ON THE COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

A thesis submitted in partial fulfillment of the requirements
For the degree of Master of Science
in Mathematics

By

Gregory B. Imhoff

August 2013
The thesis of Gregory B. Imhoff is approved:

__________________________________  
Mary Rosen, Ph.D  Date

__________________________________  
Daniel Katz, Ph.D  Date

__________________________________  
Jerry Rosen, Ph.D, Chair  Date

California State University, Northridge
Dedication

To my parents, Mark and Cathy.
# Table of Contents

Copyright ii
Signature page iii
Dedication iv
List of Tables vii
List of Figures viii
Abstract ix

1 Introduction 1
   1.1 Background . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
   1.2 Basic Definitions and Preliminaries . . . . . . . . . . . . . . . . . . . . . 2
      1.2.1 Euler’s Totient Function . . . . . . . . . . . . . . . . . . . . . . 2
      1.2.2 The Möbius Function and Inversion Formula . . . . . . . . . . . . 4
   1.3 Fundamental Properties of Cyclotomic Polynomials . . . . . . . . . . . . . 5
      1.3.1 The Irreducibility of $\Phi_n$ . . . . . . . . . . . . . . . . . . . 7
      1.3.2 Cyclotomic Extensions . . . . . . . . . . . . . . . . . . . . . . . . 8
      1.3.3 Formulas for Computing $\Phi_n$ . . . . . . . . . . . . . . . . . . 8

2 Coefficients 12
   2.1 Properties of the Coefficients of Cyclotomic Polynomials . . . . . . . . . . 13
   2.2 Bounds on $A(n)$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
   2.3 Computational Problems . . . . . . . . . . . . . . . . . . . . . . . . . . . 17

3 Cyclotomic Polynomials of Orders 1 and 2 20
   3.1 Prime Cyclotomic Polynomials . . . . . . . . . . . . . . . . . . . . . . . 20
   3.2 Binary Cyclotomic Polynomials . . . . . . . . . . . . . . . . . . . . . . 20
   3.3 The Coefficients of $\Phi_{3p}(x)$ and $\Phi_{5p}(x)$ . . . . . . . . . . . . . 22

4 Cyclotomic Polynomials of Order 3 25
   4.1 Determining $A(3pq)$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25
   4.2 The Coefficients of $\Phi_{pq}(x)$ . . . . . . . . . . . . . . . . . . . . . 31
   4.3 Beiter’s Conjecture . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33
   4.4 Flat Cyclotomic Polynomials of Order 3 . . . . . . . . . . . . . . . . . . 35
   4.5 Inverse Cyclotomic Polynomials . . . . . . . . . . . . . . . . . . . . . . 37
   4.6 Pseudocyclotomic Polynomials . . . . . . . . . . . . . . . . . . . . . . . 40

5 Cyclotomic Polynomials of Order 4 43
   5.1 Flat Cyclotomic Polynomials of Order 4 . . . . . . . . . . . . . . . . . . . 43
   5.2 Higher Order $\Phi_n(x)$ . . . . . . . . . . . . . . . . . . . . . . . . . . . 44
6 The Structure of $\Phi_{pn}(x)$
   6.1 Re-examining $\Phi_{pq}(x)$ ........................................ 46
   6.2 Redefining $\Phi_{np}$ ................................................. 48
   6.3 Reconstructing $V(np)$ ............................................. 50
   6.4 Revisiting Periodicity .............................................. 54
   6.5 Proving Flatness ...................................................... 57
      6.5.1 Proof of Theorem 4.4.4 ..................................... 58
      6.5.2 Proof of Theorem 4.4.5 ..................................... 59
      6.5.3 Proof of Theorem 5.1.2 ..................................... 60

7 Open Questions
   7.1 Classifying Flat Cyclotomic Polynomials ...................... 62
   7.2 Height Reduction ..................................................... 62

References 67
List of Tables

2.1 $B(k)$ for $1 \leq k \leq 30$ .................................................. 18
2.2 The least $n$ for which $A(n) > n^c$ ................................. 19

4.1 Counterexamples for $q = kp \pm 1$ ................................. 28
4.2 Counterexamples for $q = kp \pm 2$ ................................. 29
4.3 The case $p \equiv q \equiv 1 \pmod{3}$ ................................. 30
4.4 The case $p \equiv q \equiv 2 \pmod{3}$ ................................. 30
4.5 The case $p \equiv 2, q \equiv 1 \pmod{3}$ ................................. 30
4.6 The case $p \equiv 1, q \equiv 2 \pmod{3}$ ................................. 31

5.1 Examples of the case $A(3n) < A(n)$ for $n < 20000$ .......... 44
List of Figures

3.1 L diagram for $\Phi_{55}(x)$ ............................................. 22

6.1 L diagram for $(1 + x)\Phi_{55}(x)$ ..................................... 47
6.2 L diagram for $(1 + x + x^2)\Phi_{55}(x)$ ............................... 47
ABSTRACT

ON THE COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

A thesis submitted in partial fulfillment of the requirements
For the degree of Master of Science
in Mathematics

By

Gregory B. Imhoff

The $n$th cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial of a primitive $n$th root of unity. The order of $\Phi_n$ is the number of distinct odd prime factors of $n$ and the height of $\Phi_n = \sum a_n(k)x^k$ is $A(n) = \max_k |a_n(k)|$, the maximum absolute value of its coefficients. Polynomials of height 1 are called flat. In this thesis, we will explore the functions $a_n(k)$ and $A(n)$, establishing all the known results. In particular, we will look at the cases when $\Phi_n(x)$ is of order less than 5, since we have infinite families of $\Phi_n(x)$, up to order 4, where $A(n) = 1$, but there are no known cases of order 5 or higher. Much of the literature on the topic has focused on the order 3 case, which is the simplest non-trivial case. There has been a surge of interest recently in the study of the coefficients of cyclotomic polynomials, with much of the most significant progress occurring within the last decade. We survey much of the existing literature, including the most current progress toward classifying all flat cyclotomic polynomials. We conjecture that there are no flat cyclotomic polynomials of order 5 or greater.
Chapter 1

Introduction

1.1 Background

Cyclotomy refers to the sectioning of a circle into arcs of equal length with the use of only a straightedge and compass, a problem in geometry of classical origin. Gauss was perhaps the first to see this as an algebraic problem, with his discovery of the constructability of the regular 17-gon in 1796 when he was 19 years old. The \( n \) vertices of a regular \( n \)-gon can be represented in the complex plane by the \( n \)th roots of unity, or the complex solutions to the equation \( x^n - 1 = 0 \). The irreducible factors of \( x^n - 1 \) are the cyclotomic polynomials. The \( n \)th cyclotomic polynomial is thus the minimal polynomial over the rationals of a primitive \( n \)th roots of unity. A root of \( x^n - 1 \) is primitive if it is not a root of \( x^d - 1 \) where \( d \) is any proper divisor of \( n \). Moreover, all of the \( n \)th roots of unity are generated by a primitive \( n \)th root of unity. Amazingly, we can determine the constructability of a regular \( n \)-gon by understanding the nature of the class of extensions known as cyclotomic extensions, which are extensions of the rational field containing a primitive \( n \)th root of unity. See [20] for more on the constructability of the regular \( n \)-gon.

Cyclotomic polynomials were first studied by Vandermonde in 1771 in [48], although many of the early results were first published by Gauss in 1801 in [28]. Gauss defined the \( p \)th cyclotomic polynomial as \( \Phi_p(x) = (x^p - 1)/(x - 1) = 1 + x + \cdots + x^{p-1} \) when \( p \) is prime. Using the knowledge that the roots of the \( p \)th cyclotomic polynomial are the primitive \( p \)th roots of unity and his theory of periods, Gauss showed the \( p \)th cyclotomic polynomial to be irreducible over the rationals. This proof was greatly simplified with Eisenstein’s criterion on irreducibility, where one can easily verify that \( \Phi_p(x + 1) = [(x + 1)^p - 1]/x \) is irreducible and hence \( \Phi_p(x) \) is irreducible. It was not until Kroneker in 1854 and later Dedekind in 1870 that a proof of the irreducibility of \( \Phi_n(x) \) for composite \( n \) was published. See [50] for several proofs replicating the styles of Gauss, Eisenstein, Kronecker, Dedekind, Landau, and Schur.

For many years, it was assumed that the coefficients of the \( n \)th cyclotomic polynomial were in the set \( \{0, \pm 1\} \), as is the case for the first 104 cyclotomic polynomials. But when \( n \) is the product of 3 or more distinct, odd primes, we begin to see examples of cyclotomic polynomials with larger coefficients. As it turns out, every integer occurs as a coefficient in some cyclotomic polynomial. A great deal of research has been published regarding the size of the coefficients of the \( n \)th cyclotomic polynomial. In 1946, Erdős [22] showed that there are infinitely many \( n \) where the coefficients of the \( n \)th cyclotomic polynomial can exceed \( n^c \) for any positive constant \( c \). Computational problems, however, prevent one from easily being able to study those cyclotomic polynomials with very large coefficients. In recent years, there have been attempts to explore the coefficients of cyclotomic polynomials using powerful computing techniques. Arnold and Monagan [2] have compiled a great deal of data, finding many examples of cyclotomic polynomials with unusually large coefficients.
On the other hand, there are infinitely many \( n \) where the coefficients of the \( n \)th cyclotomic polynomial do not exceed 1 in absolute value, for instance when \( n \) is prime, we know its coefficients are all 1. Recently, there has been efforts to classify all \( n \) for which the coefficients of the \( n \)th cyclotomic polynomial are in the set \{ \(-1, 0, 1\) \}. Currently, due to the work of Kaplan [32, 33] and Elder [21], we know of infinite families of such polynomials for \( n \) with no more than 4 distinct, odd primes in their factorization. There are no known \( n \) with 5 or more distinct, odd prime divisors such that the \( n \)th cyclotomic polynomial has coefficients contained in the set \{ \(0, \pm 1\) \}; it is conjectured that none exist.

1.2 Basic Definitions and Preliminaries

An \( n \)th root of unity is a complex number \( \zeta \) such that \( \zeta^n = 1 \). Any such \( \zeta \) is of the form \( \zeta = e^{2\pi ik/n} \) for some integer \( k \) with \( 0 \leq k \leq n - 1 \). Let \( \mu_n \) denote the set of \( n \)th roots of unity. Note that \( \mu_n \) forms a cyclic group under multiplication isomorphic to the additive group \( \mathbb{Z}/n\mathbb{Z} \) via \( [k] \mapsto e^{2\pi ik/n} \). An \( n \)th root of unity is called primitive if it generates the cyclic group \( \mu_n \). It is worth noting that \( \zeta \in \mu_n \) is primitive if and only if \( \text{ord}(\zeta) = n \). And if \( \zeta \in \mu_n \) is primitive, then \( \zeta^k \) is primitive if and only if \( \gcd(k,n) = 1 \). So we say that \( \zeta \in \mu_n \) is primitive if it can be written as \( \zeta = e^{2\pi ik/n} \) where \( \gcd(k,n) = 1 \). The \( n \)th cyclotomic polynomial is the monic polynomial whose roots are the primitive \( n \)th roots of unity.

\[
\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitive}}} (x - \zeta) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} (x - e^{2\pi ik/n})
\]  

1.2.1 Euler’s Totient Function

The degree of \( \Phi_n(x) \) is determined by \( \varphi(n) \), Euler’s totient function. Let \( \varphi : \mathbb{N} \to \mathbb{N} \) be defined such that \( \varphi(n) \) represents the number of integers \( k \) satisfying \( 1 \leq k \leq n \) and \( \gcd(k,n) = 1 \). The function \( \varphi(n) \) essentially counts the number of primitive \( \zeta \in \mu_n \).

Euler’s totient function also represents the order of the multiplicative group \( U(n) \). The invertible elements of a ring \( A \) are often called units, and they form a group under the multiplicative law of \( A \). Let \( U(n) \) denote the group of units of the ring \( \mathbb{Z}/n\mathbb{Z} \). An element \( k \) in \( \mathbb{Z}/n\mathbb{Z} \) is invertible if and only if \( k \) is relatively prime to \( n \). Therefore, we can define the group of units of the ring \( \mathbb{Z}/n\mathbb{Z} \) as

\[
U(n) = \{ k \in \mathbb{Z}/n\mathbb{Z} : \gcd(k,n) = 1 \},
\]

hence \( |U(n)| = \varphi(n) \).

Proposition 1.2.1. Let \( n \in \mathbb{N} \).

(a) Then \( n = \sum_{d|n} \varphi(d) \);

(b) If \( \gcd(m,n) = 1 \), then \( U(nm) \cong U(n) \times U(m) \) and \( \varphi(nm) = \varphi(n)\varphi(m) \);

(c) If \( p \) is prime, then \( \varphi(p^k) = p^k - p^{k-1} \);
(d) If \( n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \) is the prime factorization of \( n \), then

\[
\varphi(n) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1) = n \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right). \tag{1.3}
\]

**Proof.**

(a) Let \( P_d = \{ \zeta \in \mu_d | \text{ord}(\zeta) = d \} \) and note that \( |P_d| = \varphi(d) \). Then \( \{P_d\}_{d|n} \) is a partition of \( \mu_n \). Therefore,

\[
n = |\mu_n| = \sum_{d|n} |P_d| = \sum_{d|n} \varphi(d).
\]

(b) There is an isomorphism \( \alpha : U(nm) \to U(n) \times U(m) \) defined by

\[
\alpha([a]_{nm}) = ([a]_n, [a]_m).
\]

Since the group operation in \( U(n) \) is the multiplicative operation from the ring \( \mathbb{Z}/n\mathbb{Z} \), we have multiplication in the group \( U(n) \times U(m) \) given by

\[
([a]_n, [b]_m) \cdot ([b]_n, [c]_m) = ([a]_n[b]_n, [a]_m[c]_m) = ([ac]_n, [bc]_m),
\]

hence \( \alpha \) is a group homomorphism.

