. Choi address the question of characterizing the cyclotomic Littlewood polynomials of even degree. By a cyclotomic polynomial we mean any monic polynomial with integer coefficients and all roots of modulus 1. They show in [2] that a polynomial $P(x)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\ldots\Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \dots p_r$ and the p_i are primes, not necessarily distinct. Here $\Phi_p(x) := \frac{x^p-1}{x-1}$ is the pth cyclotomic polynomial. They also give an explicit formula for the number of such polynomials. Their analysis in [2] is based on a careful treatment of Graeffe's root squaring algorithm. It transpires that all cyclotomic Littlewood polynomials of fixed degree have the same fixed point on iterating Graeffe's root squaring algorithm. This gives a characterization of all cyclotomic polynomials with odd coefficients. After substantial computations, P. Borwein and K.K. Choi conjecture that the above characterization of Littlewood cyclotomic polynomials of even degree also holds for odd degree.

In this thesis, we will give a simpler proof for P. Borwein and K.K. Choi's result which is based on properties of Ramanujan's sum. We will also prove that their conjecture holds for some special cases. We prove that the conjecture is true for polynomials of degree $2^t p^r - 1$ with odd prime p or separable polynomials of any odd degree.

This thesis is organized as follows. In chapter 1, we recall some basic and elementary results in number theory which will be used in later chapters. In chapter 2, we present P. Borwein and K.K. Choi's work on cyclotomic polynomials with odd coefficients and their result on characterization of cyclotomic polynomials of even degree with ±1 coefficients. In chapter 3, we first give a new and simpler proof for the result mentioned in chapter 2. Then we discuss the conjecture for odd degree case and prove our result on characterization of cyclotomic polynomials of some special odd degree with ±1 coefficients.

1.2 Polynomials and Newton's Identity

The main object to be studied in this thesis is the polynomials of one variable over the complex numbers. The most basic and important theorem concerning polynomials is the Fundamental Theorem of Algebra. This tells us that every polynomial can be factored completely over the complex numbers.

Theorem 1.2.1 (Fundamental Theorem of Algebra). *If*

$$P(x) = \sum_{i=0}^{n} a_i x^i, \ a_i \in \mathbb{C}, \ a_n \neq 0,$$

then there exist $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}$ such that

$$P(x) = a_n \prod_{i=1}^{n} (x - \alpha_i).$$

The complex numbers $\alpha_1, \cdots, \alpha_n$ are called the zeros (or roots) of $P(x)$ so that $P(\alpha_i) = 0$. The multiplicity of the zero at α_i is the number of times it repeats. So, for example,

$$(x-1)^3 (x+i)^2$$

is a polynomial of degree 5 with a zero of multiplicity 3 at 1 and with a zero of multiplicity 2 at $-i$.

The polynomial

$$P(x) = \sum_{i=0}^{n} a_i x^i, \; a_i \in \mathbb{C}, \; a_n \neq 0$$

is called **monic** if its **leading coefficient**, a_n, equals 1.

Let S_k be the sum of the kth power of all zeros of $P(x)$. Newton's identity below gives the relation between the coefficients and S_k.

Theorem 1.2.2 (Newton's Identity). *Let*

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots + (-1)^n c_n.$$

For non-negative integer k, let

$$S_k := \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k.$$

We have

$$S_k = (-1)^{k+1}kc_k + (-1)^{k+1}\sum_{j=1}^{k-1}(-1)^j c_{k-j}S_j, \tag{1.2.1}$$

for $k \leq n$ and

$$S_k = (-1)^{k+1}\sum_{j=k-n}^{k-1}(-1)^j c_{k-j}S_j, \tag{1.2.2}$$

for $k > n$. Here an empty sum is understood to be 0.

Proof. A standard proof of this classical result can be found in many textbooks, e.g. [6]. So we omit the proof here. ■

1.3 Möbius and Euler Totient Functions

Let n be a positive integer having prime divisors $p_1, \cdots, p_k$. The Möbius function, $\mu(n)$, is defined by

$$\mu(n) := \begin{cases} 0 & \text{if } p_i^2 \mid n \text{ for some } i; \\ (-1)^k & \text{otherwise.} \end{cases} \tag{1.3.1}$$

In other words, $\mu(n)$ is non-zero only when n is square-free and if $n = p_1 \cdots p_k$ for distinct primes p_j then $\mu(n) = (-1)^k$.

Proposition 1.3.1. *The Möbius function satisfies the following identity*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{otherwise,} \end{cases}$$

where $\sum_{d|n}$ *denotes the summation over all divisors, d, of n.*

Proof. The result is clear if $n = 1$. For $n > 1$, let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the unique factorization of n as a product of distinct prime powers. Let $N = p_1 \cdots p_k$. Then

$$\sum_{d|n} \mu(d) = \sum_{d|N} \mu(d),$$

since the Möbius function vanishes on the non-square-free numbers. Any divisor of N corresponds to a subset of $\{p_1, \cdots, p_k\}$. Thus, for $n > 1$,

$$\sum_{d|n} \mu(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = (1-1)^k = 0.$$

□

An **arithmetic function** f is a complex-valued function defined on the natural numbers.

One of the most important results about the Möbius function is the celebrated Möbius inversion formula.

Theorem 1.3.2 (Möbius Inversion Formula). *Let $f(n)$ and $g(n)$ be arithmetic functions. Then, we have*

(i)

$$f(n) = \sum_{d|n} g(d)$$

if and only if

$$g(n) = \sum_{d|n} \mu(d) f(n/d).$$

(ii)

$$f(n) = \prod_{d|n} g(d)$$

if and only if

$$g(n) = \prod_{d|n} f(n/d)^{\mu(d)}.$$

Proof. Suppose

$$f(n) = \sum_{d|n} g(d).$$

We have

$$\begin{aligned}
\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} g(e) \\
&= \sum_{des=n} \mu(d) g(e) \\
&= \sum_{e|n} g(e) \sum_{d|\frac{n}{e}} \mu(d) \\
&= g(n)
\end{aligned}$$

since the last inner summation is zero unless $n/e = 1$ by Proposition 1.3.1.

The converse can be easily established as follows. Suppose

$$g(n) = \sum_{d|n} \mu(d) f(n/d).$$

It follows that

$$\begin{aligned}
\sum_{d|n} g(d) &= \sum_{d|n} \sum_{e|d} \mu(e) f(d/e) \\
&= \sum_{est=n} \mu(e) f(s) \\
&= \sum_{s|n} f(s) \sum_{e|\frac{n}{s}} \mu(e) \\
&= f(n)
\end{aligned}$$

by Proposition 1.3.1 again. This proves part (i). The proof of part (ii) follows immediately from the proof of part (i) if we replace the sum by products and the multiples by powers. □

An arithmetic function $f(n)$ is said to be **multiplicative** if

$$f(mn) = f(m)f(n)$$

whenever $(n, m) = 1$, where (n, m) is the greatest common divisor of n and m.

Lemma 1.3.3. *If $f(n)$ is multiplicative, then the function*

$$\sum_{d|n} f(d)$$

is a multiplicative function of n.

Proof. Let $g(n) = \sum_{d|n} f(d)$. Suppose $(n, m) = 1$. Then

$$\begin{aligned} g(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= g(m)g(n). \end{aligned}$$

This proves the lemma. □

Lemma 1.3.4. *The Möbius function $\mu(n)$ is multiplicative.*

Proof. Suppose $(n, m) = 1$. If n or m is not square-free, so is nm. In that case

$$\mu(n)\mu(m) = \mu(nm) = 0.$$

Otherwise n and m are square-free, say

$$n = p_1 \cdots p_k \text{ and } m = q_1 \cdots q_s$$

where the p_i and q_j are all distinct. Then

$$nm = p_1 \cdots p_k q_1 \cdots q_s$$

so that $\mu(n) = (-1)^k, \mu(m) = (-1)^s$ and

$$\mu(n)\mu(m) = (-1)^{k+s} = \mu(nm).$$

Hence $\mu(n)$ is multiplicative. □

The Euler totient function, $\phi(n)$, is the number of the positive integers less than n and relatively prime to n, namely,

$$\phi(n) := \sum_{\substack{1 \le j \le n \\ (j,n)=1}} 1.$$

Proposition 1.3.5. *We have*

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{1.3.2}$$

Proof. Let $N(d)$ denote the number of integers $1 \le m \le n$ that are divisible by d. Suppose m is an integer between 1 and n. In the expression $\sum\limits_{d|n} \mu(d)N(d)$, the integer m is counted in those $N(d)$ for which both $d \mid m$ and $d \mid n$. It is counted with weight $\sum_{d|n,m} \mu(d)$. Note that $N(d) = n/d$ when $d \mid n$. In view of Proposition 1.3.1, we see that

$$\sum_{d|n,m} \mu(d) = \sum_{d|(n,m)} \mu(d) = \begin{cases} 1 & \text{if } (n,m) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

This proves

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Hence $\phi(n)$ is multiplicative by Lemmas 1.3.3 and 1.3.4. Now the second equality of (1.3.2) follows from the multiplicative property of the function $\sum_{d|n} \mu(d)/d$ because

$$\prod_{p|n} \sum_{d|p^l} \frac{\mu(d)}{d} = \prod_{p|n} \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p} \right) = \prod_{p|n} \left(1 - \frac{1}{p} \right).$$

□

1.4 Cyclotomic Polynomials

A nth root of unity is a solution of $z^n = 1$ in $\mathbb{C}$. There are precisely n solutions for $z^n = 1$, namely, $e^{2\pi i/n}, e^{2\pi i2/n}, \cdots, e^{2\pi in/n}$. We often write ξ_n for $e^{2\pi i/n}$ so that $\xi_n, \xi_n^2, \cdots, \xi_n^n$ are the n roots of $z^n = 1$.