This is well-defined since \([a]_nm = [b]_nm \) implies that \( nm|a - b \), thus \( n|a - b \) and \( m|a - b \) since \( \gcd(m,n) = 1 \). So \([a]_n = [b]_n \) and \([a]_m = [b]_m \).

To see that \( \alpha \) is surjective, let \((a]_n, [b]_m) \in U(n) \times U(m)\). Then since \( \gcd(m,n) = 1 \), there is \( M, N \in \mathbb{Z} \) such that \( nN + mM = 1 \). So we have

\[
\alpha([amM + bnN]_{nm}) = ([amM + bnN]_n, [amM + bnN]_m) = ([amM]_n, [bnN]_m) = ([a(1-nN)]_n, [b(1-mM)]_m) = ([a]_n, [b]_m).
\]

It is worth noting that this also follows from the Chinese Remainder Theorem.

To get injectivity, take \([a]_{nm} \in \ker \alpha \). Then \(([a]_n, [a]_m) = (0,0) \) means that \( n|a \) and \( m|a \), therefore \( nm|a \) since \( \gcd(m,n) = 1 \). Hence \([a]_{nm} = 0 \), giving \( \ker \alpha = \{0\} \).

So we now have \( U(nm) \cong U(n) \times U(m) \), giving

\[
\varphi(nm) = |U(nm)| = |U(n) \times U(m)| = \varphi(n)\varphi(m).
\]

(c) Since \( p \) is prime, \( \gcd(p^k, m) \in \{1, p, p^2, \ldots, p^k\} \). So we see there are exactly \( p^k \) possible values of \( m \) such that \( 1 \leq m \leq p^k \) and exactly \( p^{k-1} \) values of \( m \) such that \( \gcd(p^k, m) \neq 1 \). Therefore there are exactly \( p^k - p^{k-1} \) values of \( m \) satisfying \( 1 \leq m \leq p^k \) and \( \gcd(p^k, m) = 1 \).
(d) By the previous results,

\[ \varphi \left( \prod_{i=1}^{k} p_i^{e_i} \right) = \prod_{i=1}^{k} \varphi(p_i^{e_i}) = \prod_{i=1}^{k} p_i^{e_i} - p_i^{e_i-1} = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1) \]

\[ = \prod_{i=1}^{k} p_i^{e_i}(1 - \frac{1}{p_i}) = \prod_{i=1}^{k} p_i^{e_i} \prod_{i=1}^{k} (1 - \frac{1}{p_i}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}). \]

\[ \square \]

Example 1.2.1. \( U(8) = \{1, 3, 5, 7\} \) and \( \varphi(8) = 4 \). Each element is of order 2, so \( U(8) \cong (\mathbb{Z}/2\mathbb{Z})^2 \).

1.2.2 The Möbius Function and Inversion Formula

Let \( \mu : \mathbb{N} \rightarrow \{-1, 0, 1\} \) be the Möbius function defined by

\[ \mu(n) = \begin{cases} 
1 & \text{if } n = 1, \\
0 & \text{if } n \text{ contains a square factor,} \\
(-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes.}
\end{cases} \]

Proposition 1.2.2. If \( \gcd(n, m) = 1 \), then \( \mu(nm) = \mu(n)\mu(m) \).

Proposition 1.2.3. If \( n > 1 \), then \( \sum_{d|n} \mu(d) = 0 \).

We will not prove Propositions 1.2.2 or 1.2.3; see [24] for proofs.

Theorem 1.2.4 (Möbius Inversion Formula). Let \( G \) be an abelian group written additively. Let \( g : \mathbb{N}^* \rightarrow G \) be a map, and let \( f : \mathbb{N}^* \rightarrow G \) be the map defined by \( f(n) = \sum_{d|n} g(d) \).

Then

\[ g(n) = \sum_{d|n} \mu(d) f \left( \frac{n}{d} \right) = \sum_{d|n} \mu \left( \frac{n}{d} \right) f(d). \] (1.4)

Proof.

\[ \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \left( \mu(d) \sum_{e|n/d} g(e) \right) \]

\[ = \sum_{e|n} \left( g(e) \sum_{d|n, e|n/d} \mu(d) \right). \]

For every \( e|n \), we have

\[ \{d : d|n \text{ and } e|n/d\} = \{d : d|n \text{ and } d|n/e\} = \{d : d|n/e\}. \]
Therefore, we have

$$\sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \left( g(e) \sum_{d|n/e} \mu(d) \right) = g(n),$$

since $\sum_{d|n} \mu(d) = 0$ for $e < n$ by Proposition 1.2.3. 

**Remark 1.2.2.** From Proposition 1.2.1(a), if we let $f(n) = n$ and $g(d) = \varphi(d)$, then the Möbius inversion formula gives

$$\varphi(n) = \sum_{d|n} d \mu(n/d). \quad (1.5)$$

**Remark 1.2.3 (Multiplicative Möbius Inversion Formula).** If the group law of $G$ is written multiplicatively, then $f$ is defined by $f(n) = \prod_{d|n} g(d)$ and the inversion formula is written

$$g(n) = \prod_{d|n} f \left( \frac{n}{d} \right)^{\mu(d)} = \prod_{d|n} f(d)^{\mu(n/d)}. \quad (1.6)$$

### 1.3 Fundamental Properties of Cyclotomic Polynomials

The factorization of $x^n - 1$ into cyclotomic polynomials follows from the observation that for $\zeta \in \mu_n$, the $\text{ord}(\zeta)$ divides $|\mu_n|$. Therefore, for each divisor $d$ of $n$ there is $\zeta \in \mu_n$ of order $d$ and any such $\zeta$ generates a cyclic subgroup $\mu_d$ of $\mu_n$ and hence the primitive $d$th roots of unity, where $d|n$, form a partition of $\mu_n$. Thus one can easily observe that the roots of $x^n - 1$ must be the same as the product of the cyclotomic polynomials over all divisors $d$ of $n$.

**Proposition 1.3.1.** $x^n - 1 = \prod_{d|n} \Phi_d(x)$

**Proof.**

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d|n} \left( \prod_{\zeta \in \mu_d, \text{ord}(\zeta) = d} (x - \zeta) \right) = \prod_{d|n} \left( \prod_{\zeta \in \mu_d, \text{primitive}} (x - \zeta) \right) = \prod_{d|n} \Phi_d(x). \blacksquare$$

This is a somewhat convenient computational device, since we can compute $\Phi_n$ in a recursive fashion using the fact that

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}. \quad (1.7)$$
In fact, this gives a direct way of computing $\Phi_p$ for prime $p$, since by equation (1.7) we have that $\Phi_p(x) = (x^p - 1)/\Phi_1(x) = (x^p - 1)/(x - 1)$, so we have

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k = 1 + x + \cdots + x^{p-1}.$$  \hfill (1.8)

**Example 1.3.1.** Proposition 1.3.1 gives the following factorization of $x^n - 1$ for $n \leq 10$.

$$\begin{align*}
x - 1 &= \Phi_1(x), \quad x^2 - 1 = \Phi_2(x)\Phi_1(x) = (x + 1)(x - 1), \\
x^3 - 1 &= \Phi_3(x)\Phi_1(x) = (x^2 + x + 1)(x - 1), \\
x^4 - 1 &= \Phi_4(x)\Phi_2(x)\Phi_1(x) = (x^2 + 1)(x + 1)(x - 1), \\
x^5 - 1 &= \Phi_5(x)\Phi_1(x) = (x^4 + x^3 + x^2 + x + 1)(x - 1), \\
x^6 - 1 &= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x) = (x^2 - x + 1)(x^2 + x + 1)(x + 1)(x - 1), \\
x^7 - 1 &= \Phi_7(x)\Phi_1(x) = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x - 1), \\
x^8 - 1 &= \Phi_8(x)\Phi_4(x)\Phi_2(x)\Phi_1(x) = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1), \\
x^9 - 1 &= \Phi_9(x)\Phi_3(x)\Phi_1(x) = (x^6 + x^3 + 1)(x^2 + x + 1)(x - 1), \\
x^{10} - 1 &= \Phi_{10}(x)\Phi_5(x)\Phi_2(x)\Phi_1(x) \\
&= (x^4 - x^3 + x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)(x + 1)(x - 1). \end{align*}$$

The fact that the coefficients are integral can readily be seen by the fact that $\Phi_n(x)$ in equation (1.7) is inductively a quotient of two monic polynomials in $\mathbb{Z}[x]$, hence $\Phi_n(x)$ is in $\mathbb{Z}[x]$. Here we show this with the use of Gauss’ Lemma as stated below.

**Theorem 1.3.2 (Gauss’ Lemma).** Let $f(x) = \sum_{i=0}^{n} c_i x^i$ and suppose $\text{gcd}(c_0, \ldots, c_n) = 1$. If $f(x) = A(x)B(x)$ where $A(x), B(x) \in \mathbb{Q}[x]$ are non-constant, then $f(x) = a(x)b(x)$ where $a(x), b(x) \in \mathbb{Z}[x]$ with $a(x) = uA(x)$ and $b(x) = u^{-1}B(x)$ for some $u \in \mathbb{Q}$.

**Proof.** Define $m_1$ and $m_2$ as the greatest common divisors of the denominators of the coefficients of $A(x)$ and $B(x)$ respectively so that we have $m_1A(x), m_2B(x) \in \mathbb{Z}[x]$ and factor out the greatest common divisors of their coefficients $\ell_1$ and $\ell_2$ so that we have $m_1A(x) = \ell_1 a(x)$ and $m_2B(x) = \ell_2 b(x)$ where $a(x), b(x) \in \mathbb{Z}[x]$. Then if we let $u = m_1/\ell_1$ and $v = m_2/\ell_2$, we have $f(x) = uva(x)b(x)$.

If we write $a(x) = a_0 + \cdots + a_rx^r$ and $b(x) = b_0 + \cdots + b_s x^s$, then we have $\text{gcd}(a_0, \ldots, a_r) = \text{gcd}(b_0, \ldots, b_s) = 1$ and $n = r + s$. Assume without loss of generality that $uv > 0$ and write it as $uv = m/\ell$ in lowest terms. Then we have $\ell f(x) = ma(x)b(x)$. Since $\ell$ and $m$ are relatively prime, we must have $\ell | c_k$ for $k = 0, \ldots, n$ and hence $\ell = 1$ since $\text{gcd}(c_0, \ldots, c_n) = 1$. To see that $m = 1$, suppose that $m > 1$ and let $p$ be a prime such that $p | m$. Let $i$ be an integer such that $0 \leq i < r$ and $p$ divides $a_0, \ldots, a_{i-1}$ but $p$ does not divide $a_i$ and let $j$ be such that $0 \leq j < s$ and $p$ divides $b_0, \ldots, b_{j-1}$ but does not divide $b_j$. 

---

6
But
\[ mc_{i+j} = \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots, \]
where we see that \( p \) divides the terms to the left and to the right the term \( a_ib_j \) and \( p \) also divides \( mc_k \). Hence \( p|a_ib_j \), contradicting our assumption. \( \blacksquare \)

Thus, we have the following proposition.

**Proposition 1.3.3.** \( \Phi_n(x) \) is monic with integer coefficients.

Another useful construction of \( \Phi_n \) uses the multiplicative form of the Möbius inversion formula 1.6 applied to Proposition 1.3.1 to get an explicit formula for computing \( \Phi_n \) in terms of the Möbius function.

**Proposition 1.3.4.** Let \( \mu \) be the Möbius function. Then
\[
\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{1.9}
\]

**Proof.** Let \( G = \mathbb{C}(x)^* \), the group of non-zero rational functions of a single variable with complex coefficients. Then let \( f : \mathbb{N}^* \to G \) be defined by \( f(n) = x^n - 1 \) and let \( g : \mathbb{N}^* \to G \) be defined by \( g(n) = \Phi_n(x) \). Then by Proposition 1.3.1, \( f(n) = \prod_{d|n} g(d) \) and the multiplicative form of the Möbius inversion formula gives the result. \( \blacksquare \)

### 1.3.1 The Irreducibility of \( \Phi_n \)

To prove the irreducibility of \( \Phi_n(x) \) in \( \mathbb{Z}[x] \), we need to first show that the roots of the minimal polynomial of a primitive \( n \)th root of unity are stable when raised to the \( p \)th power for \( p \nmid n \), as in [24].

**Lemma 1.3.5.** Let \( \zeta \) be a primitive \( n \)th root of unity and let \( F \) be the minimal polynomial of \( \zeta \) over \( \mathbb{Q} \). Then if \( p \) is a prime not dividing \( n \), we have \( F(\zeta^p) = 0 \).

**Proof.** Suppose that \( F(\zeta) = 0 \), but \( F(\zeta^p) \neq 0 \). Then let \( G \) be such that \( x^n - 1 = F(x)G(x) \). Then since \( F(\zeta^p) \neq 0 \), we must have that \( G(\zeta^p) = 0 \). Therefore \( \zeta \) is a root of \( G(x^p) \) and by the minimality of \( F \), we have that \( F(x)|G(x^p) \). Suppose \( G(x^p) = F(x)H(x) \), then by Gauss’ lemma, \( G, H \in \mathbb{Z}[x] \). Let \( \bar{F} \) represent the image of \( F \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \). Then
\[
\bar{G}(x^p) = (\bar{G}(x))^p = \bar{F}(x)\bar{H}(x).
\]
If \( \bar{Q} \) is any irreducible factor of \( \bar{F} \), then \( \bar{Q}(x)|\bar{F}(x)\bar{H}(x) = (\bar{G}(x))^p \) gives \( \bar{Q}(x)|\bar{G}(x) \). So \( (\bar{Q}(x))^2 \) is a factor of \( x^n - 1 \) implies that \( \bar{Q}(x)|x^n - 1 \) and \( \bar{Q}(x)|nx^{n-1} \), but \( x^n - 1 \) is relatively prime to \( nx^{n-1} \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \), giving a contradiction. \( \blacksquare \)

**Proposition 1.3.6.** \( \Phi_n(x) \) is irreducible over \( \mathbb{Q} \).
Proof. Let $\zeta$ be a fixed primitive $n$th root of unity and let $F$ be the minimal irreducible polynomial over $\mathbb{Q}$ with $F(\zeta) = 0$. Then $\Phi_n(\zeta) = 0$ implies that $F(x)$ divides $\Phi_n(x)$.