A nth root of unity is said to be **primitive** if it is of the form ξ_n^k with k and n relatively prime, i.e., $(k,n) = 1$. A primitive nth root of unity, ξ, has the property that it does not satisfy any equation of the form $z^m = 1$ with $m < n$, and $\xi^k, 1 \leq k \leq n$ are precisely all the nth root of unity. There are precisely $\phi(n)$ primitive nth roots of unity. The nth roots of unity form a (multiplicative) cyclic group of order n and the primitive roots correspond to the generators of this group.

Definition 1.4.1. *The* **nth cyclotomic polynomial** *is the monic polynomial*

$$\Phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (x - \xi_n^j)$$

whose roots are precisely the primitive nth roots of unity.

Examples. $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x - (-1) = x + 1$.

$$\Phi_3(x) = (x - (-1/2 + \sqrt{3}i/2))(x - (-1/2 - \sqrt{3}i/2)) = x^2 + x + 1$$

and $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$.

Definition 1.4.2. *A* **cyclotomic polynomial** *is a monic polynomial whose roots lie on the unit circle.*

We will see in Proposition 1.4.3 below that $\Phi_n(x)$ is irreducible. Clearly, any cyclotomic polynomial is a product of irreducible cyclotomic polynomials.

Proposition 1.4.3. *Let n be a positive integer and $\Phi_n(x)$ the nth cyclotomic polynomial. Then we have*

(i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$;

(ii) The coefficients of $\Phi_n(x)$ are integers;

(iii) $\Phi_n(x)$ is of degree $\phi(n)$;

(iv) $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof.

(i) Let ξ be a primitive nth root of unity. Consider the cyclic group G of all nth roots of unity and observe that G contains all dth roots of unity for every divisor d of n. Clearly $\eta \in G$ is a primitive dth root of unity (where $d \mid n$) if and only if $\text{ord}(\eta) = d$. Here $\text{ord}(\eta)$ is the order of η in G, i.e, the smallest positive integer m, such that $\eta^m = 1$. Therefore for each divisor d of n, $\Phi_d(x) = \prod_{\substack{\eta \in G \\ \text{ord}(\eta)=d}} (x - \eta)$ and

$$x^n - 1 = \prod_{\eta \in G} (x - \eta) = \prod_{d|n} \left(\prod_{\substack{\eta \in G \\ \text{ord}(\eta)=d}} (x - \eta) \right) = \prod_{d|n} \Phi_d(x).$$

(ii) We prove this part by induction on n. Clearly $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Assume that (ii) is true for all $k < n$ and let $f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$. Then $f \in \mathbb{Z}[x]$ by the induction hypothesis and $x^n - 1 = f(x)\Phi_n(x)$ by (i). On the other hand $x^n - 1 \in \mathbb{Z}[x]$ and $f(x)$ is monic. Consequently the division algorithm in $\mathbb{Z}[x]$ implies that $x^n - 1 = f(x)h(x) + r(x)$ for some $h(x), r(x) \in \mathbb{Z}[x]$. Therefore by the uniqueness of quotient and reminder of the division algorithm in $\mathbb{Z}[x]$ we must have $r(x) \equiv 0$ and $\Phi_n(x) \equiv h(x) \in \mathbb{Z}[x]$. This completes the induction.

(iii) The degree of $\Phi_n(x)$ is clearly the number of primitive nth roots of unity. Let ξ be such a primitive nth root of unity so that every root of unity is a power of ξ. Then ξ^i $(1 \leq i \leq n)$ is a primitive root of unity if and only if $(i, n) = 1$ and the number of such i is precisely $\phi(n)$.

(iv) Let $h(x)$ be an irreducible factor of $\Phi_n(x)$ in $\mathbb{Z}[x]$ with $\deg(h) \geq 1$ where $\deg(h)$ is the degree of $h(x)$. Then $\Phi_n(x) = f(x)h(x)$ with monic polynomials $f(x), h(x) \in \mathbb{Z}[x]$. Let ξ be any root of $h(x)$ and p any prime number such that $(p, n) = 1$. We shall first show that ξ^p is a root of $h(x)$. Since ξ is a root of $\Phi_n(x)$, ξ is a primitive nth root of unity. From the proof of (iii), ξ^p is also a primitive nth root of unity and therefore a root of either $f(x)$ or $h(x)$. Suppose ξ^p is not a root of $h(x)$. Then ξ^p is a root of $f(x) = \sum_{i=0}^{r} b_i x^i$ and hence ξ is a root of $f(x^p) = \sum_{i=0}^{r} b_i x^{ip}$. Since $h(x)$ is irreducible in $\mathbb{Z}[x]$ and has ξ as a root, $h(x)$ must divide $f(x^p)$, say $f(x^p) = h(x)k(x)$ with $k(x) \in \mathbb{Z}[x]$. Recall that the canonical projection $\mathbb{Z} \to \mathbb{Z}_p$ (denoted on elements by $b \mapsto \bar{b}$) induces a ring epimorphism $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ defined by $g = \sum_{i=0}^{t} c_i x^i \mapsto \bar{g} = \sum_{i=0}^{t} \bar{c}_i x^i$. Consequently, in $\mathbb{Z}_p[x]$, $\bar{f}(x^p) = \bar{h}(x)\bar{k}(x)$. But in $\mathbb{Z}_p[x]$, $\bar{f}(x^p) = \bar{f}(x)^p$. Therefore,

$$\bar{f}(x)^p = \bar{h}(x)\bar{k}(x) \in \mathbb{Z}_p[x].$$

Consequently, some irreducible factor of $\bar{h}(x)$ of positive degree must divide $\bar{f}(x)^p$ and hence $\bar{f}(x)$ in $\mathbb{Z}_p[x]$. On the other hand, since $\Phi_n(x)$ is a factor of $x^n - 1$, we have $x^n - 1 = \Phi_n(x)r(x) = f(x)h(x)r(x)$ for some $r(x) \in \mathbb{Z}[x]$. Thus in $\mathbb{Z}_p[x]$

$$x^n - \bar{1} = \overline{x^n - 1} = \bar{f}(x)\bar{h}(x)\bar{r}(x).$$

Since $\bar{f}(x)$ and $\bar{h}(x)$ have a common factor, $x^n - \bar{1}$ must have a multiple root. This contradicts the fact that the roots of $x^n - \bar{1}$ are all distinct since $(p, n) = 1$. Therefore ξ^p is a root of $h(x)$. If $r \in \mathbb{Z}$ is such that $1 \leq r \leq n$ and $(r, n) = 1$, then $r = p_1^{k_1} \cdots p_s^{k_s}$ where $k_i > 0$ and each p_i is a prime such that $(p_i, n) = 1$. Repeating the same argument for ξ^{p_i} whenever ξ is a root of $h(x)$, it follows that ξ^r is a root of $h(x)$. However, the ξ^r ($1 \leq r \leq n$ and $(r, n) = 1$) are precisely all of the primitive roots of unity from the proof of (iii). Thus $h(x)$ is divisible by $\prod_{\substack{1 \leq r \leq n \\ (r,n)=1}} (x - \xi^r) = \Phi_n(x)$ whence $\Phi_n(x) = h(x)$. Therefore $\Phi_n(x)$ is irreducible.

□

We should note that $\Phi_n(x)$, $n \in \mathbb{N}$, are all of the irreducible cyclotomic polynomials.

The nth cyclotomic polynomial, $\Phi_n(x)$, can be written as

$$\Phi_n(x) = \sum_{k=0}^{\phi(n)} a_n(k) x^k. \tag{1.4.1}$$

We have seen that $a_n(k) \in \mathbb{Z}$ in Proposition 1.4.3 (iii). Note that

$$x^n - 1 = \prod_{d|n} \prod_{\substack{1 \leq j \leq n \\ (j,n)=d}} (x - \xi_n^j) = \prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x).$$

By applying the Möbius inversion formula, one infers that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}. \tag{1.4.2}$$

In view of (1.4.2), we now have

Corollary 1.4.4. *Let $n > 1$ be an integer and $\Phi_n(x)$ the nth cyclotomic polynomial. Then*

$$x^{\phi(n)}\Phi_n(1/x) = \Phi_n(x).$$

Theorem 1.4.5. *The cyclotomic polynomials $\Phi_n(x)$ have the following properties.*

(i) If p is prime and $k \geq 1$, then $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.

(ii) If $n = p_1^{r_1}\dots p_k^{r_k}$ with distinct primes p_i and $r_i > 0$ then

$$\Phi_n(x) = \Phi_{p_1\dots p_k}(x^{p_1^{r_1-1}\dots p_k^{r_k-1}}).$$

(iii) If n is odd, then $\Phi_{2n} = \Phi_n(-x)$.

(iv) If p is prime and $p \nmid n$, then $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

Proof.

(i) This is a special case of (ii).