Now let $j$ be relatively prime to $n$. Then if $j = p_1 \cdots p_r$ is the prime factorization of $j$, we have that each $p_i$ is relatively prime to $n$. So by successive application of the previous lemma, we have that $\zeta^{p_1}, \zeta^{p_1p_2}, \ldots, \zeta^{p_1p_2\cdots p_r}$ are each roots of $F$. So every primitive $n$th root of unity is a root of $F$. So $\Phi_n(x)$ divides $F(x)$.

1.3.2 Cyclotomic Extensions

Cyclotomic extensions are of the form $\mathbb{Q}(\zeta)$ where $\zeta \in \mu_n$ is a primitive $n$th root of unity.

Proposition 1.3.7. Let $n \geq 2$ be an integer and $\zeta$ a primitive $n$th root of unity in $\mathbb{C}$. Then

(a) $\mathbb{Q}(\zeta)$ is a normal extension of $\mathbb{Q}$;
(b) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$;
(c) $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(n)$; in particular this group is abelian.

Proof.

(a) $\mathbb{Q}(\zeta)$ is the splitting field of $x^n - 1$ or of $\Phi_n$ over $\mathbb{Q}$.
(b) The minimal polynomial of $\zeta$ over $\mathbb{Q}$ is $\Phi_n$ which is of degree $\varphi(n)$.
(c) Set $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and let $\sigma \in G$. Then $\sigma$ is determined by $\sigma(\zeta)$ which is a conjugate of $\zeta$ and therefore a primitive $n$th root of unity. Thus it is of the form $\zeta^k$ for some $k$ relatively prime to $n$. Use this to construct the map $\Psi : G \to U(n)$, defined by $\Psi(\sigma) = k$. If $\sigma'(k) = \zeta^{k'}$, we have $(\sigma \circ \sigma')(\zeta) = \sigma(\zeta^{k'}) = \zeta^{kk'}$, so $\Psi(\sigma \circ \sigma') = \Psi(\sigma)\Psi(\sigma')$, which proves that $\Psi$ is a group homomorphism. Also, we see $\Psi$ is injective because if $\Psi(\sigma) = 1$, then $\sigma = \text{id}$. Furthermore, we have

$$|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = |U(n)|.$$  

So $\Psi$ is an isomorphism.

1.3.3 Formulas for Computing $\Phi_n$

The formula in Proposition 1.3.4 leads to several useful reductions.

Proposition 1.3.8. If $p|n$, then $\Phi_{np}(x) = \Phi_n(x^p)$. And if $m$ is product of the distinct prime divisors of $n$, then $\Phi_n(x) = \Phi_m(x^{n/m})$.

Proposition 1.3.9. $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ when $p$ is a prime such that $p \nmid n$.  

Proposition 1.3.10. \( \Phi_{2k}(x) = \Phi_k(-x) \) when \( k > 1 \) is odd.

We will prove these directly from the formula given in Proposition 1.3.4.

Proof of Proposition 1.3.8. When \( p|n \), we can write

\[
\Phi_{np}(x) = \prod_{d|np} (x^{np/d} - 1)^{\mu(d)} = \prod_{d|n} (x^{np/d} - 1)^{\mu(d)} \prod_{d|np} (x^{np/d} - 1)^{\mu(d)}
\]

\[
= \prod_{d|n} ((x^p)^{n/d} - 1)^{\mu(d)} = \Phi_n(x^p),
\]

since \( d|np \) but \( d \nmid n \) implies \( \mu(d) = 0 \).

Now let \( m \) be the product of the distinct prime factors of \( n \). Note that if \( d|n \) but \( d \nmid m \), then \( d \) must contain a square factor and hence this particular \( d \) must be such that \( \mu(d) = 0 \). Therefore,

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

\[
= \prod_{d|m} ((x^{n/m})^{m/d} - 1)^{\mu(d)} = \Phi_m(x^{n/m}).\quad \blacksquare
\]

Proof of proposition 1.3.9. Note that when \( p \) is a prime such that \( p \nmid n \), we have \( \mu(pn) = -\mu(n) \), so

\[
\Phi_{pn}(x) = \prod_{d|pn} (x^{pn/d} - 1)^{\mu(d)} \prod_{d|pn} (x^{pn/d} - 1)^{\mu(d)}
\]

\[
= \prod_{d|n} ((x^p)^{n/d} - 1)^{\mu(d)} \prod_{(d/p)n} (x^{n/d/p} - 1)^{\mu(p/d/p)}
\]

\[
= \Phi_n(x^p) \prod_{q|n} (x^{n/q} - 1)^{-\mu(q)}
\]

\[
= \frac{\Phi_n(x^p)}{\Phi_n(x)}.\quad \blacksquare
\]

Proof of proposition 1.3.10. Note that since \( k \) is odd, \( -x^{k/d} = (-x)^{k/d} \), so
\[
\Phi_{2k}(x) = \frac{\Phi_k(x^2)}{\Phi_k(x)} \\
= \prod_{d | k} (x^{2k/d} - 1)^{\mu(d)}(x^{k/d} - 1)^{-\mu(d)} \\
= \prod_{d | k} (x^{k/d} + 1)^{\mu(d)} \\
= (-1)^\sum_{d | k} \mu(d) \prod_{d | k} (-x^{k/d} - 1)^{\mu(d)} \\
= \prod_{d | k} ((-x)^{k/d} - 1)^{\mu(d)} = \Phi_k(-x).
\]

Thus we see that the \(n\)th cyclotomic polynomial is determined by the \(m\)th cyclotomic polynomial where \(m\) is the largest odd, square-free factor of \(n\).

**Example 1.3.2.** If \(n = p^k\), then \(p\) is the largest square-free factor of \(n\), so

\[
\Phi_n(x) = \Phi_p(x^{p^{k-1}}) = \sum_{i=0}^{p-1} x^{ip^{k-1}}.
\]

(1.10)

**Example 1.3.3.** We can construct an infinite family of flat cyclotomic polynomials with non-zero coefficients alternating between 1 and \(-1\). Suppose that \(p > 2\) is prime. Then

\[
\Phi_{2p^k}(x) = \Phi_p(-x^{p^{k-1}}) = \sum_{i=0}^{p-1} (-1)^i x^{ip^{k-1}}.
\]

(1.11)

Note that the non-zero coefficients here can be made arbitrarily sparse, that is, we can choose \(k\) large enough so that the coefficients are as far apart as we need.

**Example 1.3.4.** The formulae in Proposition 1.3.4, Proposition 1.3.9 or equation (1.7) all give the following for distinct primes \(p\) and \(q\):

\[
\Phi_{pq}(x) = \frac{\Phi_p(x^q)}{\Phi_p(x)} = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.
\]

(1.12)

**Example 1.3.5.** A similar observation can be made when \(n = pqr\) for distinct odd primes \(p, q\) and \(r\), giving

\[
\Phi_{pqr}(x) = \frac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)} = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x - 1)(x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)}.
\]

(1.13)

In studying the coefficients of the \(n\)th cyclotomic polynomial we only need to consider the distinct, odd prime factors of \(n\). Define the order of \(\Phi_n\) to be the number of distinct, odd
prime factors of $n$. We will refer to $n$ as the index of $\Phi_n$. Cyclotomic polynomials of order 1, 2, 3, 4, and 5 are called prime, binary, ternary, quaternary, and quinary, respectively. Here we note that the order is defined in this way because by Proposition 1.3.8 we have that the coefficients of $\Phi_n$ depend only on the largest square-free factor of $n$. Moreover, we only consider odd factors of $n$ since the coefficients of $\Phi_n$ and $\Phi_{2n}$ are the same in absolute value.
Chapter 2

Coefficients

In this chapter, we focus our attention on the function $a_n(k)$, or the $k$th coefficient of $\Phi_n$. The size of these coefficients is a topic that has been heavily researched, yet the behavior of the coefficients of $\Phi_n$ in general is somewhat mysterious. Essentially this is because we have yet to completely understand what makes the coefficients of $\Phi_n$ small, with much of the recent efforts put toward the case when $\Phi_n$ has coefficients contained in the set $\{-1, 0, 1\}$. D.H. Lehmer in [36] put it this way: “The smallness of $a_n(m)$ would appear to be one of the fundamental conspiracies of the primitive $n$th roots of unity. When one considers that $a_n(m)$ is a sum of $(\varphi(n))$ unit vectors (for example 73629072 in the case of $n = 105$ and $m = 7$) one realizes the extent of the cancellation that takes place.”

To refer to the coefficients of a general polynomial in $\mathbb{Z}[x]$, we will use $[x^k]f(x)$ to denote the coefficient of the $x^k$ term of the polynomial $f(x)$. When referring to the coefficients of $\Phi_n$, we use the standard representation of

$$\Phi_n(x) = \sum_k a_n(k)x^k$$

where $a_n(k) = 0$ for $k > \varphi(n)$ and $k < 0$.

Let $V(f(x))$ denote the set of coefficients of the polynomial $f(x)$. The set of coefficients of $\Phi_n(x)$ will be

$$V(n) = \{a_n(k) : k = 0, \cdots, \varphi(n)\}.$$

Throughout this chapter and subsequent chapters, we will survey much of the existing literature on the coefficients of $\Phi_n$. In particular, we are interested in questions regarding the height of the cyclotomic polynomials. Here, we say the height of a polynomial in $\mathbb{Z}[x]$ is the maximum absolute value of its coefficients. Polynomials of height 1 are called flat. We denote the height of $\Phi_n$ as

$$A(n) = \max_k |a_n(k)|.$$

At present, there are many open questions regarding the height of $\Phi_n$, for instance we have yet to completely classify all $n$ for which $A(n) = 1$. Furthermore, numerical evidence suggests that the coefficients of $\Phi_n$ are generally very large, so its become particularly interesting to investigate those cases where $A(n)$ tends to be relatively small for $n$ with three or more distinct, odd prime factors.

As we will see, much of the literature has focused on the simplest non-trivial case. That is the case when $n$ is a product of three distinct, odd primes. The situation becomes
more and more complex as the order of $\Phi_n$ increases, so in general it will be difficult to look at specific examples of higher order cyclotomic polynomials, yet we will look at computational data accumulated from various other sources, namely [1, 34].

2.1 Properties of the Coefficients of Cyclotomic Polynomials

The coefficients of $\Phi_n(x)$ are palindromic. In other words, they are the same whether you read them backwards or forwards. This fact can be deduced from the following reciprocity law.

Theorem 2.1.1 (Reciprocity). Let $n > 1$. Then $\Phi_n(x) = x^{\varphi(n)}\Phi_n(x^{-1})$

Proof. Recall that $\varphi(n) = \sum_{d | n} d\mu(n/d)$ and $\sum_{d | n} \mu(n/d) = 0$ when $n > 1$, therefore

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

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

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

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

$$= \Phi_n(x).$$

By Theorem 2.1.1,

$$x^{\varphi(n)} \sum_{k=1}^{\varphi(n)} a_n(k)x^{-k} = \sum_{k=1}^{\varphi(n)} a_n(k)x^{\varphi(n)-k} = \Phi_n(x).$$

So it is apparent that the coefficient on the term with $x^{\varphi(n)-k}$ is the same as the coefficient on the term with $x^k$, thus we have the so-called self reciprocal property that

$$a_n(k) = a_n(\varphi(n) - k) \quad (2.1)$$

for $k = 0, 1, \ldots, \varphi(n)$.

Given the symmetry in the coefficients, it is only necessary to compute the terms up to degree $\varphi(n)/2$. This shows that $\Phi_n(x)$ is determined by its value modulo $x^{\varphi(n)/2} + 1$ and this computation can be done in the ring $A = \mathbb{Z}[x]/(x^{\varphi(n)/2} + 1)$. So the set of coefficients
of $\Phi_n$ can be written

$$V(n) = \{a_n(k) : 0 \leq k \leq \varphi(n)/2\}.$$ 

When computing $\Phi_n$ for small values of $n$, it appears that the coefficients are relatively small. In general, the coefficients of $\Phi_n(x)$ can become arbitrarily large, especially if $n$ is the product of many distinct prime factors. In 1936, Emma Lehmer in [37] described a way to construct a cyclotomic polynomial with arbitrarily large coefficients, credited to Schur (in a letter to Landau in 1931). Later, Suzuki in 1987 in [47] used this construction to show that every integer is a coefficient in some cyclotomic polynomial. This construction requires $n$ to be the product of as many distinct prime factors as needed, satisfying the following lemma.

**Lemma 2.1.2.** Given any $t \geq 3$, there are $t$ distinct primes $p_1 < p_2 < \cdots < p_t$, such that $p_1 + p_2 > p_t$.