(ii) We have

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$$

If $\mu(n/d) \neq 0$ then by the definition of Möbius function there is no square factor in n/d. So $p_1^{r_1-1}\dots p_k^{r_k-1}$ divides d. Let $d = d'p_1^{r_1-1}\dots p_k^{r_k-1}$. We have

$$\begin{aligned}\Phi_n(x) &= \prod_{d'|p_1\dots p_k}(x^{p_1^{r_1-1}\dots p_k^{r_k-1}d'} - 1)^{\mu(n/d)}\\ &= \prod_{d'|p_1\dots p_k}(x^{p_1^{r_1-1}\dots p_k^{r_k-1}d'} - 1)^{\mu(\frac{p_1\cdots p_k}{d'})}\\ &= \Phi_{p_1\dots p_k}(x^{p_1^{r_1-1}\dots p_k^{r_k-1}}).\end{aligned}$$

(iii) Let n be an odd integer. By (1.4.2)

$$\Phi_{2n}(x) = \prod_{d|n}(x^d - 1)^{\mu(2n/d)}\prod_{d|n}(x^{2d} - 1)^{\mu(2n/2d)}$$

Since n is odd, $\mu(\frac{2n}{d}) = 0$ if and only if $\mu(\frac{2n}{2d}) = 0$. If $\mu(\frac{2n}{2d}) = (-1)^k$ then $\mu(\frac{2n}{d}) = (-1)^{k+1}$. So we have

$$\begin{aligned}\Phi_{2n}(x) &= \prod_{d|n}\left(\frac{x^{2d}-1}{x^d-1}\right)^{\mu(2n/2d)}\\ &= \prod_{d|n}(x^d + 1)^{\mu(n/d)} \qquad (1.4.3)\end{aligned}$$

Now suppose that n has $k \neq 0$ distinct prime factors. Then the number of d for which $\mu(n/d) \neq 0$ is 2^k, which is an even integer. We can rewrite (1.4.3) as

$$\begin{aligned}\Phi_{2n}(x) &= \prod_{d|n}(x^d+1)^{\mu(n/d)} \\ &= (-1)^{2^k}\prod_{d|n}(x^d+1)^{\mu(n/d)} \\ &= \prod_{d|n}(-x^d-1)^{\mu(n/d)} \\ &= \Phi_n(-x).\end{aligned}$$

(iv) By (1.4.2)

$$\begin{aligned}\Phi_{pn}(x) &= \prod_{d|pn}(x^d-1)^{\mu(\frac{pn}{d})} \\ &= \prod_{d|n}(x^d-1)^{\mu(\frac{pn}{d})}\prod_{d|n}(x^{pd}-1)^{\mu(\frac{pn}{pd})}.\end{aligned} \tag{1.4.4}$$

Since $p \nmid n$, $\mu(\frac{pn}{d}) = (-1)\mu(\frac{n}{d})$. So we can rewrite (1.4.4) as

$$\begin{aligned}\Phi_{pn}(x) &= \prod_{d|n}\left(\frac{x^{pd}-1}{x^d-1}\right)^{\mu(n/d)} \\ &= \Phi_{pn}(x^p)/\Phi_n(x).\end{aligned}$$

□

Theorem 1.4.5 implies that

$$a_n(k) = \begin{cases} a_{\gamma(n)}(\frac{k\gamma(n)}{n}) & \text{if } \frac{n}{\gamma(n)} \mid k; \\ 0 & \text{otherwise;}\end{cases}$$

where $a_n(k)$ is defined in (1.4.1) and $\gamma(n) = \prod_{p|n} p$ is the square free kernel of n. Also

$$a_{2n}(k) = (-1)^k a_n(k) \text{ for } n > 1 \text{ and } 2 \nmid n.$$

The size of the coefficients of the nth cyclotomic polynomial has been widely studied. It has been observed that the coefficients are quite often in the set $\{0, \pm 1\}$. Indeed, only for $n \geq 105$ some coefficients outside this range appear. Amazement over the smallness of $a_n(m)$ was expressed by D. Lehmer [11]. Mogotti showed in 1883 that $a_{pq}(i) \in \{0, \pm 1\}$, with p and q odd primes. On the other hand, E. Lehmer showed that $a_{pqr}(i)$ can be arbitrarily large when p, q and r are odd primes. There are more related details in [12].

Let $B(k) = \max_{n\geq 1} |a_n(k)|$. Bachman [1] showed that

$$\log B(k) = C_0 \frac{\sqrt{k}}{(\log k)^{1/4}} \left(1 + O\left(\frac{\log\log k}{\sqrt{\log k}}\right)\right) \tag{1.4.5}$$

for some constant C_0. Here $f(x) = O(g(x))$ or $f(x) \ll g(x)$ means $|f(x)| \leq Cg(x)$ for some constant $C > 0$.

Now put $A(n) = \max_m |a_n(m)|$. Erdös has shown that there exist $c > 0$ and infinitely many n such that

$$\log A(n) \gg \exp\left(\frac{c\log n}{\log\log n}\right).$$

On the other hand, it is known that

$$\log A(n) < \exp\left((\log 2 + o(1))\frac{\log n}{\log\log n}\right),$$

where the constant $\log 2$ is the best possible and $f(x) = o(1)$ means $\lim_{x\longrightarrow+\infty} f(x) = 0$.

Jiro Suzuki [9] proved the following result.

Theorem 1.4.6. *We have* $\{a_n(k) : n, k \in \mathbb{N}\} = \mathbb{Z}$.

1.5 Ramanujan's Sums

The Ramanujan's sum $c_n(m)$ is defined as

$$c_n(m) := \sum_{\substack{1\leq h\leq n \\ (h,n)=1}} e\left(\frac{hm}{n}\right),$$

where $e(t) = e^{2\pi it}$ and m, n are positive integers. Note that $c_n(m)$ is the sum of mth powers of the roots of $\Phi_n(x)$.

Proposition 1.5.1. *Let $\mu(n)$ be the Möbius function. We have*

(i) $c_n(m) = \sum_{d|(n,m)} d\mu(n/d)$;

(ii) $\mu(n) = \sum_{\substack{1\leq h\leq n \\ (h,n)=1}} e\left(\frac{h}{n}\right)$;

(iii) $c_n(m) = \mu(n/\delta)\phi(n)/\phi(n/\delta)$, *where* $\delta = (n, m)$.

Proof.

(i) Let

$$g(n) = \sum_{1 \le h \le n} e\left(\frac{hm}{n}\right).$$

Since this is a sum of a geometric progression, we find that

$$g(n) = \begin{cases} n & \text{if } n \mid m; \\ 0 & \text{otherwise.} \end{cases} \tag{1.5.1}$$

However, we can write

$$\begin{aligned} g(n) &= \sum_{d|n} \sum_{\substack{1 \le h \le n \\ (h,n)=d}} e\left(\frac{hm}{n}\right) \\ &= \sum_{d|n} \sum_{\substack{1 \le h_1 \le n_1 \\ (h_1,n_1)=1}} e\left(\frac{h_1 m}{n_1}\right), \end{aligned}$$

where $h = dh_1$ and $n = dn_1$ with $(h_1, n_1) = 1$ in the last summation. Thus,

$$g(n) = \sum_{d|n} c_{n/d}(m).$$

By the Möbius inversion formula, we get

$$c_n(m) = \sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(n/d) g(d).$$

Therefore, using (1.5.1), we have

$$c_n(m) = \sum_{d|(n,m)} d\mu(n/d)$$

as required.

(ii) Result follows by putting $m = 1$ in part (i).

(iii) By part (i), we have

$$\begin{aligned} c_n(m) &= \sum_{d|\delta} d\mu(n/d) \\ &= \sum_{de=\delta} d\mu(ne/\delta) \\ &= \sum_{de=\delta} d\mu(n_1 e), \end{aligned}$$

where $\delta = (n, m)$ and $n = \delta n_1$. Now,

$$\mu(n_1 e) = \begin{cases} \mu(n_1)\mu(e) & \text{if } (n_1, e) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$\begin{aligned} c_n(m) &= \sum_{\substack{de=\delta \\ (n_1,e)=1}} d\mu(n_1)\mu(e) \\ &= \mu(n_1)\delta \sum_{\substack{e|\delta \\ (n_1,e)=1}} \frac{\mu(e)}{e} \\ &= \mu(n_1)\delta \prod_{\substack{p|\delta \\ p\nmid n_1}} \left(1-\frac{1}{p}\right). \end{aligned}$$

By (1.3.2)

$$\frac{\phi(n)}{\phi(n/\delta)} = \frac{n}{n/\delta} \prod_{\substack{p|\delta \\ p\nmid n_1}} \left(1-\frac{1}{p}\right) = \delta \prod_{\substack{p|\delta \\ p\nmid n_1}} \left(1-\frac{1}{p}\right),$$

and hence the result follows.

□

Although $c_q(m)$ is not a multiplicative function of m,it is a multiplicative function of q and this gives a complete evaluation of $c_q(m)$ below.

Lemma 1.5.2. *We have*

$$c_{q_1q_2}(m) = c_{q_1}(m)c_{q_2}(m), \quad \textit{if} \;\; (q_1,q_2) = 1, \tag{1.5.2}$$

and

$$c_q(m) = \mu\left(\frac{q}{(m,q)}\right)\phi(q)\phi^{-1}\left(\frac{q}{(m,q)}\right). \tag{1.5.3}$$

Proof. Since $(q_1,q_2) = 1$, so for every integer h we write $h = q_2h_1 + q_1h_2$, and if $(h,q_1q_2) = 1$, we must have $(h_1,q_1) = 1$ and $(h_2,q_2) = 1$. We write

$$\begin{aligned} c_{q_1q_2}(m) &= \sum_{\substack{1\le h\le q_1q_2 \\ (h,m)=1}} e\left(\frac{mh}{q}\right) \\ &= \sum_{\substack{1\le h_1\le q_1 \\ (h_1,q_1)=1}} \sum_{\substack{1\le h_2\le q_2 \\ (h_2,q_2)=1}} \left(\frac{m(q_2h_2+q_1h_2)}{q_1q_2}\right) \\ &= \sum_{\substack{1\le h_1\le q_1 \\ (h_1,q_1)=1}} e\left(\frac{mh_1}{q_1}\right) \sum_{\substack{1\le h_2\le q_2 \\ (h_2,q_2)=1}} e\left(\frac{mh_2}{q_2}\right), \end{aligned}$$

and this proves (1.5.2).

Because of the multiplicative property, we only need to prove (1.5.3) for the case $q = p^l$. Note that if $q = p^l$, $l \geq 1$, we have

$$\begin{aligned} c_{p^l}(m) &= \sum_{\substack{1 \leq h \leq p^l \\ (h,p^l)=1}} e\left(\frac{hm}{p^l}\right) \\ &= \sum_{h=1}^{p^l} e\left(\frac{hm}{p^l}\right) - \sum_{h=1}^{p^{l-1}} e\left(\frac{hm}{p^{l-1}}\right) \\ &= \begin{cases} p^l - p^{l-1} & \text{if } p^l \mid m; \\ -p^{l-1} & \text{if } p^{l-1} \parallel m; \\ 0 & \text{if } p^{l-1} \nmid m. \end{cases} \end{aligned}$$

Here $p^l \parallel m$ means $p^l | m$ but $p^{l+1} \nmid m$. So in any case we always have

$$C_{p^l}(m) = \mu\left(\frac{p^l}{(m,p^l)}\right) \phi(p^l) \phi^{-1}\left(\frac{p^l}{(m,p^l)}\right).$$

Then (1.5.3) follows from (1.5.2). □

Lemma 1.5.3. *For $n > 1$ and $m \not\equiv 0 \pmod{n}$, we have*

$$\sum_{d|n} c_d(m) = 0. \tag{1.5.4}$$

Proof. We first note that the above summation is the sum of the mth power of all the roots of the polynomial $\prod_{d|n} \Phi_d(x)$ which equals $x^n - 1$ by Lemma 1.4.3 (i). Since all the coefficients of the polynomial $x^n - 1$ are 0 except the first and the last coefficients, so by Newton's identity, the summation in (1.5.4) is zero. □

Chapter 2

Cyclotomic Polynomials With Odd Coefficients

2.1 Factorization over $\mathbb{Z}_p[x]$ and Graeffe's Algorithm

In this section, we summarize the results about the factorization of cyclotomic polynomials with odd coefficients as a product of irreducible cyclotomic polynomials in [2]. These results are essential to our results in the next chapter. For the sake of completeness, we record and reorganize most of the proofs here.

Let p be a prime.

Lemma 2.1.1. *Suppose n and m are distinct positive integers relatively prime to p. Then $\Phi_n(x)$ and $\Phi_m(x)$ are relatively prime in $\mathbb{Z}_p[x]$.*

Proof. Suppose e and f are the smallest positive integers such that

$$p^e \equiv 1 \pmod{n} \quad \text{and} \quad p^f \equiv 1 \pmod{m}.$$

Let F_{p^k} be the field of order p^k. Then F_{p^e} contains exactly $\phi(n)$ elements of order n and over $\mathbb{Z}_p$, $\Phi_n(x)$ is a product of $\phi(n)/e$ irreducible factors of degree e and each irreducible factor is a minimal polynomial for an element in F_{p^e} of order n over $\mathbb{Z}_p$. So $\Phi_n(x)$ and $\Phi_m(x)$ cannot have a common factor in $\mathbb{Z}_p[x]$ since their irreducible factors are minimal polynomials of different orders. □

Definition 2.1.2. *For each prime p let T_p be the operator defined over all monic polynomials in $\mathbb{Z}[x]$ by*

$$T_p[P(x)] := \prod_{i=1}^{N} (x - \alpha_i^p)$$

for every $P(x) = \prod_{i=1}^{N}(x - \alpha_i)$ *in* $\mathbb{Z}[x]$.

By Newton's identity $T_p[P(x)]$ is also a monic polynomial in $\mathbb{Z}[x]$. The operator $T_p[\cdot]$ can be extended to be defined over the quotient of two monic polynomials in $\mathbb{Z}[x]$ by $T_p[(P/Q)(x)] := T_p[P(x)]/T_p[Q(x)]$. This operator takes a polynomial to the polynomial whose roots are the pth power roots of $P(x)$. This is referred as Graeffe's root squaring algorithm if $p = 2$.

Lemma 2.1.3. *Let n be a positive integer relatively prime to p and $i \geq 2$. Then we have*

(i) $T_p[\Phi_n(x)] = \Phi_n(x)$;

(ii) $T_p[\Phi_{pn}(x)] = \Phi_n(x)^{p-1}$;

(iii) $T_p[\Phi_{p^i n}(x)] = \Phi_{p^{i-1}n}(x)^p$.

Proof. If $(n,p) = 1$ then T_p just permutes the roots of $\Phi_n(x)$ and this proves (i). To prove (ii) and (iii), we consider

$$\begin{aligned} T_p[P(x^p)] &= T_p\left[\prod_{j=1}^{N}(x^p - \alpha_i)\right] \\ &= T_p\left[\prod_{j=1}^{N}\prod_{l=1}^{p}(x - e^{\frac{2\pi i l}{p}}\alpha_i^{\frac{1}{p}})\right] \\ &= \prod_{j=1}^{N}\prod_{l=1}^{p}(x - \alpha_i) = P(x)^p. \end{aligned}$$

Thus (ii), (iii) follow from (i) and Lemma 1.4.5. □

Definition 2.1.4. *For each prime p let M_p be the natural projection from $\mathbb{Z}[x]$ onto $\mathbb{Z}_p[x]$. So*

$$M_p[P(x)] = P(x) \pmod{p}.$$

When $P(x)$ is cyclotomic, the iterates $T_p^n[P(x)]$ converge in a finite number of steps to a fixed point of T_p and we define this to be the **fixed point** of $P(x)$ with respect to T_p.

Lemma 2.1.5. *If $P(x)$ is a monic cyclotomic polynomial in $\mathbb{Z}[x]$, then*

$$M_p[T_p[P(x)]] = M_p[P(x)] \tag{2.1.1}$$

in $\mathbb{Z}_p[x]$.

Proof. Since both T_p and M_p are multiplicative, it suffices to consider the primitive cyclotomic polynomials $\Phi_n(x)$. Let n be an integer relatively prime to p. Then (2.1.1) is true for $P(x) = \Phi_n(x)$, by (i) of Lemma 2.1.3. For $P(x) = \Phi_{pn}(x)$, we have

$$M_p[T_p[\Phi_{pn}(x)]] = M_p[\Phi_n(x)^{p-1}] = M_p[\Phi_n(x)]^{p-1}$$

by (ii) of Lemma 2.1.3. However,

$$M_p[\Phi_{pn}(x)] = \frac{M_p[\Phi_n(x^p)]}{M_p[\Phi_n(x)]} = \frac{M_p[\Phi_n](x^p)}{M_p[\Phi_n(x)]} = M_p[\Phi_n(x)]^{p-1},$$

in $\mathbb{Z}_p[x]$. This proves that (2.1.1) is also true for $P(x) = \Phi_{pn}(x)$. Finally, if $P(x) = \Phi_{p^in}(x)$ then

$$M_P[T_p[\Phi_{p^in}(x)]] = M_p[\Phi_{p^{i-1}n}(x)^p] = M_p[\Phi_{p^{i-1}n}(x^p)] = M_p[\Phi_{p^in}(x)]$$

by (iii) of Lemma 2.1.3. This completes the proof. □

Lemma 2.1.5 shows that if $T_p[P(x)] = T_p[Q(x)]$ then $M_p[P(x)] = M_p[Q(x)]$. In the next theorem we see that the converse is also true.

Theorem 2.1.6. *$P(x)$ and $Q(x)$ are monic cyclotomic polynomials in $\mathbb{Z}[x]$ and $M_p[P(x)] = M_p[Q(x)]$ in $\mathbb{Z}_p[x]$ if and only if both $P(x)$ and $Q(x)$ have the same fixed point with respect to iteration of T_p.*

Proof. Suppose

$$P(x) = \prod_{d\in\mathfrak{D}} \Phi_d^{e(d)}(x)\Phi_{pd}^{e(pd)}(x)\cdots\Phi_{p^td}^{e(p^td)}(x)$$

and

$$Q(x) = \prod_{d\in\mathfrak{D}} \Phi_d^{e(d)'}(x)\Phi_{pd}^{e(pd)'}(x)\cdots\Phi_{p^td}^{e(p^td)'}(x)$$

where $t, e(j), e(j)' \geq 0$ and $\mathfrak{D}$ is a set of positive integers relatively prime to p. Then using Lemma 2.1.3, we have for $l \geq t$

$$T_p^l[P(x)] = \prod_{d\in\mathfrak{D}} \Phi_d(x)^{f(d)} \text{ and } T_p^l[Q(x)] = \prod_{d\in\mathfrak{D}} \Phi_d(x)^{f(d)'} \tag{2.1.2}$$

where

$$f(d) = e(d) + (p-1)\sum_{j=1}^{t} p^{j-1}e(p^jd)$$

and

$$f(d)' = e(d)' + (p-1)\sum_{j=1}^{t} p^{j-1}e(p^jd)'.$$

From Lemma 2.1.5, we have

$$\prod_{d\in\mathfrak{D}} M_p[\Phi_d(x)]^{f(d)} = \prod_{d\in\mathfrak{D}} M_p[\Phi_d(x)]^{f(d)'}.$$

However, with Lemma 2.1.1, $M_p[\Phi_d(x)]$ and $M_p[\Phi'_d(x)]$ are relatively prime if $d \neq d'$. So we must have $f(d) = f(d)'$ for all $d \in \mathfrak{D}$ and hence from (2.1.2), $P(x)$ and $Q(x)$ have the same fixed point with respect to T_p. □

The following lemma tells us which $\Phi_m(x)$ can possibly be factors of polynomials with odd coefficients.

Lemma 2.1.7. *Suppose $P(x)$ is a polynomial with odd coefficients of degree $N-1$. If $\Phi_m(x)$ divides $P(x)$, then m divides $2N$.*

Proof. Since $\Phi_m(x)$ divides $P(x)$, $\Phi_m(x)$ also divides $P(x)$ in $\mathbb{Z}_2[x]$. However, in $\mathbb{Z}_2[x]$, $P(x)$ equals to $1+x+\cdots+x^{N-1}$ and can be factored as

$$P(x) = \Phi_1(x)^{-1} \prod_{d|M} \Phi_d^{2^t}(x), \tag{2.1.3}$$

where $N = 2^t M$, $t \geq 0$ and M is odd. In view of Lemma 2.1.1, $\Phi_{d_1}(x)$ and $\Phi_{d_2}(x)$ are relatively prime in $\mathbb{Z}_2[x]$ if d_1 and d_2 are distinct odd integers. So if m is odd, then $\Phi_m(x)$ is a factor of $P(x)$ and hence $m = d$ for some $d \mid M$. On the other hand, if m is even and $m = 2^l m'$ where $l \geq 1$ and m' is odd, then

$$\Phi_m(x) = \Phi_{2m'}(x^{2^{l-1}}) = \Phi_{m'}(x^{2^{l-1}}) = \Phi_{m'}(x)^{2^{l-1}} \tag{2.1.4}$$

in $\mathbb{Z}_2[x]$. Thus, we must have $m' = d$ for $d \mid M$ and $l \leq t+1$. Hence in both case, we have m divides $2N$. □

2.2 Characterization of Cyclotomic Polynomials with Odd Coefficients

In this section, we will characterize the cyclotomic polynomials with odd coefficients in Corollary 2.2.2 below. In view of Lemma 2.1.7, every cyclotomic polynomial, $P(x)$, with odd coefficients of degree $N-1$ can be written as

$$P(x) = \prod_{d|2N} \Phi_d^{e(d)}(x), \tag{2.2.1}$$

where $e(d) \geq 0$.