**Proof.** Let $t \geq 3$ and suppose that for any distinct primes satisfying $p_1 < p_2 < \cdots < p_t$ we must have $p_1 + p_2 \leq p_t$ so $2p_1 < p_t$. This implies that for any positive $k$, there are less than $t$ distinct primes between $2^k$ and $2^{k-1}$, otherwise $2^{k-1} < p_1 < p_t < 2^k$ while at the same time $2^k < 2p_1 < p_t$. So we must have $\pi(2^i) - \pi(2^{i-1}) < t$ and hence $\pi(2^k) = \sum_{i=1}^k \pi(2^i) - \pi(2^{i-1}) < kt$, contradicting the prime number theorem. ■

**Theorem 2.1.3.** $\{a_n(k) : k, n \in \mathbb{N}\} = \mathbb{Z}$

**Proof.** Let $t \geq 3$ be odd and let $p_1 < p_2 < \cdots < p_{t-1} < p$ be distinct primes satisfying $p_1 + p_2 > p$. This guarantees that $p_i p_j > p + 1$, so $x^{p_i p_j} \equiv 0 \pmod{x^{p+1}}$ for $i, j = 1, \ldots, t$. Then if $n = p_1 p_2 \cdots p_{t-1} p$, we have

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

$$\equiv (1 - x^{p_1})(1 - x^{p_2}) \cdots (1 - x^{p_{t-1}})(1 - x)/ (1 - x) \pmod{x^{p+1}}$$

$$\equiv (1 - x^{p_1} - x^{p_2} - \cdots - x^{p_{t-1}})(1 + x + \cdots + x^{p-2} + x^{p-1}) \pmod{x^{p+1}}.$$

Among the monomial factors $x^{p_1}, x^{p_2}, \ldots, x^{p_{t-1} p}$, we will have exactly one occurrence of $x^p$ for each $i = 1, \ldots, t - 1$. So in the expansion above, there will be exactly $t - 1$ terms with coefficient of $-1$ on $x^p$, thus $a_n(p) = -(t - 1)$. And furthermore, there will be exactly 1 occurrence of $x^{p-2}$ for each $i = 1, \ldots, t - 1$ with a coefficient of $-1$ and one term with with 1 as a coefficient, thus $a_n(p - 2) = -(t - 2)$. As $t$ takes on odd values greater than 3, the values of $a_n(p)$ take on even integers $\leq -2$ and $a_n(p - 2)$ takes on odd integers $\leq -1$. So we see that

$$\{a_n(k) : k, n \in \mathbb{N}\} \supseteq \{-1, -2, \ldots\}.$$

To see that the values can be any positive number, recall from Proposition 1.3.10 that $\Phi_{2n}(x) = \Phi_n(-x)$ when $n$ is odd. So, since the $p_i$ as chosen above are all odd, we have that $a_{2n}(p)p^p = a_n(p)(-x)^p$, giving $a_{2n}(p) = -a_n(p) = t - 1$ and similarly, $a_{2n}(p - 2) = t - 2$.
So as \( t \) takes on values \( \geq 3 \), the value of \( a_{2n}(p) \) takes on all positive even numbers from \( \geq 2 \) and \( a_{2n}(p-2) \) takes on all odd numbers \( \geq 1 \). So we have

\[
\{a_n(k) : k, n \in \mathbb{N}\} \supseteq \{1, 2, \ldots\}.
\]

It is easy to find \( \Phi_n \) with a 0 as a coefficient, for instance \( \Phi_4(x) = x^2 + 1 \), so \( a_4(1) = 0 \).

Thus we have shown that every integer occurs as a coefficient in some \( \Phi_n \). ■

There are a number of subsets of \( \{a_n(k) : k, n \in \mathbb{N}\} \) which are known to contain every integer. Ji and Li [30] showed that \( \{a_{p\ell_n}(k) : k, n \in \mathbb{N}\} = \mathbb{Z} \) for any prime \( p \) and \( \ell \in \mathbb{N} \). Subsequently Ji, Li, and Moree [31] showed that \( \{a_{mn}(k) : k, n \in \mathbb{N}\} = \mathbb{Z} \) for any integer \( m \geq 1 \). More generally, Yuan [51] showed that \( \{a_{ns+t}(k) : k, n \in \mathbb{N}\} = \mathbb{Z} \) for any \( s, t \in \mathbb{Z} \) with \( s > t \geq 0 \).

So the question remains, what restrictions can be made on \( n \) so that the set of coefficients of \( \Phi_n \) can still become very large? As we will see, the coefficients of \( \Phi_n \) tend to be very large indeed, despite certain restrictions on \( n \).

### 2.2 Bounds on \( A(n) \)

While Schur’s construction in Theorem 2.1.3 shows that

\[
\limsup_{n \to \infty} A(n) = \infty,
\]

we can find an upper bound on \( |a_n(i)| \) for all \( i \) in terms of \( n \). A very trivial upper bound of

\[
\left| \sum_{i=0}^{\varphi(n)} a_n(i) \right| < 2^{\varphi(n)}
\]

arises from (1.1) using the fact that \( |\zeta| = 1 \).

In 1949, Bateman [10] gave the estimate

\[
\log A(n) \leq \exp \left( (\log 2 + o(1)) \frac{\log n}{\log \log n} \right),
\]

where it was shown by Vaughan [49] that the log 2 is best possible. On the other hand, Erdős in [23] showed that the coefficients can become very large. In particular, he showed there exists \( c > 0 \) where

\[
\log(A(n)) \gg \exp \left( \frac{c \log n}{\log \log n} \right),
\]

for infinitely many \( n \). Previously, in 1946 [22], Erdős showed that there are infinitely many \( n \) where \( A(n) > n^c \) for any given constant \( c \). More precisely, [22] shows that given the
constant $c$, there are infinitely many $n$ with
\[ A(n) > \exp[c(\log n)^{4/3}] \]
by taking $n = 2 \cdot 3 \cdot 5 \cdots p_k$ for sufficiently large $k$. Subsequently, Erdős improved this estimate with (2.3), which is best possible because of (2.2).

Later, in 1981, Bateman, Pomerance, and Vaughan in [11] refined these results, giving the sharper estimate
\[ S(n)/n \leq A(n) \leq n^{2k-1}, \]
where $S(n) = \sum m|a_n(m)$ is the length of $\Phi_n$ and $k$ is the number of distinct prime factors of $n$.

If we write $n = p_1 \cdots p_k$ and $M_k = \prod_{i=1}^{k-2} p_i^{2^{i-1}-1}$, then we also have from Bateman, Pomerance, and Vaughan in 1981 [11] that
\[ A(p_1 \cdots p_k) \leq M_k \leq n^{k-12^{k-1}-1}, \]
where it was conjectured that $n$ can be replaced with $\varphi(n)$. Bzdega proves this conjecture in [19] and improves it with a positive constant multiplied to the right side which depends only on $k$ and which quickly decreases as $k$ grows.

For a general lower bound, $A(n) \geq 1$ is the only one which is valid for all $n$ since $A(p) = 1$ when $p$ is prime. So instead, we can look at lower bounds which hold for almost all integers. The assertion that almost all positive integers have a certain property $P$ means that the set of integers having the property $P$ has asymptotic density 1. Or, if property $P$ holds for all $n$ except for a sequence of asymptotic density 0, then $P$ holds for almost all $n$.

We define the asymptotic density of a set $S$ of natural numbers to be
\[ \delta(s_n) = \lim_{n \to \infty} \frac{s_n}{n}, \]
where $s_n$ gives the number of elements of $S$ that do not exceed $n$.

In [40] and [41], Maier shows that for any $\varepsilon(n)$ satisfying $\lim_{n \to \infty} \varepsilon(n) = 0$ and for any $\psi(n)$ satisfying $\lim_{n \to \infty} \psi(n) = \infty$, then the inequalities
\[ n^{\varepsilon(n)} \leq A(n) \leq n^{\psi(n)} \]
hold on a set of integers of asymptotic density 1, and that they are, in fact, best possible. This settled a long standing conjecture of Erdős which asserted that $A(n) \to \infty$ for almost all $n$.

The results of Erdős in [22] showed that the coefficients of the $n$th cyclotomic polynomial can become much larger than $n$ in absolute value. However, these results were formulated long before we had the sophisticated computing techniques capable of handling such large numbers. So, while those concerned with the analytic interpretation of $A(n)$
presumed that there exists \( n \) with \( A(n) \gg n \), those concerned with the construction of such a \( \Phi_n \) would not be able to compute its coefficients explicitly.

The use of supercomputers opened the way for finding explicit examples of extremely large \( A(n) \). However, the computing techniques used in the formulation of \( a_n(k) \) have their limits, as we will see in the next section.

### 2.3 Computational Problems

In 1991, Grytczuk and Tropak in [29] posed the following question: Given an integer \( k \) with \( |k| \geq 2 \), what is the minimal \( m \) such that there exists a number \( n \) for which \( a_n(m) = k \)? That is, we want to find \( m \) such that \( a_n(m) = k \) but \( a_n(r) \neq k \) for \( r < m \).

Following the methods of D.H. Lehmer in [36] and Möller in [43], for \( n > 1 \), we can write Proposition 1.3.4 as

\[
\Phi_n(x) = \prod_{d \mid n} (1 - x^d)^{\mu(n/d)} = \prod_{d=0}^{\infty} (1 - x^d)^{\mu(n/d)}
\]

by setting \( \mu(n/d) = 0 \) when \( n/d \) is not an integer. This way, for square-free \( n \), the value of \( a_n(m) \) depends only on the values of \( \mu(n) \), \( \mu(n/d) \) and on the primes less than \( m + 1 \) that divide \( n \).

If \( |x| < 1 \), then we have

\[
(1 - x^d)^{\mu(n/d)} = \left( 1 - \mu\left(\frac{n}{d}\right)x^d + \frac{1}{2}\mu\left(\frac{n}{d}\right)(\mu\left(\frac{n}{d}\right) - 1) \sum_{j=2}^{\infty} x^{jd} \right). \tag{2.6}
\]

Therefore, we can write

\[
\prod_{d=0}^{\infty} \left( 1 - \mu\left(\frac{n}{d}\right)x^d + \frac{1}{2}\mu\left(\frac{n}{d}\right)(\mu\left(\frac{n}{d}\right) - 1) \sum_{j=2}^{\infty} x^{jd} \right). \tag{2.7}
\]

So in obtaining the coefficient on \( x^k \), we have

\[
a_n(1) = -\mu(n),
a_n(2) = \frac{1}{2}\mu(n)(\mu(n) - 1) - \mu(n/2),
a_n(3) = \frac{1}{2}\mu(n)^2 - \frac{1}{2}\mu(n) + \mu(n/2)\mu(n) - \mu(n/3), \ldots
\]

Put \( B(k) = \max_n \{|a_n(k)|\} \). We know that the values of \( B(k) \) are finite because the set \( \{a_n(k) : n \geq 1\} \) is finite. This can be deduced from the fact that for a fixed \( k \), the coefficient on \( x^k \) in \( \prod_{d \leq k+1} (1 - x^d)^{\mu(n/d)} \) is really \( a_n(k) \) and since \( \mu(r) \in \{-1, 0, 1\} \), we have that \( a_n(k) \) takes on finitely many values for a fixed \( k \).
The function $B(k)$ was studied recently by Gallot, Moree, and Hommersom in [27], where they considered the density of the integers $n$ satisfying $a_n(k) = v$ for any particular $v \in \{a_n(k) : n \geq 1\}$,

$$\delta(a_n(k) = v) = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \chi_v(a_n(k)).$$

They also considered the average values of $a_n(k)$,

$$M(a_n(k)) = \lim_{x \to \infty} \frac{\sum_{n \leq x} a_n(k)}{x}.$$ 

They discovered that the values of $a_n(k)$ for a fixed $k$ behave very similarly to the values of the $k$ coefficient of the Taylor series expansion of $\frac{1}{\Phi_n(x)}$. Their work expanded on the results of Möller [43] from 1970, which was previously the only other author to have written on the densities and averages of the $a_n(k)$.

Bachman [3] showed that for $k > 1$

$$\log B(k) = C_0 \sqrt{k} \left( 1 + O \left( \frac{\log \log k}{\sqrt{\log k}} \right) \right),$$

where we see that $B(k)$ can, in fact, be much larger than $k$. However, looking at the values of $B(k)$ for small $k$, this would not seem to be the case. Möller [43] computed $B(k)$ for $k = 1, \ldots, 30$.

### Table 2.1: $B(k)$ for $1 \leq k \leq 30$

<table>
<thead>
<tr>
<th>$k$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>$B(k)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$k$</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>$B(k)$</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Grytczuk and Tropak in [29] found a recurrence relation for computing the coefficients of $\Phi_n$. Let $T_{m-\ell} = \mu(n)\mu(\gcd(n, m-\ell))\varphi(\gcd(n, m-\ell))$, then

$$a_n(m) = -\frac{1}{m} \sum_{\ell=0}^{m-1} a_n(\ell)T_{m-\ell}$$

where $a_n(0) = 1$. This allowed them to answer their question of finding the smallest $m$ for which there exists $n$ such that $a_n(m) = k$ for the integers $k$ in the interval $[-9, 10]$.

In 2000, Koshiba [34] used the formula of Grytczuk and Tropak to compute one tenth
of the terms of $\Phi_n(x)$ for

$$n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 111546435.$$ 

That is, he computed the terms up to degree $\varphi(n)/10 = 3649536$. He found that among those terms that he was able to compute, the maximum $a_n(k)$ was 4071770387 and the minimum was -4248451085. This was the first known example of the case where $A(n) > n$.

Arnold and Monagan in [2] found that $A(1181895) = 14102773$ and verified that this is, in fact, the smallest $n$ for which $A(n) > n$. Looking at the multiples of 1181895, Arnold and Monagan also found $n$ where $A(n) > n^2$ and $A(n) > n^4$. Furthermore, the algorithms developed by Arnold and Monagan allowed them to find the least $n$ for which $A(n) > n^c$ for $c = 1, \ldots, 7$.

Table 2.2: The least $n$ for which $A(n) > n^c$

<table>
<thead>
<tr>
<th>$c$</th>
<th>$n$</th>
<th>$A(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1181895</td>
<td>14102773</td>
</tr>
<tr>
<td>2</td>
<td>43730115</td>
<td>862550638890874931</td>
</tr>
<tr>
<td>3</td>
<td>416690995</td>
<td>80103182105128365570406901971</td>
</tr>
<tr>
<td>4</td>
<td>1880394945</td>
<td>6454099703601091156682644618152388971563</td>
</tr>
<tr>
<td>5,6</td>
<td>17917712785</td>
<td>$\approx 8.103388 \cdot 10^{63}$</td>
</tr>
<tr>
<td>7</td>
<td>99660932085</td>
<td>$\approx 6.126721 \cdot 10^{87}$</td>
</tr>
</tbody>
</table>

So we have explicit computations from Arnold and Monagan [1] exemplifying the Theorem of Erdős from [22] proved more than fifty years prior. But even with the powerful computers available today, there are limitations. For instance, Arnold and Monagan were unable to compute the heights of cyclotomic polynomials of order greater than 9. They attempted to compute $\Phi_n(x)$ for

$$n = 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 37 \cdot 43 \cdot 53,$$

which has degree 38041436160. The computation was slow and caused hardware problems, so no further attempts were made.