Now we characterize the monic cyclotomic polynomials by their image in $\mathbb{Z}_p[x]$ under the projection M_p. They all have the same fixed point under T_p. In particular, when $p = 2$ we have:

Corollary 2.2.1. *All monic cyclotomic polynomials with odd coefficients of degree $N-1$ have the same fixed point under iteration of T_2. Specifically, if $N = 2^t M$ where $t \geq 0$ and $(2, M) = 1$ then the fixed point occurs at the $t+1$-th step of the iteration and equals*

$$(x^M - 1)^{2^t}(x-1)^{-1}.$$

Proof. The first part follows directly from Theorem 2.1.6 and the fact that

$$M_2[P(x)] = 1 + x + \cdots + x^{N-1}$$

in $\mathbb{Z}_2[x]$ if $P(x)$ is a monic polynomial with odd coefficients of degree $N-1$. If $N = 2^t M$, then from (2.2.1),

$$P(x) = \prod_{d|M} \Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)}(x)\cdots\Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x).$$

Over $\mathbb{Z}_2[x]$,

$$1 + x + \cdots + x^{N-1} = \Phi_1(x)^{-1} \prod_{d|M} \Phi_d^{2^t}(x),$$

so

$$f(d) = e(d) + \sum_{i=1}^{t+1} 2^{i-1} e(2^i d) = \begin{cases} 2^t & \text{for } d \mid M \ , d > 1; \\ 2^t - 1 & \text{for } d = 1. \end{cases} \tag{2.2.2}$$

Therefore, from (2.2.2) and Lemma 2.1.3, we have

$$\begin{aligned} T_2^{t+1}[P(x)] &= \prod_{d|M} \Phi_d^{f(d)}(x) \\ &= \Phi_1(x)^{-1} \prod_{d|M} \Phi_d^{2^t}(x) \\ &= (x^M - 1)^{2^t}(x-1)^{-1}. \end{aligned}$$

□

Corollary 2.2.1, when N is odd ($t = 0$), shows that $T_2[P(x)]$ equals to $1 + x + \cdots + x^{N-1}$ for all cyclotomic polynomials with odd coefficients and from (2.2.1) and (2.2.2) , we have the following characterization of cyclotomic polynomials with odd coefficients.

Corollary 2.2.2. *Let $N = 2^t M$ with $t \geq 0$ and $(2, M) = 1$. A polynomial, $P(x)$, with odd coefficients of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \prod_{d|M} \Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)}(x)\cdots\Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x),$$

and the $e(d)$ satisfy the condition (2.2.2). Furthermore, if N is odd, then any polynomial, $P(x)$, with odd coefficients of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \prod_{d|N, d>1} \Phi_d^{e(d)}(\pm x) \tag{2.2.3}$$

where the $e(d)$ are non-negative integers.

In view of Corollary 2.2.2, we are able to compute the number of cyclotomic polynomials with odd coefficients. Let $p(n)$ be the number of partitions of n into a sum of terms of the sequence $\{1, 2, 4, 8, 16, \cdots\}$. Then $p(n)$ has generating function

$$f(x) = (1-x)^{-1} \prod_{k=0}^{\infty} (1 - x^{2^k})^{-1}. \tag{2.2.4}$$

It follows from (2.2.2) and Corollary 2.2.2 that

Corollary 2.2.3. *Let $N = 2^t M$ with $t \geq 0$ and $(2, M) = 1$. The number of cyclotomic polynomials with odd coefficients of degree $N-1$ is*

$$q(N) = p(2^t)^{d(M)-1} \cdot p(2^t - 1) \tag{2.2.5}$$

where $d(M)$ denotes the number of divisors of M. Furthermore,

$$\log q(N) \sim (\frac{t^2}{2} \log 2)(d(M) - 1) + \frac{(\log(2^t - 1))^2}{\log 4}. \tag{2.2.6}$$

Proof. Formula (2.2.5) follows from (2.2.2) and Corollary 2.2.2. To prove (2.2.6), we use de Brujin's asymptotic estimate for $p(n)$ in [4],

$$p(n) \sim \exp((\log n)^2 / \log 4).$$

Here $f(x) \sim g(x)$ means $\lim_{x \longrightarrow +\infty} \frac{f(x)}{g(x)} = 1$. Now (2.2.6) follows from this and (2.2.5). □

2.3 Characterization of Littlewood Cyclotomic Polynomials

Among all cyclotomic polynomials, we are particularly interested in Littlewood polynomials, i.e., with ±1 coefficients. In this section, we consider the characterization of such polynomials. In [2], Borwein and Choi proved Theorem 2.3.1 below. Since we will give a simpler proof of this result in the next chapter, so we simply quote the result without proof here.

Theorem 2.3.1. *Suppose N is odd. A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}), \tag{2.3.1}$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct.

Corollary 2.3.2. *Suppose N is odd. Then $P(x)$ is a Littlewood cyclotomic polynomial of degree $N-1$ if and only if*

$$P(x) = \pm \prod_{i=1}^{t} \frac{x^{N_i} + (-1)^{\varepsilon+i}}{x^{N_{i-1}} + (-1)^{\varepsilon+i}}$$

where $\varepsilon = 0$ or 1, $N_0 = 1$, $N_t = N$ and N_{i-1} is a proper divisor of N_i for $i = 1,\ 2, \cdots, t$.

Proof. From Theorem 2.3.1 $P(x)$ is a Littlewood cyclotomic polynomial if and only if

$$\begin{aligned} P(x) &= \Phi_{p_1}(x)\Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}) \\ &= \Phi_{p_1}(x) \cdots \Phi_{p_{n_1}}(x^{p_1 \cdots p_{n_1} - 1})\Phi_{p_{n_1+1}}(-x^{p_1 \cdots p_{n_1}}) \cdots \Phi_{p_{n_2}}(-x^{p_1 \cdots p_{n_2 - 1}}) \\ &\quad \cdots \Phi_{p_{n_{t-1}+1}}((-1)^{t-1} x^{p_1 \cdots p_{n_{t-1}}}) \cdots \Phi_{p_{n_t}}((-1)^{t-1} x^{p_1 \cdots p_{n_t - 1}}) \end{aligned} \tag{2.3.2}$$

where $N = p_1 \cdots p_{n_t}$. Since $\Phi_p(x) = \frac{x^p-1}{x-1}$, (2.3.2) becomes

$$P(x) = \prod_{i=1}^{t} \frac{x^{N_i} + (-1)^i}{x^{N_{i-1}} + (-1)^i}$$

where $N_0 = 1$ and $N_i = p_1 \cdots p_{n_i}$ for $i = 1, \cdots, t$. This proves the corollary. □

P. Borwein and K.K. Choi conjecture that Theorem 2.3.1 also holds for polynomials of odd degree. They computed up to degree 210 (expect for the case $n-1 = 191$). The computation was based on computing all cyclotomic polynomials with odd coefficients of a given degree and then checking which were actually Littlewood and setting that this set matched the set generated by the conjecture. For example, for $N-1 = 143$ there are 6773464 cyclotomic polynomials with odd coefficients of which 416 are Littlewood.

Conjecture 2.3.3. *A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}), \tag{2.3.3}$$

where $N = p_1 p_2 \cdots p_r$ and all p_i are primes, not necessarily distinct.

Using Corollary 2.3.2, we can count the number of cyclotomic Littlewood polynomials of given even degree. For any positive integer N and t, define

$$r(N,t) := \#\{(N_1, N_2, \cdots, N_t) : \; N_1 \mid N_2 \mid \cdots \mid N_t, \; 1 < N_1 < N_2 < \cdots < N_t = N\};$$

and for $i \geq 1$,

$$d_i(N) := \sum_{n|N} d_{i-1}(n) \tag{2.3.4}$$

where $d_0(N) = 1$.

Lemma 2.3.4. *For $l, t \geq 0$ and p prime, we have*

$$d_t(p^l) = \binom{l+t}{t}. \tag{2.3.5}$$

Proof. We prove the lemma by induction on t. Equality (2.3.5) is clearly true for $t = 0$ because $d_0(N) = 1$. We then suppose (2.3.5) is true for $t-1$ where $t \geq 1$. Then

$$d_t(p^l) = \sum_{n|p^l} d_{t-1}(n) = \sum_{i=0}^{l} d_{t-1}(p^i) = \sum_{i=0}^{l} \binom{i+t-1}{t-1}.$$

So $d_t(p^l)$ is the coefficient of x^{t-1} in

$$\begin{aligned} & (x+1)^{t-1} + (x+1)^t + \cdots + (x+1)^{l+t-1} \\ = \;& (x+1)^{t-1}\{\frac{(x+1)^{l+1}-1}{x}\} \\ = \;& \frac{(x+1)^{l+t} - (x+1)^{t-1}}{x}. \end{aligned}$$

Hence $d_t(p^l)$ is the coefficient of x^t in $(x+1)^{l+t} - (x+1)^{t-1}$. Therefore, $d_t(p) = \binom{l+t}{t}$. □

Since $d_t(N)$ is a multiplicative function of N, we have

Corollary 2.3.5. *If $N = p_1^{r_1} \cdots p_s^{r_s}$ where $r_i \geq 1$ and p_i are distinct primes, then*

$$d_t(N) = \prod_{i=1}^{s} \binom{r_i + t}{t}.$$

Lemma 2.3.6. *For any positive integer N and t, we have*

$$r(N,t) := \begin{cases} 0 & \text{if } N = 1; \\ \sum_{i=1}^{t} (-1)^{t-i} \binom{t}{i} d_{i-1}(N) & \text{if } N > 1. \end{cases} \tag{2.3.6}$$

Proof. The proof is by induction on t. It is clear from the definition that $r(1,t) = 0$ and $r(N,1) = 1$ for any $t, N \geq 1$. We then suppose $N > 1$ and (2.3.6) is true for $t-1$ where $t \geq 2$. Then

$$\begin{aligned} r(N,t) &= \sum_{\substack{N_1 \mid N \\ N_1 > 1}} r(N/N_1, t-1) \\ &= \sum_{\substack{N_1 \mid N \\ N > N_1 > 1}} r(N/N_1, t-1) \\ &= \sum_{N_1 \mid N} \left\{ \sum_{i=1}^{t-1} (-1)^{t-i-1} \binom{t-1}{i} d_{i-1}(N/N_1) \right\} \\ &\quad - \sum_{i=1}^{t-1} (-1)^{t-i-1} \binom{t-1}{i} \{ d_{i-1}(1) + d_{i-1}(N) \} \\ &= \sum_{i=2}^{t} (-1)^{t-i} \binom{t-1}{i-1} d_{i-1}(N) \\ &\quad - \sum_{i=1}^{t-1} (-1)^{t-i-1} \binom{t-1}{i} d_{i-1}(N) + (-1)^{t-1} \\ &= \sum_{i=1}^{t} (-1)^{t-i} \binom{t}{i} d_{i-1}(N) \end{aligned}$$

from (2.3.4) and the fact that $\binom{t-1}{i-1} + \binom{t-1}{i} = \binom{t}{i}$. □

Corollary 2.3.7. *The number of Littlewood cyclotomic polynomials of degree $N-1$ where $N = p_1^{r_1} \cdots p_s^{r_s}$, $r_i \geq 1$ and the p_i are distinct odd primes, is*

$$4 \sum_{i=1}^{r_1+\cdots+r_s} \sum_{j=1}^{i} (-1)^{i-j} \binom{i}{j} \prod_{k=1} s \binom{r_k + j - 1}{j-1}.$$

Proof. From Corollary 2.3.4, the number of Littlewood cyclotomic polynomials of degree $N-1$ is

$$4 \sum_{i=1}^{r_1+\cdots+r_s} r(N,j).$$

The corollary now follows from Corollary 2.3.5 and Lemma 2.3.6. □

Chapter 3

Littlewood Cyclotomic Polynomials

3.1 Littlewood Cyclotomic Polynomials

In this chapter, we consider Littlewood cyclotomic polynomials of odd degree and prove that Conjecture 2.3.3 is true for certain special cases.

Let $P(x) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1}$, $a_i = \pm 1$ and $N = 2^tM$ with $2 \nmid M$. Without loss of generality, assume $a_0 = a_1 = +1$, by replacing by $-P(x)$ or $P(-x)$ if necessary. Now consider

$$\begin{aligned} Q(x) &= -\Phi_1(x)P(x) \\ &= (1-x)P(x) \\ &= a_0 + (a_1 - a_0)x + \cdots + (a_{N-1} - a_{N-2})x^{N-1} - a_{N-1}x^N \\ &:= b_0 + b_1x + \cdots + b_Nx^N \end{aligned} \tag{3.1.1}$$

with $b_0 = a_0 = 1$ and $b_N = -a_{N-1} = \pm 1$ but $b_1, b_2, \ldots, b_{N-1} \in \{-2, 0, 2\}$. Also since $a_1 = 1$, so $b_1 = 0$.

We now suppose

$$b_0 = 1,\ b_1 = \cdots = b_{i-1} = 0,\ b_i = -2, \tag{3.1.2}$$

for some $i \geq 2$. By Corollary 2.2.2,

$$Q(x) = \prod_{d|M} \prod_{l=0}^{t+1} \Phi_{2^ld}^{e(2^ld)}(x) \tag{3.1.3}$$

where for any $d|M$

$$e(d) + e(2d) + 2e(4d) + \cdots + 2^te(2^{t+1}d) = \sum_{l=0}^{t+1} \phi(2^l)e(2^ld) = 2^t. \tag{3.1.4}$$

Let S_j be the sum of the jth power of all the roots of $Q(x)$. Since the sum of the jth power of all the roots of $\Phi_n(x)$ is $c_n(j)$, so

$$S_j = \sum_{d|M}\sum_{l=0}^{t+1} e(2^l d)c_{2^l d}(j).$$

From Newton's identity, we have

$$S_j + b_1 S_{j-1} + \cdots + b_{j-1}S_1 + jb_j = 0 \tag{3.1.5}$$

for $j \le N-1$. For $j=1$, we have $S_1 + b_1 = 0$. However, $b_1 = 0$ and hence $S_1 = 0$. For $j=2$, since $b_1 = b_2 = 0$, so

$$S_2 = -b_1 S_1 - 2b_2 = 0.$$

Inductively, we have

$$S_1 = \cdots = S_{i-1} = 0.$$

For $j = i$, we have

$$S_i = -ib_i = 2i. \tag{3.1.6}$$

Lemma 3.1.1. *Let $N = 2^t M$ with $2 \nmid M$. Suppose $(N,k) = m = (N,m)$. Then*

$$(2^j d, k) = (2^j d, m) \textit{ for } j = 0,1,\cdots,t \textit{ and } d \mid M.$$

Proof. For any $l \mid N$, we claim that

$$(l,k) = (l,m).$$

Indeed, since $m \mid k$, so $(l,m) \mid (l,k)$. Suppose there is $p^\alpha \mid (l,k)$ but $p^\alpha \nmid (l,m)$. Then $p^\alpha \nmid m$. However, since $(l,k) \mid (N,k)$, it follows that $p^\alpha \mid (N,k) = (N,m)$ and hence $p^\alpha \mid m$. Contradiction arises. So $(l,m) = (l,k)$ and hence $(2^j d, m) = (2^j d, k)$ for $j = 0,1,\cdots,t$ and $d \mid M$. □

Lemma 3.1.2. *Let $N = 2^t M$ with $2 \nmid M$. If $2^{t+1} \nmid k$ and $(N,k) = m = (N,m)$ then $(2^{t+1}d,k) = (2^{t+1}d,m)$ for any $d \mid M$.*

Proof. Since $m = (N,k)$, so $m \mid k$ and for any $d|M$, we have

$$(2^{t+1}d,m) \mid (2^{t+1}d,k).$$

It remains to prove that

$$(2^{t+1}d,k) \mid (2^{t+1}d,m).$$

Let p be an odd prime. If $p^\alpha \mid (2^{t+1}d,k)$ then $p^\alpha \mid (d,k)$. Since $d \mid N$, $p^\alpha \mid (N,k)$. Since $(N,k) = (N,m)$, therefore $p^\alpha \mid (N,m)$ and hence $p^\alpha \mid m$. Now we know that p^α divides both d and m. So $p^\alpha \mid (2^{t+1}d,m)$. If $2^\alpha \mid (2^{t+1}d,k)$ then $2^\alpha \mid k$. Because $2^{t+1} \nmid k$ we get $\alpha \le t$. Since $N = 2^t M$, so $2^\alpha \mid N$. Now we know that 2^α divides both N and k. So $2^\alpha \mid (N,k) = m$. Therefore, $2^\alpha \mid (2^{t+1}d,m)$ and hence $(2^{t+1}d,k) \mid (2^{t+1}d,m)$. This completes the proof. □

Recall (1.5.3) that

$$c_q(m) = \mu\left(\frac{q}{(m,q)}\right)\phi(q)\phi^{-1}\left(\frac{q}{(m,q)}\right).$$

Note that if $(q, m_1) = (q, m_2)$ then

$$c_q(m_1) = c_q(m_2).$$

Lemma 3.1.3. *If $2^{t+1} \nmid k$, then*

$$S_k = S_{(N,k)}.$$

Proof. If $2^{t+1} \nmid k$, then suppose $(N,k) = m$. Then $(N,k) = m = (N,m)$ and $(2^j d, k) = (2^j d, m)$ for $j = 0, 1, \cdots, t+1$ and $d \mid M$ by Lemmas 3.1.1 and 3.1.2. Hence

$$\begin{aligned} S_k &= \sum_{d|M}\sum_{l=0}^{t+1} e(2^l d) c_{2^l d}(k) \\ &= \sum_{d|M}\sum_{l=0}^{t+1} e(2^l d) c_{2^l d}(m) \\ &= S_m = S_{(N,k)}. \end{aligned}$$

□

Lemma 3.1.4. *If $2^{t+1} \mid k$ and $k \leq N-1$, then $S_k = 0$.*

Proof. Let $k = 2^{t+1}k'$. Then for any $j \in \{0, 1, \cdots, t+1\}$ and $d \mid M$, we have

$$\begin{aligned} c_{2^j d} &= \mu\left(\frac{2^j d}{(2^j d, k)}\right)\phi(2^j d)\phi^{-1}\left(\frac{2^j d}{(2^j d, k)}\right) \\ &= \mu\left(\frac{d}{(d,k)}\right)\phi(2^j)\phi(d)\phi^{-1}\left(\frac{d}{(d,k)}\right) \\ &= c_d(k)\phi(2^j). \end{aligned}$$

So

$$\begin{aligned} S_k &= \sum_{d|M}\sum_{j=0}^{t+1} e(2^j d) c_{2^j d}(k) \\ &= \sum_{d|M}\sum_{j=0}^{t+1} e(2^j d)\phi(2^j) c_d(k) \\ &= \sum_{d|M} c_d(k) \sum_{j=0}^{t+1} e(2^j d)\phi(2^j) \\ &= \sum_{d|M} c_d(k) 2^t \\ &= 2^t \sum_{d|M} c_d(k) = 0 \end{aligned}$$

by (3.1.4) and Lemma 1.5.3 because $k \not\equiv 0 \pmod{M}$ otherwise $N|k$ and $k \geq N$. □