A low-memory algorithm was used by Arnold and Monagan [2] to compute the value of the largest coefficient of $\Phi_n$ without actually storing the complete set of coefficients. This approach is sufficient when studying the height of cyclotomic polynomials, since retrieving all the coefficients would not improve the calculation of $A(n)$. Besides, one is not entirely sure what one can do with a complete set of coefficients for a polynomial whose degree is in the billions, so there seems to be very little reason to store them all to memory.

However, for lower order examples, we will see that a complete ordered list of coefficients will be extremely helpful in understanding the structure of $\Phi_n$. 

19
Chapter 3
Cyclotomic Polynomials of Orders 1 and 2

3.1 Prime Cyclotomic Polynomials

When $p$ is prime, $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is flat, and its coefficients are easy to compute since $a_p(k) = 1$ for $k = 0, \ldots, p - 1$. Thus $V(p) = \{1\}$ and hence cyclotomic polynomials of order 1 are not particularly interesting, when it comes to computing the coefficients. The structure will, however, be useful as we derive a formula for the $pq$th cyclotomic polynomial below.

3.2 Binary Cyclotomic Polynomials

In the order 2 case, it was shown in the late 19th century by Migotti [42] that $V(pq) = \{-1, 0, 1\}$ for distinct prime $p$ and $q$, although more recent results from [35, 38, 21] provide explicit formulas for computing $a_{pq}(k)$. To increase the order of $\Phi_p$, recall that when $p$ and $q$ are prime, Proposition 1.3.9 gives

$$\Phi_{pq}(x) = \Phi_p(x^q) = \Phi_q(x^p) .$$

(3.1)

Therefore, if $\zeta$ is a primitive $pq$th root of unity, then $\Phi_p(\zeta^q) = \Phi_q(\zeta^p) = 0$. Following the procedure described by Lam and Leung in [35], we then consider the unique non-negative integers $r$ and $s$ satisfying $(p - 1)(q - 1) = rp + sq$ (see [39, 12] for the existence of such a representation). So we have

$$\sum_{i=0}^{r} (\zeta^p)^i = - \sum_{i=r+1}^{q-1} (\zeta^p)^i, \quad \sum_{j=0}^{s} (\zeta^q)^j = - \sum_{j=s+1}^{p-1} (\zeta^q)^j .$$

Multiplying these and transposing, we get

$$\left( \sum_{i=0}^{r} \zeta^{ip} \right) \left( \sum_{j=0}^{s} \zeta^{jq} \right) - \left( \sum_{i=r+1}^{q-1} \zeta^{ip} \right) \left( \sum_{j=s+1}^{p-1} \zeta^{jq} \right) = 0 .$$

Thus, $\zeta$ is a zero of the function

$$f(x) = \left( \sum_{i=0}^{r} x^{ip} \right) \left( \sum_{j=0}^{s} x^{jq} \right) - \left( \sum_{i=r+1}^{q-1} x^{ip} \right) \left( \sum_{j=s+1}^{p-1} x^{jq} \right) x^{-pq} .$$

(3.2)

The first product in equation 3.2 is clearly a monic polynomial of degree $(p - 1)(q - 1)$ and the second product is monic of degree $(p - 1)(q - 1) - 1$. So $f(x) \in \mathbb{Z}[x]$ is monic of degree $(p - 1)(q - 1) = \varphi(pq)$. Since $f(x)$ in (3.2) has the same roots as $\Phi_{pq}(x)$, we have that $f(x) = \Phi_{pq}(x)$. Also note that upon expanding the products, the resulting monomial
terms are distinct. Let \(i, i' \in [0, q - 1]\), \(j, j' \in [0, p - 1]\), then \(ip + jq = i'p + j'q\) or \(ip + jq = i'p + j'q - pq\) gives \(q|(i - i')\) hence \(i = i'\), and similarly \(j = j'\). Thus we have the following theorem of Lam and Leung.

**Theorem 3.2.1** (Lam and Leung). Let \(p\) and \(q\) be odd primes and let \(r\) and \(s\) be the unique non-negative integers satisfying \(\varphi(pq) = rp + sq\). Then \(f(x)\) in (3.2) is \(\Phi_{pq}(x)\) and we have the following:

(a) \(a_{pq}(k) = 1\) if and only if \(k = ip + jq\) for some \(i \in [0, r]\) and \(j \in [0, s]\),
(b) \(a_{pq}(k) = -1\) if and only if \(k + pq = ip + jq\) for some \(i \in [r + 1, q - 1]\) and \(j \in [s + 1, p - 1]\),
(c) \(a_{pq}(k) = 0\) otherwise.
(d) The number of terms with \(a_{pq}(k) = 1\) is \((r + 1)(s + 1)\) and the number of terms with \(a_{pq}(k) = -1\) is \((p - s - 1)(q - r - 1)\) and they differ by 1.

A similar formula was independently shown by Lenstra [38]. Note that if we let \(\mu\) be the inverse of \(q\) modulo \(p\) and let \(\lambda\) be the inverse of \(p\) modulo \(q\), then \(r = \mu - 1\) and \(s = \lambda - 1\). Thus the following formula for \(\Phi_{pq}\) is the same as equation (3.2).

\[
\Phi_{pq}(x) = \left( \sum_{i=0}^{\mu-1} x^{ip} \right) \left( \sum_{j=0}^{\lambda-1} x^{jq} \right) - x \left( \sum_{i=0}^{q-\mu-1} x^{ip} \right) \left( \sum_{j=0}^{p-\lambda-1} x^{jq} \right) \tag{3.3}
\]

It is easily verified that the non-zero coefficients of \(\Phi_{pq}(x)\) alternate \(+1, -1, +1, -1, \ldots\). Take the power series expansion of \(\frac{1}{1-x} = 1 + x + x^2 + \cdots\) and write

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

Notice that no two termwise products have the same exponent upon expansion, because \(\gcd(p, q) = 1\) and hence the \(q\) exponents in the left product will have different residues modulo \(q\). Therefore, this power series has coefficients of 1 and 0 and hence the coefficients of \(\Phi_{pq}(x)\) will be given as a difference between two distinct consecutive terms.

**Example 3.2.1.** We can demonstrate an easy technique of Elder from [21]. Using the results of Lam, Leung, and Lenstra we obtain the so-called L diagram by placing the values \(ip + jq\) for \(i = 0, \cdots, q - 1\) and \(j = 0, \cdots, p - 1\) on a grid of size \(p \times q\) and reduce the values modulo \(pq\). In this case, consider \(p = 5\) and \(q = 11\).
The lines are placed to the right of the column $i = 9$, since the inverse of 5 modulo 11 is $\mu = 9$, and below the row $j = 1$, since $\lambda = 1$ is the inverse of 11 modulo 5. Thus we have the degrees of the terms with a coefficient of $+1$ occurring in the upper left quadrant of the L diagram and the degrees of the terms with coefficient of $-1$ occurring in the bottom right quadrant, and the terms with coefficient 0 occurring the other two quadrants. So we have up to degree $\varphi(n)/2$

$$\Phi_{55}(x) = 1 - x + x^5 - x^6 + x^{10} - x^{12} + x^{15} - x^{17} + x^{20} - \cdots,$$

where we see the first pairs of terms are the difference of two consecutive non-zero terms, but the gap increases in the later terms. Also, since $\lambda = 1$ in this case, we have that the positive terms of $\Phi_{55}$ are all multiples of $p = 5$.

3.3 The Coefficients of $\Phi_{3p}(x)$ and $\Phi_{5p}(x)$

We now consider the cyclotomic polynomials of the form $\Phi_{3p}(x)$ and develop a formula for the coefficients. We begin with Proposition 1.3.9 to get the identity $\Phi_{3p}(x)\Phi_3(x) = \Phi_3(x^p)$. Hence we have

$$2(p-1)\sum_{i=0}^{i} a_{3p}(i) x^{i} (x^2 + x + 1) = x^{2p} + x^p + 1. \tag{3.4}$$

If we collect the terms with degree less than $p$ on the left of equation (3.4), then we can equate the coefficients on the left to the coefficients of the same degree on the right. In other words, we have

$$a_{3p}(0) = 1$$
$$a_{3p}(0) + a_{3p}(1) = 0$$
$$a_{3p}(0) + a_{3p}(1) + a_{3p}(2) = 0$$
$$\vdots$$
$$a_{3p}(p-3) + a_{3p}(p-2) + a_{3p}(p-1) = 0$$
This allows us to define the following recursion relation for $a_{3p}(i)$.

**Theorem 3.3.1.** $a_{3p}(0) = 1$, $a_{3p}(1) = -1$ and $a_{3p}(i) = -a_{3p}(i - 1) + a_{3p}(i - 2)$ for $i = 2, \ldots, p - 1$.

Note that this completely determines the coefficients of $\Phi_{3p}$ since $\varphi(3p)/2 = p - 1$. Following this recursion, we can write the sequence of coefficients of $\Phi_{3p}(x)$ as

$$\{a_{3p}\} = \{1, -1, 0, 1, -1, 0, \ldots, 0, -1, 1, 0, -1, 1\}.$$  

This leads to the following corollary.

**Corollary 3.3.2.** If $0 \leq k \leq p - 1$, then we have

$$a_{3p}(k) = \begin{cases} 1 & \text{if } k \equiv 0 \pmod{3}, \\ -1 & \text{if } k \equiv 1 \pmod{3}, \\ 0 & \text{if } k \equiv 2 \pmod{3}. \end{cases}$$

If $p \leq k \leq 2(p - 1)$, we write $a_{3p}(k) = a_{3p}(2(p - 1) - k)$.

A similar strategy works for other cases, for example, we can determine the coefficients of $\Phi_{5p}(x)$ up to degree $p - 1$ by equating the terms of both sides of the equation

$$\sum_{i=0}^{4(p-1)} a_{5p}(i)x^i(x^4 + x^3 + x^2 + x + 1) = x^{4p} + x^{3p} + x^{2p} + xp + 1. \quad \text{(3.5)}$$

So we have a similar recursion relation of the form

$$a_{5p}(0) = 1$$
$$a_{5p}(0) + a_{5p}(1) = 0$$
$$a_{5p}(0) + a_{5p}(1) + a_{5p}(2) = 0$$
$$a_{5p}(0) + a_{5p}(1) + a_{5p}(2) + a_{5p}(3) = 0$$
$$a_{5p}(0) + a_{5p}(1) + a_{5p}(2) + a_{5p}(3) + a_{5p}(4) = 0$$
$$\vdots$$
$$a_{5p}(p - 6) + a_{5p}(p - 4) + a_{5p}(p - 3) + a_{5p}(p - 2) + a_{5p}(p - 1) = 0$$

So we have the following for the coefficients of $\Phi_{5p}(x)$ up to degree $p - 1$.

**Theorem 3.3.3.** Let $i = 0, \ldots, p - 1$, then we have

$$a_{5p}(i) = \begin{cases} 1 & \text{if } i \equiv 0 \pmod{5}, \\ -1 & \text{if } i \equiv 1 \pmod{5}, \\ 0 & \text{otherwise}. \end{cases}$$
However, for the higher degree terms of $\Phi_5 p(x)$, we must consider the possible congruence classes of $p$ modulo 5. Let $1 \leq \ell \leq 4$ be the unique integer with $p \equiv \ell \pmod{5}$. Then we have the following formula for the remaining terms of $\Phi_5 p(x)$.

**Theorem 3.3.4.** For $i = p, \ldots, 2(p - 1)$, we have $a_5 p(i) = a_5 p(i - p) + a_5 p(i - p + \ell)$. For the terms of degree greater than $2(p - 1)$, we apply reciprocity.

So we see that the structures of the polynomials $\Phi_{3p}(x)$ and $\Phi_{5p}(x)$ are easily characterized, and for the general binary case, $\Phi_{pq}(x)$, the coefficients are determined by the formula in Theorem 3.2.1.

As we will see, the structure of higher order $\Phi_n(x)$ is much more complicated.
Chapter 4
Cyclotomic Polynomials of Order 3

The coefficients of $\Phi_{pqr}(x)$ are a great deal more interesting than the lower order cases. First of all, the cyclotomic polynomials of order three are not always flat. When $n = pqr$ for odd primes $p < q < r$, we begin to see many examples of non-flat $\Phi_n$, the first case being $n = 3 \cdot 5 \cdot 7 = 105$. By the construction in Theorem 2.1.3 we see that 3, 5 and 7 satisfy $3 + 5 > 7$, so $a_{105}(7) = -2$, which is apparent in the following expansion.

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$$

(4.1)

Migotti [42] was the first to discover that $a_{105}(7) = -2$ in 1883, disproving the conjecture that $V(n) \subseteq \{-1, 0, 1\}$ for all $n$. Let $p < q < r$ be distinct odd primes. The coefficients of $\Phi_{pqr}$ have long been a source of interesting questions going back to a classic result of Bang [9] from 1895 which showed that

$$A(pqr) \leq p - 1.$$  (4.2)

The behavior of the coefficients of $\Phi_{pqr}$ in general are not completely characterized at present, despite the wealth of literature on the topic. Several authors, namely Sister Marion Beiter in [12, 13, 14, 15] and more currently Gennady Bachman in [4, 5, 6, 7, 8], have studied this case extensively. We must also mention the contributions of Gallot and Moree [27, 25, 26, 45], who are frequent collaborators, for they inspired much of the recent development of the topic.