Lemma 3.1.5. *We have $i \mid N$, where i is defined in* (3.1.2)

Proof. Since $S_i \neq 0$, by Lemma 3.1.4, $2^{t+1} \nmid i$. By Lemma 3.1.3, $S_i = S_{(N,i)}$. If $(N,i) < i$ then $S_{(N,i)} = 0 \neq S_i$ by (3.1.2). Hence $(N,i) = i$ and $i \mid N$. □

We wish to show that

$$\begin{gathered} S_1 = \cdots = S_{i-1} = 0 \\ S_{i+1} = \cdots = S_{2i-1} = 0 \\ \vdots \\ S_{(N/i-1)i+1} = \cdots = S_{N-1} = 0 \end{gathered}$$

i.e.

$$S_j = 0 \text{ for all } j \not\equiv 0 \pmod{i}. \tag{3.1.7}$$

Suppose (3.1.7) is proved. Then we claim that

$$b_j = 0 \text{ for all } j \not\equiv 0 \pmod{i}.$$

For, by Newton's identity, if $j \not\equiv 0 \pmod{i}$, then

$$S_j + \sum_{l=1}^{j-1} b_l S_{j-l} + j b_j = 0.$$

For $1 \leq l \leq j-1$, either $l \not\equiv 0 \pmod{i}$ or $j - l \not\equiv 0 \pmod{i}$ because $j \not\equiv 0 \pmod{i}$. By (3.1.7) and the induction assumption, we have $b_l S_{j-l} = 0$ for $1 \leq l \leq j-1$. Hence $S_j + j b_j = 0$. From (3.1.7) again, $b_j = 0$. This proves the claim.

Therefore, we aim to prove (3.1.7) and hence we have the next proposition.

Proposition 3.1.6. *If the set $\{j : S_j \neq 0, i \nmid j\}$ is empty then Conjecture 2.3.3 is true.*

Proof. Since $\{j : S_j \neq 0, i \nmid j\}$ is empty, we have $b_l = 0$ for all $l \not\equiv 0 \pmod{i}$ or by (3.1.1)

$$\begin{gathered} a_0 = \cdots = a_{i-1} \\ a_i = \cdots = a_{2i-1} \\ \vdots \\ a_{(N/i-1)i} = \cdots = a_{N-1}. \end{gathered}$$

It then follows that

$$P(x) = (1 + x + \cdots + x^{i-1})F(x^i)$$

where the coefficients of $F(x)$ are $+1$ or -1. Indeed, since $F(x^i)$ is a factor of $P(x)$, so $F(x)$ is cyclotomic. Now the induction assumption applies to $F(x)$ and by induction on the degree of the polynomials, we prove the proposition. □

From now on, we may assume the set $\{j : S_j \neq 0, i \nmid j\}$ is non-empty and let j be the least positive integer in this set. From the definition of j, if there exists $l < j$ such that $S_l \neq 0$, then $i|l$.

Lemma 3.1.7. *We have $j \mid N$.*

Proof. Since $S_j \neq 0$, so $2^{t+1} \nmid j$ by Lemma 3.1.4 and hence by Lemma 3.1.3, $S_j = S_{(j,N)}$. So, if $(j, N) < j$ then by the definition of j, $i \mid (j, N)$. It follows that $i \mid j$ which contradicts the definition of j. Therefore, $(j, N) = j$ and hence $j \mid N$. □

Lemma 3.1.8. *For any $k < j$ and $i \nmid k$, $b_k = 0$.*

Proof. For any $k < j$ and $i \nmid k$, by the definition of j, we have $S_k = 0$. By Newton's identity,

$$S_k + b_1 S_{k-1} + \cdots + b_{i-1} S_{k-(i-1)} + b_i S_{k-i} + b_{i+1} S_{k-(i+1)} + \cdots + b_{k-1} S_1 + k b_k = 0.$$

Since $i \nmid k$, so either $i \nmid l$ or $i \nmid k - l$. That is either $b_l = 0$ or $S_{k-l} = 0$ by the definition of j and the induction assumption. So $S_k + k b_k = 0$ and hence $b_k = 0$. □

Lemma 3.1.9. *We have $S_j = -j b_j$.*

Proof. By Newton's identity, we have

$$S_j + \sum_{l=1}^{j-1} b_l S_{j-l} + j b_j = 0$$

and by Lemma 3.1.8,

$$S_j + \sum_{0<l<j/i} b_{il} S_{j-il} + j b_j = 0.$$

But $i \nmid j - il$ because $i \nmid j$, $S_{j-il} = 0$. Thus $S_j + j b_j = 0$ and hence $S_j = -j b_j$. □

Lemma 3.1.10. *We have $S_{i+j} \neq 0$*

Proof. By Newton's identity,

$$S_{i+j} + \sum_{l=1}^{i-1} b_l S_{i+j-l} + b_i S_j + \sum_{l=1}^{j-i-1} b_{i+l} S_{j-l} + b_j S_i + \sum_{l=1}^{i-1} b_{j+l} S_{i-l} + (i + j) b_{i+j} = 0.$$

Now we note that since $b_1 = \cdots = b_{i-1} = 0$, so

$$\sum_{l=1}^{i-1} b_l S_{i+j-l} = 0.$$

For $1 \leq l \leq j-i-1$, then $i+l < j$. So if $i \nmid l$, then by Lemma 3.1.8, $b_{i+l} = 0$; if $i|l$ then $i \nmid j-l$ and by the definition of j, we have $S_{j-l} = 0$. Thus

$$\sum_{l=1}^{j-i-1} b_{i+l} S_{j-l} = 0.$$

For $1 \leq l \leq i-1$, we have $i \nmid i-l$ and hence $S_{i-l} = 0$. We conclude that

$$S_{i+j} + b_j S_i + b_i S_j + (i+j) b_{i+j} = 0.$$

Since $S_i = 2i$ and $S_j = -jb_j$ by Lemma 3.1.9 and (3.1.6), we get

$$S_{i+j} = -(i+j)(2b_j + b_{i+j}).$$

If $S_{i+j} = 0$ then $2b_j + b_{i+j} = 0$. Since $b_N = \pm 1$, so $i+j \neq N$ and hence $b_{i+j} \in \{-2, 0, +2\}$.

Because $S_j = -jb_j \neq 0$, so $b_{i+j} \neq 0$ and hence

$$b_{i+j} = \pm 2 \equiv 2 \pmod{4}.$$

Therefore,

$$\begin{aligned} 0 &\equiv b_{i+j} + 2b_j \pmod{4} \\ &\equiv 2 + 2b_j \pmod{4}. \end{aligned}$$

It follows that $1 + b_j \equiv 0 \pmod{2}$ and hence $b_j \equiv\!\Box 1 \pmod{2}$. This contradicts $b_j \in \{-2, 0, +2\}$. □

Lemma 3.1.11. *We have $i+j \mid N$.*

Proof. Since $S_{i+j} \neq 0$, so $2^{t+1} \nmid N$ by Lemma 3.1.4 and $S_{i+j} = S_{(N,i+j)}$ by Lemma 3.1.3. If $k = (N, i+j) < i+j$ then since $i+j < 2j$, every proper divisor of $i+j$ is less than j. In particular, $k < j$ but $S_k = S_{i+j} \neq 0$ by the definition of j. So $i|k$ and hence $i|j$. This contradiction shows that $k = (N, i+j) = i+j$ and $i+j|N$. □

In summary, we let

$$b_0 = 1, b_1 = \cdots = b_{i-1} = 0, b_i = -2.$$

We have

$$S_1 = \cdots = S_{i-1} = 0, \quad S_i = 2i$$

and $i|N$. Suppose the set $\{j : S_j \neq 0, i \nmid j\}$ is non-empty and let j be the least positive integer in this set. Then we have $j|N, i+j|N$ and $S_j = -b_j \neq 0, S_{i+j} \neq 0$. We also have for any $l < j$ and $i \nmid l$, $S_l = 0$.

3.2 Littlewood cyclotomic polynomials of even degree

In this section, we recover Borwein-Choi's result Theorem 2.3.1.

Proposition 3.2.1. *Suppose N is odd. Then $S_{2k}=0$ for $1 \le k \le N-1$.*

Proof. Since N is odd, from (3.1.3) we have

$$Q(x)=\prod_{d|N}\Phi_d^{e(d)}(x)\Phi_{e(2d)}^{e(2d)}(x),$$

where $e(d)+e(2d)=1$. If $1 \le k \le N-1$, then

$$\begin{aligned} S_{2k} &= \sum_{d|N}(e(d)c_d(2k)+e(2d)c_{2d}(2k)) \\ &= \sum_{d|N}(e(d)+e(2d))c_d(k) \\ &= \sum_{d|N}c_d(k) \\ &= 0 \end{aligned}$$

by (1.5.3) and Lemma 1.5.3. □

Theorem 3.2.2. *Suppose N is odd. A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x)=\pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1p_2\cdots p_{r-1}}),$$

where $N=p_1p_2\cdots p_r$ and the p_i are primes, not necessarily distinct.

Proof. It is clear that if $P(x)$ is in the form of (2.3.1), then $P(x)$ is a cyclotomic Littlewood polynomial. Conversely suppose that $P(x)$ is a cyclotomic Littlewood polynomial. As before we may assume that $a_0=a_1=\cdots=a_{i-1}=1$ and $a_i=-1$. So $S_i \neq 0$ as we proved before. Now let $A=\{j : S_j \neq 0, i \nmid j\}$ and if A is empty by Proposition 3.1.6 we are done. Suppose A is not empty, let j be the least positive integer in A. By Lemma 3.1.10, $S_{i+j}\neq 0$ as well as S_i and S_j. By Proposition 3.2.1 $i, j, i+j$ must be all odd, but this is impossible. So A must be empty. Therefore, by Proposition 3.1.6, this proves the theorem. □

3.3 Separable Littlewood Cyclotomic Polynomials

In [10], R. Thangadurai proves that Conjecture 2.3.3 is true for separable polynomials of degree $N-1=2^rp^l-1$. There is apparently a typographical error in the abstract of [10] where the word "separable" is forgotten to be written. In this section we prove that Conjecture 2.3.3 is true for all separable polynomials, which improves Thangadurai's result. In the next section we will give a proof for polynomials of degree $N-1=2^r p^l-1$ without the restriction of being separable.

Theorem 3.3.1. *Conjecture 2.3.3 is true for separable Littlewood cyclotomic polynomials.*

Proof. Suppose $P(x)$ is a separable cyclotomic Littlewood polynomial of degree $N-1$ with $N=2^tM$, $t \geq 0$ and odd M. Then

$$P(x) = \prod_{d|M} \Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)} \cdots \Phi_{2^{t+1}d}^{e(2^{t+1}d)}$$

where $e(l)$ is either 0 or 1 (because $P(x)$ is separable) and satisfies

$$e(d) + \sum_{i=1}^{t+1} 2^{i-1}e(2^i d) = \begin{cases} 2^t & \text{if } d \mid M, d>1; \\ 2^t-1 & \text{if } d=1. \end{cases}$$

For $d=1$, we have

$$e(1)+e(2)+2e(4)+\cdots+2^t e(2^{t+1}) = 2^t-1.$$

Since $e(j)$ is either 0 or 1, so $e(2^{t+1})=0$ and

$$e(1)+e(2)=e(4)=e(8)=\cdots=e(2t)=1.$$

Hence by Theorem 1.4.5 (i),

$$\begin{aligned} \Phi_1^{e(1)}(x)\Phi_2^{e(2)}(x)\cdots\Phi_{2^{t+1}}^{e(2^{t+1})}(x) &= \Phi_1^{e(1)}(x)\Phi_2^{e(2)}(x)\Phi_4(x)\cdots\Phi_{2^t}(x) \\ &= \Phi_2(\pm x)F_1(x^2) \end{aligned}$$

for some polynomial $F_1(x)$ in $\mathbb{Z}[x]$. For $d>1$, we have

$$e(d)+e(2d)+2e(4d)+\cdots+2^t e(2^{t+1}d) = 2^t.$$

So either

$$e(2^{t+1}d)=1 \text{ and } e(d)=\cdots=e(2^t d)=0$$

or

$$e(2^{t+1}d)=0 \text{ and } e(d)=\cdots=e(2^t d)=1.$$

So $\Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)}(x)\cdots\Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x)$ is either

$$\Phi_{2^{t+1}d}(x) = \Phi_{2d}(x^{2^t})$$

or

$$\Phi_d(x)\Phi_{2d}(x)\cdots\Phi_{2^t d}(x) = F_2(x^2)$$

for some $F_2(x)$ in $\mathbb{Z}[x]$. In either case, it is in the form of $F_2(x^2)$ for some $F_2(x)$ in $\mathbb{Z}[x]$. Therefore,

$$P(x) = \Phi_2(\pm x)F(x^2)$$

for some polynomial $F(x)$ in $\mathbb{Z}[x]$. Hence induction applies to $F[x]$ and this proves the theorem. □

3.4 Cyclotomic Littlewood polynomials of odd degree

In this section, we prove that Conjecture 2.3.3 is true for some special cases of N.

Theorem 3.4.1. *Conjecture 2.3.3 is true when N is a power of 2.*

Proof. By Corollary 2.2.2, we have

$$P(x) = \Phi_1^{e(1)}(x)\Phi_2^{e(2)}\cdots\Phi_{2^{\iota+1}}^{e(2^{\iota+1})}.$$

Again we assume $a_0 = a_1 = 1$. Since $\Phi_1(x)\Phi_2(x) = x^2 - 1$ and

$$\Phi_{2^l}(x) = \Phi_2(x^{2^{l-1}})$$

for $l \geq 2$, we have $e(2) - e(1) = 1$ and hence

$$P(x) = \Phi_2(x)R(x^2),$$

for some cyclotomic Littlewood polynomial $R(x)$. Therefore by induction, $P(x)$ satisfies (2.3.3). $\square$

Theorem 3.4.2. *Conjecture 2.3.3 is true for the Littlewood cyclotomic polynomials of degree $N-1$ where $N = 2^\alpha p^\beta$ and p is an odd prime.*

Proof. Let i and j be as above. Since $i, j \mid N$, we have $i = 2^{\alpha_1}p^{\beta_1}$ and $j = 2^{\alpha_2}p^{\beta_2}$ where $0 \leq \alpha_1, \alpha_2 \leq \alpha$ and $0 \leq \beta_1, \beta_2 \leq \beta$. Since $i \nmid j$, either $\alpha_1 > \alpha_2$ or $\beta_1 > \beta_2$.

If $i = 2^{\alpha_1}$ then $\alpha_2 < \alpha_1$ (since $\beta_1 = 0$) and $\beta_2 \neq 0$ otherwise $j \mid i$. Then

$$\begin{aligned} i + j &= 2^{\alpha_1} + 2^{\alpha_2}p^{\beta_2} \\ &= 2^{\alpha_2}(2^{\alpha_1-\alpha_2} + p^{\beta_2}). \end{aligned}$$

By Lemma 3.1.11, $i + j \mid N$, but $2^{\alpha_2}(2^{\alpha_1-\alpha_2} + p^{\beta_2}) \nmid 2^\alpha p^\beta$. So by Proposition 3.1.6, Conjecture 2.3.3 is true for $N = 2^\alpha p^\beta$. $\square$

We will end this thesis by proving Theorem 3.4.4 which gives a general critetion to verify Conjecture 2.3.3 in particular cases. Before stating Theorem 3.4.4, we prove

Lemma 3.4.3. *We can find divisors of N, $i_1, \cdots, i_n$, all greater than 1, such that if $S_k \neq 0$ then $i_l \mid k$ for some $1 \leq l \leq n$.*

Proof. Suppose that $S_{a_1}, \cdots, S_{a_m}$ are all nonzero S_k and $a_1 < a_2 < \cdots < a_m$. We give an algorithm to find $i_1, \cdots, i_n$, divisors of N, such that if $S_k \neq 0$ then $i_l \mid k$ for some $1 \leq l \leq n$.
Put $i_1 = a_1$. By Lemma 3.1.5, $a_1 = i$ and $a_1 \mid N$.

Now suppose that $i_1, \cdots, i_l$ are chosen and all of them divide N. If for every $S_k \neq 0$, one can find x, $1 \leq x \leq l$, such that $i_x \mid k$, we will stop here. Otherwise pick the least j such that $S_{a_j} \neq 0$

and $i_1 \nmid a_j, \cdots, i_l \nmid a_j$. Put $i_{l+1} = a_j$. By Lemma 3.1.4, since $S_{i_{l+1}} \neq 0$, so $2^{t+1} \nmid i_{l+1}$ and by Lemma 3.1.3, we have $S_{(N,i_{l+1})} = S_{i_{l+1}}$. Suppose that $(N, i_{l+1}) < i_{l+1}$ so at least one of $i_1, i_2 \cdots, i_l$ must divide (N, i_{l+1}) by the way that we choose i_{l+1}. This contradicts $i_1 \nmid a_j, \cdots, i_l \nmid a_j$. Therefore $(N, i_{l+1}) = i_{l+1}$ and $i_{l+1} \mid N$. Since N has only finitely many divisors, this process must stop at some point. □

Let $i_1, \cdots, i_n$ be the same as in Lemma 3.4.3 and $i = gcd(i_1, \cdots, i_n)$. Then we have

$$\begin{aligned} S_1 = \cdots = S_{i-1} = 0 \\ S_{i+1} = \cdots = S_{2i-1} = 0 \\ \vdots \\ S_{(N/i-1)i+1} = \cdots = S_{N-1} = 0 \end{aligned}$$

i.e.

$$S_j = 0 \text{ for all } j \not\equiv 0 \pmod{i}.$$

Theorem 3.4.4. *Let $i_1, \cdots, i_n$ be as in Lemma 3.4.3. If $gcd(i_1, \cdots, i_n) \neq 1$ then Conjecture 2.3.3 is true.*

Proof. Let $i = gcd(i_1, \cdots, i_n) \neq 1$. Since $\{j : S_j \neq 0, i \nmid j\}$ is empty, then Conjecture 2.3.3 is true by Proposition 3.1.6. □

Bibliography

[1] G. Bachman, On the coefficients of cyclotomic polynomials, Mem. Amer. Math. Soc. 106 (1993), no. 510, vi+80 pp.

[2] P. Borwein and K.K. Choi, On Cyclotomic Polynomials with ±1 Coefficients, Experiment. Math. 9 (2000), no. 1, 153-158.

[3] P.Borwein and T. Erdelyi, Polynomials and Polynomial Inequalities, GTM 161, Springer-Verlag, New York, 1995.

[4] N.J.de Bruijn, On Mahler's partition problems, Indagationes Math., 10 (1948), 210-220.

[5] T.W Hungerford, Algebra, GTM 73. Springer-Verlag, New York, 1996.

[6] A.L. Kostrikin, Introduction to Algebra, Springer-Verlag, New York, 1982.

[7] R. Lidi and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Cambridge, 1994.

[8] M. Ram Murty, Problems in analytic number theory, GTM 206. Springer-Verlag, New York, 2001.

[9] J.Suzuki, On coefficients of cyclotomic polynomials, Proc. Japan Acad. Ser. A Math. Sci. 63(1987), 279-280.

[10] R. Thangadurai, A note on the conjecture of Borwein and Choi, Arch. Math. (Basel) 78 (2002), no. 5, 386-396.

[11] D. H. Lehmer, Some properties of cyclotomic polynomials, J. Math. Anal. Appl. 15 (1966), 105-117.

[12] P. Moree and H. Hommerson,Value distribution of Ramanujan sums and of cyclotomic polynomial coefficients, Master thesis, Korteweg-de Vries Institute (University of Amsterdam), 2003.