Before examining the general case, we will begin by looking at the specific case where $n = 3pq$. Once we establish the structure of $\Phi_{3pq}(x)$, we can extend it to the general case of $\Phi_{pqr}(x)$.

4.1 Determining $A(3pq)$

The height of $\Phi_{3pq}(x)$ was studied by Beiter in [15]. Her results completely characterize the height of $\Phi_{3pq}$. We will reprove some of her results using a slightly different construction of $\Phi_{3pq}(x)$.

From Proposition 1.3.9, we write

$$\Phi_{3pq}(x) = \frac{\Phi_{3p}(x^q)}{\Phi_{3p}(x)} = \frac{\Phi_{3p}(x^q)\Phi_3(x)}{\Phi_3(x^p)} = \frac{-\Phi_{3p}(x^q)\Phi_3(x)(x^p - 1)}{1 - x^{3p}}.$$  (4.3)
From Corollary 3.3.2 we can write $\Phi_{3p}(x)$ up to degree $p - 1$ as

$$\Phi_{3p}(x) = 1 - x + x^3 - x^4 + x^6 - x^7 + \cdots,$$

so working modulo $x^{(p-1)(q-1)/2+1}$, we have

$$\Phi_{3p}(x^q) \equiv (1 - x^q) \sum_{j \geq 0} x^{3qj} \pmod{x^{\varphi(pq)/2+1}}.$$

So we then apply this to the formula in equation (4.3) and use the power series expansion of $\sum_{i \geq 0} x^{3pi} = 1/(1 - x^{3p})$ to obtain the following congruence.

$$\Phi_{3pq}(x) = (1 + x + x^2 - x^p - x^{p+1} - x^{p+2}) \Phi_{3p}(x^q) \sum_{i \geq 0} x^{3pi}$$

$$\equiv (1 + x + x^2 - x^p - x^{p+1} - x^{p+2})(1 - x^q) \sum_{j \geq 0} x^{3qj} \sum_{i \geq 0} x^{3pi} \pmod{x^{\varphi(pq)/2+1}}$$

$$\equiv \sum x^\alpha (1 + x + x^2 - x^p - x^{p+1} - x^{p+2}$$

$$- x^q - x^{q+1} - x^{q+2} + x^{p+q} + x^{p+q+1} + x^{p+q+2}) \pmod{x^{\varphi(pq)/2+1}},$$

where $\alpha$ ranges over all values of the form $\alpha = 3(pi + qj)$ for $i, j \geq 0$. Therefore, in determining the value of $a_{3pq}(k)$ for $0 \leq k \leq (p - 1)(q - 1)$, we need to consider the partitions of $k$ into the form

$$k = a + 3pi + 3qj + \delta_1 p + \delta_2 q,$$

(4.4)

where $a = 0, 1, 2, i, j \geq 0$, and $\delta_1, \delta_2 \in \{0, 1\}$. We see that partitions with $\delta_1 = \delta_2$ contribute +1 to the value of $a_{3pq}(k)$ and partitions with $\delta_1 \neq \delta_2$ contribute −1 to the value of $a_{3pq}(k)$. If $k$ has no partitions of the form (4.4), then $a_{3pq}(k) = 0$. Therefore, we are looking for partitions of $k$ into one of the following forms:

$$P_1 = a_1 + 3i_1p + 3j_1q;$$
$$P_2 = a_2 + 3i_2p + 3j_2q + p + q;$$
$$P_3 = a_3 + 3i_3p + 3j_3q + p;$$
$$P_4 = a_4 + 3i_4p + 3j_4q + q.$$

The partitions in $P_1$ and $P_2$ will each contribute +1 to $a_{3pq}(k)$ while the partitions in $P_3$ and $P_4$ will each contribute −1 to $a_{3pq}(k)$. Note that when $k \leq (p - 1)(q - 1)$, there will only be one possible partition of each of the forms $P_1, P_2, P_3,$ and $P_4$.

Now consider the possible values of $j_t$ in the partitions $P_t$ for $t = 1, \ldots, 4$.

**Lemma 4.1.1.** For any $j_t$, we have $3j_t \leq p - 2$ for all $p$.

**Proof.** From [16] we have $3j_tr \leq (p - 1)(q - 1) < (p - 1)r$, giving $3j_t < q - 1$. ■
Note that in the partitions $P_2$ and $P_1$ we have $3j_h \leq q - 3$. We should also mention that for all primes $3 < p < q$, we have either $p + q \equiv 0 \pmod{3}$ or $p - q \equiv 0 \pmod{3}$. These facts will come in handy in the following theorems.

**Theorem 4.1.2.** In $\Phi_{3pq}(x)$,

(a) if $p - q \equiv 0 \pmod{3}$, then $-1 \leq a_{3pq}(i) \leq 2$.

(b) if $p + q \equiv 0 \pmod{3}$, then $-2 \leq a_{3pq}(i) \leq 1$.

**Proof.** Consider the following equations:

$$P_4 - P_3 = a_4 - a_3 + 3p(i_4 - i_3) + 3q(j_4 - j_3) + q - p = 0. \quad (4.5)$$

$$P_2 - P_1 = a_2 - a_1 + 3p(i_2 - i_1) + 3q(j_2 - j_1) + p + q = 0. \quad (4.6)$$

(a) Suppose $p - q \equiv 0 \pmod{3}$ and $a_{3pq}(k) = -2$ for some $k$ so that partitions of $k$ of the forms $P_3$ and $P_4$ exist. Take the value of equation (4.5) modulo 3 to obtain $a_4 - a_3 \equiv 0 \pmod{3}$ and hence $a_4 = a_3$ since $a < 3$. Now if we take equation (4.5) modulo $p$ we obtain $3(j_4 - j_3) + 1 \equiv 0 \pmod{p}$. Therefore, we can write $3(j_4 - j_3) = \beta p - 1$ for some non-zero $\beta \in \mathbb{Z}$. This gives either

$$3(j_4 - j_3) = \beta p - 1 \geq p - 1 \text{ or } 3(j_3 - j_4) = |\beta|p + 1 \geq p + 1. \quad (4.7)$$

However, this is not possible, since Lemma 4.1.1 gives $3j_3, 3j_4 \leq p - 2$ for all $p$. Therefore, the partitions $P_3$ and $P_4$ can not both exist.

(b) The proof of part (b) follows the same argument as part (a) applied to equation (4.6). \[\blacksquare\]

So we see that $\Phi_{3pq}(x)$ can have a coefficient of $-2$ or 2, but not both. Note that if $p$ and $q$ are twin primes then $a_{3pq}(q) = -2$ with $P_3 = p + 2$ and $P_4 = q$, otherwise $a_{3pq}(q) = -1$. When $q = 2p + 1$, we have $a_{3pq}(p + q) = 2$ with $P_1 = 3p + 1$ and $P_2 = p + q$, otherwise $a_{3pq}(p + q) = 1$.

Now, we will consider the specific cases when $q = kp \pm 1$ and $q = kp \pm 2$.

**Theorem 4.1.3.** Let $q = kp \pm 1$. Then $A(3pq) = 1$ if and only if $k \equiv 0 \pmod{3}$.

**Proof.** Suppose that $q = 3hp + 1$ with $p \equiv 1 \pmod{3}$, in which case we have $q - p \equiv 0 \pmod{3}$, so by Theorem 4.1.2, we have $a_{3pq}(i) \neq -2$. In equation (4.6), we see that $a_2 - a_1 = 1$ if $p + q \equiv 2 \pmod{3}$ and $a_2 - a_1 = -2$ if $p + q \equiv 1 \pmod{3}$, so taking (4.6) modulo $p$ gives either

$$3(j_2 - j_1) = \beta p - 2 \text{ or } 3(j_2 - j_1) = \beta p + 1$$
where $\beta \equiv 2 \pmod{3}$. But Lemma 4.1.1 gives $3j_1, 3j_2 \leq p - 2$ for all $p$, so we can not have $0 \leq k \leq (p - 1)(q - 1)$ for which $k$ has both partitions $P_1$ and $P_2$. When $p \equiv 2 \pmod{3}$, the argument is the same, but applied to equation (4.5), in which case we see that partitions of $k$ of the form $P_3$ and $P_4$ can not both exist.

If $q = 3hp - 1$, we have $q \equiv 2 \pmod{3}$, so we consider the congruence classes of $p$ modulo 3. When $p \equiv 2 \pmod{3}$, we get the same equations as above with $\beta \equiv 1 \pmod{3}$. This leads to the same contradiction. And we see that when $p \equiv 1 \pmod{3}$, we have the same equations with $\beta \equiv 2 \pmod{3}$ and replacing $j_1$ and $j_2$ with $j_3$ and $j_4$, respectively. Thus, we see in any case, $|a_{3pq}(i)| \leq 1$.

Conversely, we can construct counterexamples to show that for $k \equiv 1 \pmod{3}$ or $k \equiv 2 \pmod{3}$, coefficients of 2 or $-2$ occur. See Table 4.1 for the counterexamples.

<table>
<thead>
<tr>
<th>$k \pmod{3}$</th>
<th>$q$</th>
<th>Partitions of $i$</th>
<th>$a_{3pq}(i)$</th>
<th>Examples $p$ $q$ $i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$kp + 1$</td>
<td>$P_3 = 1 + (k - 1)p + p$</td>
<td>$P_4 = q$</td>
<td>$-2$ $7$ $29$</td>
</tr>
<tr>
<td>1</td>
<td>$kp - 1$</td>
<td>$P_3 = (k - 1)p + p$</td>
<td>$P_4 = 1 + q$</td>
<td>$-2$ $5$ $19$</td>
</tr>
<tr>
<td>2</td>
<td>$kp + 1$</td>
<td>$P_1 = 1 + (k + 1)p$</td>
<td>$P_2 = p + q$</td>
<td>$2$ $5$ $41$</td>
</tr>
<tr>
<td>2</td>
<td>$kp - 1$</td>
<td>$P_1 = (k + 1)p$</td>
<td>$P_2 = 1 + p + q$</td>
<td>$2$ $7$ $13$</td>
</tr>
</tbody>
</table>

The next theorem addresses the case when $q \equiv \pm 2 \pmod{p}$.

**Theorem 4.1.4.** Let $q = kp \pm 2$. Then $|a_{3pq}(i)| \leq 1$ if and only if $k \equiv 0$ and $p \equiv 1 \pmod{3}$.

The proof of this follows the proof of Theorem 4.1.3, so we will just show some counterexamples to the case when $k \equiv 0$ and $p \equiv 2 \pmod{3}$ and the cases when $k \equiv 1, 2 \pmod{3}$.

First consider the case when $k \equiv 0$ and $p \equiv 2 \pmod{3}$. If $q = kp + 2$, then the partitions $P_1 = 2 + (p + 1)q/2$ and $P_2 = 1 + (p - 1)kp/2 + p + q$ give $a_{3pq}(i) = 2$ for example $p = 5, q = 17$ give $a_{3pq}(53) = 2$. And in the case that $q = kp - 2$, the partitions $P_3 = (p + 1)q/2 + p$ and $P_4 = 1 + (p - 1)kp/2 + q$ give $a_{3pq}(i) = -2$ for example when $p = 5$ and $q = 13$, we have $a_{3pq}(44) = -2$. See Table 4.2 below for counterexamples to the remaining cases.
Now, consider a more general situation. Let $3 < p < q$ be primes with $q = (kp + 1)/h$ or $q = (kp - 1)/h$ for $h \leq \frac{p-1}{2}$. Theorem 4.1.3 is the case $h = 1$. So let $h > 1$. In $q = (kp \pm 1)/h$, we may consider $p, q, k,$ and $\pm 1$ as four independent variables with $h$ dependent. There are two possible values for $p$ and $q$ modulo 3 and three possible values for $k$ modulo 3. That leaves 24 cases to examine.

For the first case, let $p \equiv q \equiv 1$ and $k \equiv 0 \pmod{3}$, with $q = (kp - 1)/h$ for some $1 < h \leq \frac{p-1}{2}$. In this case, we must have $h \equiv 2 \pmod{3}$. Since $q - p \equiv 0$, we have $a_{3pq}(i) \neq -2$ by Theorem 4.1.2. Taking equation (4.6) modulo 3, we obtain $a_2 - a_1 = -2$ or 1. Then taking equation (4.6) modulo $p$, we have either

$$-2 + [3(j_2 - j_1) + 1]/h \equiv 0 \text{ or } 1 + [3(j_2 - j_1) + 1]/h \equiv 0.$$ 

So one possibility is $3(j_2 - j_1) = \beta p - 2h - 1$ with $\beta \equiv 2$, but no such $\beta$ satisfies the inequality $3j_i \leq p - 2$ from Lemma 4.1.1. The other possibility is that $3(j_2 - j_1) = \beta p + h - 1$ with $\beta \equiv 2 \pmod{3}$. If $h = 2$, then clearly the inequality does not hold. If $h > 2$, then $3j_1 = p - h + 1$ satisfies the inequality in Lemma 4.1.1, but substituting this value into equation (4.6), we obtain $3i_2 = q - k - 1$. So we have $P_1 = (p - h + 1)$ and $P_2 = (q - k - 1)p + q + p$ by using $a_1 = 0$ and $a_2 = 1$. But setting $a_3 + 3i_3p + 3j_3q + p = (p-1)/h$, we can have a partition of $P_3 = 2 + (q - 2k - 1) + (h+1)q + p$. Or, we can set $a_1 = 1$ and $a_2 = 2$ and we can have the partitions $P_1$, $P_2$, and $P_4$ will exist. In any case, we have $a_{3pq}(i) \neq 2$ for any $i$. Thus we state the following theorem with the remaining cases presented in Tables 4.3, 4.4, 4.5, and 4.6.

**Theorem 4.1.5.** Let $q = (kp \pm 1)/h$ for $1 \leq h \leq (q - 1)/2$. Then $A(3pq) = 1$ if and only if one these conditions holds:

(a) $k \equiv 0$ and $h + q \equiv 0 \pmod{3}$ or

(b) $h \equiv 0$ and $k + r \equiv 0 \pmod{3}$. 

<table>
<thead>
<tr>
<th>$k \pmod{3}$</th>
<th>$q$</th>
<th>Partitions of $i$</th>
<th>$a_{3pq}(i)$</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$kp + 2$</td>
<td>$P_3 = (k - 1)p + p + 2$</td>
<td>$P_4 = q$</td>
<td>$-2$</td>
</tr>
<tr>
<td>1</td>
<td>$kp - 2$</td>
<td>$P_3 = (k - 1)q + q$</td>
<td>$P_4 = q + 2$</td>
<td>$-2$</td>
</tr>
<tr>
<td>2</td>
<td>$kp + 2$</td>
<td>$P_1 = (k + 1)p$</td>
<td>$P_2 = p + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>2</td>
<td>$kp - 2$</td>
<td>$P_1 = (k + 1)$</td>
<td>$P_2 = p + q + 2$</td>
<td>$2$</td>
</tr>
</tbody>
</table>
Table 4.3: The case $p \equiv q \equiv 1 \pmod{3}$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$h$</th>
<th>$\pm1$</th>
<th>Partitions of $i$</th>
<th>$A(3pq)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>$+$</td>
<td>$P_1 = 2 + (p - 2h + 1)q$</td>
<td>$2$</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>$+$</td>
<td>$P_1 = 2 + (2k + 1)p$</td>
<td>$2$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>$+$</td>
<td>$P_2 = (q - 2k - 1)p + p + q$</td>
<td>$1$</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>$-$</td>
<td>$P_1 = 2 + (2h + 1)q$</td>
<td>$2$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$-$</td>
<td>$P_1 = 2 + (q - 2k + 1)p$</td>
<td>$2$</td>
</tr>
</tbody>
</table>

Table 4.4: The case $p \equiv q \equiv 2 \pmod{3}$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$h$</th>
<th>$\pm1$</th>
<th>Partitions of $i$</th>
<th>$A(3pq)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>$+$</td>
<td>$P_1 = (q - 2k + 1)p$</td>
<td>$2$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>$+$</td>
<td>$P_2 = 2 + (p - 2h - 1)q + p + q$</td>
<td>$1$</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>$+$</td>
<td>$P_2 = 2 + (2k - 1)p + p + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>$-$</td>
<td>$P_2 = 2 + (2k - 1)q + p + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>$-$</td>
<td>$P_2 = 2 + (q - 2k - 1)p + p + q$</td>
<td>$2$</td>
</tr>
</tbody>
</table>

Table 4.5: The case $p \equiv 2, q \equiv 1 \pmod{3}$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$h$</th>
<th>$\pm1$</th>
<th>Partitions of $i$</th>
<th>$A(3pq)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>$+$</td>
<td>$P_3 = 2 + (p - 2h + 1)p + p$</td>
<td>$1$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>$+$</td>
<td>$P_4 = (q - 2k + 1)p + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$+$</td>
<td>$P_4 = (2h - 1)q + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>$-$</td>
<td>$P_4 = (p - 2h - 1)q + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$-$</td>
<td>$P_4 = 1 + (h - 1)q + q$</td>
<td>$2$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>$-$</td>
<td>$P_4 = 1 + (h - 1)q + q$</td>
<td>$1$</td>
</tr>
</tbody>
</table>
Table 4.6: The case $p \equiv 1, q \equiv 2 \pmod{3}$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$h$</th>
<th>$\pm 1$</th>
<th>Partitions of $i$</th>
<th>$A(3pq)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>+</td>
<td>$P_3 = 1 + (k - 1)p + p$</td>
<td>$P_4 = (h - 1)q + q$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>+</td>
<td>$P_3 = (q - 2k - 1)p + p$</td>
<td>$P_4 = 2 + (p - 2h - 1)q + q$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>+</td>
<td>$P_3 = (p - 2h + 1)q + p$</td>
<td>$P_4 = 2 + (q - 2k + 1)p + q$</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>-</td>
<td>$P_3 = (p - 2h + 1)q + p$</td>
<td>$P_4 = 2 + (q - 2k + 1)p + q$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-</td>
<td>$P_3 = (p - 2h + 1)q + p$</td>
<td>$P_4 = 2 + (q - 2k + 1)p + q$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>-</td>
<td>$P_3 = (p - 2h + 1)q + p$</td>
<td>$P_4 = 2 + (q - 2k + 1)p + q$</td>
</tr>
</tbody>
</table>

These theorems were proved by Beiter in [15] using her previous results from [13, 12]. The next section will derive some results for the coefficients of $\Phi_{pqr}(x)$ for general primes $p, q, r$.

4.2 The Coefficients of $\Phi_{pqr}(x)$

In her dissertation [12], Beiter proves a method for determining the $k$th coefficient of $\Phi_{2pq}$ by examining the allowable partitions of $k$.

**Theorem 4.2.1.** Let $2 < p < q < r$ be primes. Then $(-1)^{\alpha + \beta_1 + \beta_2 + \beta_3}$ is contributed to $a_{2pq}(k)$ for each partition of the form

$$k = \alpha + \beta_1 pq + \beta_2 pr + \beta_3 qr + \gamma_1 q + \gamma_2 r$$

where $\alpha = 0, \ldots, p - 1$; $\beta_i = 0, 1, \ldots$; and $\gamma_i = 0, 1$. And $a_{2pq}(k) = 0$ if $k$ has no partition of that form.

Beiter used this construction in her papers [13, 14] to prove results about the height of $\Phi_{pqr}(x)$. In particular, she examined the possible partitions of the form

$$P_{3i} = a_{3i} + \alpha_{3i} pq + \beta_{3i} qr + iqr,$$
$$P_{3i} = a_{3i} + \alpha_{3i} pq + \beta_{3i} pr + iqr + q + r,$$
$$P_{4i} = a_{4i} + \alpha_{4i} pq + \beta_{4i} qr + iqr + q,$$
$$P_{4i} = a_{4i} + \alpha_{4i} pq + \beta_{4i} pr + iqr + q,$$

for $i = 0, \ldots, (p - 3)/2$.

This approach is rather complicated and relies heavily on counting arguments and examining specific cases of $p, q, r$.

In 2007, Kaplan [32] also gives a method of determining any particular coefficient of $\Phi_{pqr}$ using the coefficients of $\Phi_{pq}$. This result will be used later in Section 4.4 to prove Kaplan’s family of flat cyclotomic polynomials of order three.
Lemma 4.2.2. Given fixed $0 \leq n \leq \varphi(pqr)$, let $f(m)$ be the unique value $0 \leq f(m) < pq$ such that
\[ f(m) \equiv r^{-1}(n - m) \pmod{pq}. \]

Then we have
\[ a_{pqr}(n) = \sum_{m=0}^{p-1} a'_pq(f(m)) - \sum_{m=q}^{q+p-1} a'_pq(f(m)), \]
where $a'_pq(i) = a_{pq}(i)$ if $ri \leq n$ and 0 otherwise.

Proof. By Proposition 1.3.9 we can write
\[ \Phi_{pqr}(x) = \frac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)} = \frac{\Phi_{pq}(x^r)\Phi_1(x)\Phi_p(x)\Phi_q(x)}{x^{pq} - 1}. \]

Using the power series expansion of $\frac{1}{x^{pq} - 1}$ we get
\[ \Phi_{pqr}(x) = (1 + x^{pq} + \cdots)(1 + x + \cdots + x^{p-1} - x^q - x^{q+1} - \cdots - x^{p+q+1})\Phi_{pq}(x^r). \]

Now let
\[ g(x) = (1 - x^{pq})\Phi_{pqr}(x) = (1 + x + \cdots + x^{p-1} - x^q - x^{q+1} - \cdots - x^{p+q+1})\Phi_{pq}(x^r). \]

We now gather the terms of $g(x)$ which have exponent congruent to $n \pmod{pq}$. Define
\[ \chi_m = \begin{cases} 1 & \text{if } m \in [0, p-1], \\ -1 & \text{if } m \in [q, p+q-1], \\ 0 & \text{otherwise}. \end{cases} \]

Recall that $f(m) \equiv r^{-1}(n - m) \pmod{pq}$, thus $\chi_m x^m a_{pq}(f(m)) x^{rf(m)}$ is a term in $g(x)$ with exponent congruent to $n$ modulo $pq$. As we range $m$ over $[0, pq - 1]$, we find all terms in $g(x)$ with exponent congruent to $n$ modulo $pq$, so for $a_{pq}(n) \neq 0$ we require $a'_pq(f(m)) \neq 0$ or in other words $rf(m) \leq n$, therefore $m \leq pq$ and $f(m) \equiv r^{-1}(n - m) \pmod{pq}$.

However $rf(m) \leq n$ if and only if $m + rf(m) \leq n$ thus, in order to compute $a_{pqr}(n)$, we need to sum all the terms of $g(x)$ with exponent at most $n$ modulo $pq$ corresponding to all these $m$’s,
\[ a_{pqr}(n) = \sum_{m \geq 0} \chi_m a'_pq(f(m)) = a_{pqr}(n) = \sum_{m=0}^{p-1} a'_pq(f(m)) - \sum_{m=q}^{q+p-1} a'_pq(f(m)). \]

This formula also relies heavily on counting arguments when used in practice, so we are somewhat limited in its ability to compute coefficients explicitly. But as we will see in Theorem 4.4.1, it handles the case when $r \equiv 1 \pmod{pq}$ particularly well, allowing us to show this case is flat.
4.3 Beiter’s Conjecture

In [14], Beiter successfully showed the following improvement to Bang’s bound.

**Theorem 4.3.1** (Beiter’s Bound). $A(pqr) \leq p-k$ when $p = 4k+1$ and $A(pqr) \leq p-(k+1)$ when $p = 4k+3$.

Sometimes this result is stated as

$$A(pqr) \leq p - \left\lfloor \frac{p}{4} \right\rfloor,$$

although Beiter’s statement is more precise since $p - (k + 1) < p - \left\lfloor \frac{p}{4} \right\rfloor$ when $p = 4k + 3$. Beiter’s statement can be made stronger if we consider the slightly sharper bound using the ceiling function instead of the floor function

$$A(pqr) \leq p - \left\lceil \frac{p}{4} \right\rceil.$$

This bound is verified by Bachman in [5] as a consequence of a much stronger result.

Beiter’s original conjecture originated in her paper [13] in which she attempted to improve upon Bang’s bound by showing that

$$A(pqr) \leq \frac{1}{2}(p+1)$$

when $q$ or $r \equiv \pm 1 \pmod{p}$, a result which was simultaneously shown by Bloom [16]. Beiter was also able to verify (4.8) for $p = 3, 5$ and any primes $q < r$. She conjectured this to be the case for all prime $p < q < r$.

It was proved by Möller [44] that, if her conjecture were true, it would be the best bound possible since for prime numbers $3 < p < q < r$ with $q \equiv 2 \pmod{p}$ and $r = \frac{1}{2}(mpq - 1)$ for some integer $m$, we have

$$a_{pqr}((p-1)(qr+1)/2) = \frac{1}{2}(p+1).$$

Gallot and Moree [26] showed Beiter’s conjecture to be false when $p \geq 11$ and a number of counterexamples were given such as $A(11 \cdot 59 \cdot 877) = 7$. In particular, it was shown that for any fixed $\varepsilon > 0$ and for every sufficiently large prime $p$, there exist $q$ and $r$ such that

$$A(pqr) > \left(\frac{2}{3} - \varepsilon\right)p.$$  

Gallot and Moree’s estimate in (4.10) suggests that Beiter’s original conjecture in (4.8) can be adjusted to be more accurate, in fact Gallot and Moree conjectured that

$$A(pqr) \leq \frac{2}{3}p.$$  

(4.11)
A proof of this corrected upper bound was published by Zhao and Zhang in [52] after giving sufficient conditions in [53] while also showing that Beiter’s original conjecture holds in the case that \( p = 7 \). The estimate in (4.11) is the best possible general upper bound for \( A(pqr) \) where \( p \) is fixed and \( q < r \) are any distinct primes because of (4.10).

In [18], Bzdega shows that if we let \( A_+(pqr) = \max_k \{ a_{pqr}(k) \} \) and \( A_-(pqr) = \min_k \{ a_{pqr}(k) \} \), then we can obtain a bound on the height of \( \Phi_{pqr}(x) \) which depends only on the inverses of \( q \) and \( r \) modulo \( p \) (which we denote by \( q' \) and \( r' \) respectively). Bzdega’s bound can be stated as follows.

**Theorem 4.3.2.** \( A_+(pqr) \leq \min \{ 2\alpha + \beta, p - \beta \} \); \(-A_-(pqr) \leq \min \{ p + 2\alpha - \beta, \beta \} \), where \( \alpha = \min \{ q', r', p - q', p - r' \} \) and \( \alpha \beta qr \equiv 1 \pmod{p} \) with \( 0 < \beta < p \).

Bzdega also shows the following bound on \( A(pqr) \).

**Theorem 4.3.3.** Let \( \beta^* = \min \{ \beta, p - \beta \} \). Then \( A(pqr) \leq \min \{ 2\alpha + \beta^*, p - \beta^* \} \).

This improves on a theorem of Bachman from [4] which showed the estimate

\[
A(pqr) \leq \min \left\{ \frac{p - 1}{2} + \alpha, p - \beta^* \right\}.
\]

Bzdega in [18] also provides a simplified proof of the so called *jump one ability* of the ternary cyclotomic coefficients, a result which was independently shown by Gallot and Moree in [25], which states that the neighboring coefficients of \( \Phi_{pqr}(x) \) differ by at most 1. Or

\[
|a_{pqr}(n) - a_{pqr}(n - 1)| \leq 1.
\]

The coefficients of \( \Phi_{pqr} \) can get large. In E. Lehmer’s paper [37] it was proved that the coefficients \( a_{pqr}(i) \) can become arbitrarily large in absolute value, a result that Bungers had previously showed assuming that there are infinitely many twin primes. Lehmer’s proof does not require this assumption. H. Möller’s construction in equation (4.9) shows this as well, since Dirichlet’s theorem on primes in arithmetic progressions says that there are infinitely many primes \( r = \frac{1}{2}(mpq - 1) \) for some integer \( m \).

Bachman in [5] showed that the set of coefficients of \( \Phi_{pqr} \) are contained in a particular interval.

**Theorem 4.3.4.** For every odd prime \( p \) there exists an infinite family of polynomials \( \Phi_{pqr} \) such that the set of coefficients of each of these polynomials coincides with the set of integers in the interval \([- (p - 1)/2, (p + 1)/2]\). Moreover, the latter assertion is also true if we state it with the interval \([- (p + 1)/2, (p - 1)/2]\) instead.

This shows that every integer is a coefficient in some cyclotomic polynomial of order 3.
4.4 Flat Cyclotomic Polynomials of Order 3

Currently, we know of several infinite families of flat cyclotomic polynomials of order 3. Bachman in [6] showed that for any prime \( p \geq 5 \), we can find infinitely many pairs of prime \((q, r)\) with \( \Phi_{pqr} \) flat, where \( q \equiv -1 \pmod{p} \). Kaplan in [32] gives an infinite family of flat cyclotomic polynomials of order 3 where given any pair of primes \((p, q)\), there exist infinitely many \( r \) with \( \Phi_{pqr} \) flat. The following results are from Kaplan’s paper [32].

**Theorem 4.4.1** (Kaplan). Let \( p < q \) be primes and let \( r \equiv \pm 1 \pmod{pq} \) be prime. Then \( A(pqr) = 1 \).

**Proof.** Assume \( r \equiv 1 \pmod{pq} \). So \( r^{-1} \equiv 1 \pmod{pq} \). Given \( n \), let \( f(i) \) be the unique value \( 0 \leq f(i) \leq q \) such that \( f(i) \equiv n - i \pmod{pq} \). So from Lemma 4.2.2 we have

\[
a_{pqr}(n) = \sum_{i=0}^{p-1} a'_{pq}(f(i)) - \sum_{j=q}^{q+p-1} a'_{pq}(f(j)).
\]

Let

\[
S = \sum_{i=0}^{p-1} a'_{pq}(f(i)), \quad T = \sum_{j=q}^{q+p-1} a'_{pq}(f(j))
\]

and as in the proof of Lemma 4.2.2, let

\[
g(x) = (1 - x^{pq})\Phi_{pqr}(x) = (1 + x + \cdots + x^{p-1} - x^q - x^{q+1} - \cdots - x^{p+q+1})\Phi_{pq}(x^r).
\]

Now we note that the degree of \( g(x) \) is \( r(p-1)(q-1) + p + q - 1 = (p-1)(q-1)(r-1) + pq \) and we have that \( a_{pqr}(n) = 0 \) for \( n > \varphi(pqr) = (p-1)(q-1)(r-1) \). Since \( a_{pq}(i) \neq 0 \) implies that \( i \leq (p-1)(q-1) \), for \( n \geq r(p-1)(q-1) \), we have \( a_{pq}(f(i)) = a'_{pq}(f(i)) \) for all \( i \). This implies that

\[
\sum_{i=0}^{p-1} a_{pq}(f(i)) = \sum_{j=q}^{q+p-1} a_{pq}(f(j)),
\]

which clearly holds for all \( n \). Since we have that the non-zero coefficients of \( \Phi_{pq}(x) \) alternate \(+1, -1, +1, -1, \ldots\) as shown in Theorem 3.2.1, for any values of \( \alpha \) and \( \beta \),

\[
\left| \sum_{i=\alpha}^{\beta} a_{pq}(i) \right| \leq 1.
\]

We note that \( f(i + k) \equiv f(i) - k \pmod{pq} \) and that \( pq - (p-1)(q-1) = q + p - 1 \). Let \( j \leq i \leq j + p - 1 \). The values of \( f(i) \) that give \( a_{pq}(f(i)) \neq 0 \) lie in some interval \([\ell, \ell + p - 1]\). This is because if \( (p-1)(q-1) < f(i) < pq \), then \( a_{pq}(f(i)) = 0 \). Thus \( S \) and \( T \) have absolute value at most 1. If \( T = 0 \), then we have \( |a_{pqr}(n)| \leq 1 \), so suppose that \( T = 1 \).

First, consider the case that there exists \( k \) with \( q \leq k \leq q+p-1 \) such that \( a_{pq}(f(k)) \neq 0 \)
and \( rf(k) > n \), so that \( a'_{pq}(f(k)) = 0 \). Now we see that \( f(k) \leq (p-1)(q-1) \), so its not possible to have both \( f(k) = (p-1)(q-1) \) and \( k = q+p-1 \). In the case that \( k = q+p-1 \), we must have \( f(j) \geq f(k) \) for all \( q \leq j \leq q + p - 1 \), so \( a'_{pq}(f(j)) = 0 \), contradicting the assumption that \( T = 1 \). So \( k \) must satisfy \( k + f(k) < pq \), therefore if \( 0 \leq i \leq p-1 \), then \( f(i) > f(k) \), so we have that \( a'_{pq}(f(i)) = 0 \) and hence \( S = 0 \).

Now assume that for all \( q \leq k \leq q + p - 1 \), we have \( a'_{pq}(f(k)) = a_{pq}(f(k)) \). Then

\[
T = \sum_{j=q}^{q+p-1} a_{pq}(f(j)) = 1 = \sum_{i=0}^{p-1} a_{pq}(f(i)).
\]

Since the coefficients of the non-zero terms alternate between +1 and –1, the non-zero term giving the minimum value of \( f(j) \) and the non-zero term giving the maximum value of \( f(j) \) must both be 1. So for each \( n \), either \( S = 0 \) or \( S = 1 \), thus \( |a_{pqr}(n)| \leq 1 \).

For the case when \( r \equiv -1 \pmod{pq} \), we define \( f(i) \) to be the unique value \( 0 \leq f(i) < pq \) such that \( f(i) \equiv -(n-i) \pmod{pq} \). The rest of the argument is the same. ■

In the same paper, Kaplan showed that given primes \( p \) and \( q \), the height \( A(pqr) \) is determined by \( \pm r \pmod{pq} \).

**Theorem 4.4.2** (Periodicity of \( A(pqr) \)). Let \( p < q < r \) be primes. Then for any prime \( s > q \) such that \( s \equiv \pm r \pmod{pq} \), \( A(pqr) = A(pqs) \).

Observing computational data, several new families of flat cyclotomic polynomials of order three were discovered by David Broadhurst and conjectured in [17]. His conjecture looked at three different categories of the ordered triple \([p, q, r]\) in which he observed \( \Phi_{pqr} \) to be flat. Let \( p < q < r \) be distinct primes and \( w \) the unique value with \( 0 < w \leq \frac{pq-1}{2} \) satisfying \( r \equiv \pm w \pmod{pq} \). Broadhurst’s three categories are as follows:

- If \( w = 1 \) then we say \([p, q, r]\) is Type 1.
- If \( w > 1, q \equiv 1 \pmod{pw}, p \equiv 1 \pmod{w} \), then \([p, q, r]\) is Type 2.
- If \( w > p, q > p(p-1), q \equiv \pm 1 \pmod{p} \), and \( w \equiv 1 \pmod{p} \) where we have \( wp \nmid q+1 \) and \( wp \nmid q-1 \), then we say \([p, q, r]\) is Type 3.

Broadhurst made the following claims about the three types in a discussion on line in [17].

**Conjecture 4.4.3** (Broadhurst).

(a) If \([p, q, r]\) is of Type 1 or Type 2, then \( A(pqr) = 1 \).

(b) If \([p, q, r]\) is not of Type 1, 2, or 3, then \( A(pqr) > 1 \).
(c) If \([p, q, r]\) is of Type 3, then \(A(pqr) = 1\) if and only if the polynomial \(\Phi_{pq}(x^s)/\Phi_{pq}(x)\) is flat for the smallest positive integer \(s\) with \(s \equiv 1 \pmod{p}\) and \(s \equiv \pm r \pmod{pq}\).

At present, the results of Elder in [21] have classified all the known families of flat cyclotomic polynomials. He reproves Kaplan’s family which we state in Theorem 4.4.1. In addition, the following two theorems were proved, which partially covers the first part of Broadhurst’s claims in Conjecture 4.4.3.

**Theorem 4.4.4.** Let \(p < q < r\) be odd primes such that \(r \equiv \pm 2 \pmod{pq}\). Then \(A(pqr) = 1\) if and only if \(q \equiv 1 \pmod{p}\).

**Theorem 4.4.5.** Let \(p < q < r\) be odd primes and let \(w\) be a positive integer such that \(r \equiv w \pmod{p}\), \(p \equiv 1 \pmod{w}\), and \(q \equiv 1 \pmod{pw}\). Then \(A(pqr) = 1\).

### 4.5 Inverse Cyclotomic Polynomials

We define the inverse cyclotomic polynomial \(\Psi_n(x)\) as the monic polynomials whose roots are the non-primitive \(n\)th roots of unity. That is,

\[
\Psi_n(x) = \frac{x^n - 1}{\Phi_n(x)}.
\]  

(4.12)

By (1.7),

\[
\Psi_n(x) = \prod_{d|n, d \neq n} \Phi_d(x).
\]  

(4.13)

Similarly to \(\Phi_n\), the inverse cyclotomic polynomial \(\Psi_n\) has integer coefficients which are relatively small for small values of \(n\). In fact, \(\Psi_n\) is flat for \(n < 561\).

Note that \(\Psi_n(x)\) is in the power series expansion of

\[
\frac{1}{\Phi_n(x)} = -\frac{\Psi_n(x)}{1-x^n} = -\Psi_n(x)(1 + x^n + x^{2n} + \cdots),
\]

so from Proposition 1.3.9, we can write \(\Phi_{np}\) as

\[
\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)} = -\Psi_n(x)\Phi_n(x^p)(1 + x^n + x^{2n} + \cdots).
\]

Moree’s paper [45] establishes various properties of the coefficients of \(\Psi_n(x)\), focusing on the easiest non-trivial case where \(n\) is the product of three distinct odd primes. Here, we will let

\[
\Psi_n(x) = \prod_{1 \leq k \leq n, \gcd(k,n) > 1} (x - e^{2\pi ik/n}) = \sum_{j=0}^{n-\varphi(n)} c_n(j)x^j,
\]

(4.14)
and we will write the height of $\Psi_n(x)$ as

$$C(n) = \max_k \{|c_n(k)|\}.$$  

Applying the formula from Proposition 1.3.4, we can write the formula for $\Psi_n(x)$ as

$$\Psi_n(x) = -\prod_{\substack{d|n \atop d \neq n}} (1 - x^d)^{-\mu(n/d)}. \tag{4.15}$$

The following proposition establishes some basic properties of $\Psi_n(x)$.

**Proposition 4.5.1.**

(a) $\Psi_{2n}(x) = (1 - x^n)\Psi_n(-x)$ if $n$ is odd;

(b) $\Psi_{pn}(x) = \Psi_n(x^p)$ if $p$ is prime and $p|n$;

(c) $\Psi_{pn}(x) = \Psi_n(x^p)\Phi_n(x)$ if $p$ is prime and $p \nmid n$;

(d) $\Psi_n(x) = \Psi_m(x)(x^{n/m})$ where $m$ is the product of the distinct prime factors of $n$;

(e) $\Psi_n(x) = -\Psi_{n}(1/x)x^{n-\varphi(n)}$.

Denote the set of coefficients of $\Psi_n$ as $W(n) = \{c_n(k) : 0 \leq k \leq n - \varphi(n)\}$. By Proposition 4.5.1(e), for $n > 1$ we have that if $a \in W(n)$, then $-a \in W(n)$. And we can also deduce that if $n - \varphi(n)$ is even, then $c_n((n - \varphi(n))/2) = 0$. Note that $W(1) = \{1\}$ and if $p$ is prime then $W(p) = \{-1, 1\}$ since $\Psi_1(x) = 1$ and $\Psi_p(x) = x - 1$. In equation (4.15) we have $\Psi_n(x) = -1 + O(x^2)$ in the case that $n$ is not square-free, thus $c_1(1) = 0$. If $n$ is odd and square-free with $\mu(n) = -1$, then we have $\Psi_n(x) = -1 + x + O(x^3)$ and hence $c_n(2) = 0$. If $n$ is odd and square-free with $\mu(n) = 1$, then we have

$$\Psi_n(x) = \frac{(x^p - 1)}{1 - x}(1 + O(x^{p+1})),$$

where $p$ is the smallest prime divisor of $n$ and hence $c_n(p) = 0$. And when $n$ is even and square-free, part (a) of Proposition 4.5.1 reduces $\Psi_n$ to the odd and square-free case. Therefore, we have shown that for composite $n > 1$, there is a coefficient of 0 for some term of $\Psi_n(x)$, thus $\{-1, 0, 1\} \subseteq W(n)$.

The order of $\Psi_n$ will be defined to be the same as the order of $\Phi_n$. Similar to the cyclotomic polynomials, the inverse cyclotomic polynomials are flat for orders 1 and 2. This is easily seen in the following examples.

$$\Psi_1(x) = 1;$$
$$\Psi_p(x) = x - 1;$$
$$\Psi_{pq}(x) = x^{p+q-1} + \cdots + x^{q+1} + x^q - x^{p-1} - \cdots - x^2 - x - 1.$$
So we now examine $\Psi_{pqr}(x)$ and apply the formula in equation (4.15) to get

$$\Psi_{pqr}(x) = \frac{(x - 1)(1 - x^{pq})(1 - x^{pr})(1 - x^{qr})}{(1 - x^p)(1 - x^q)(1 - x^r)}. \quad (4.16)$$

Or as in part (c) of Proposition 4.5.1,

$$\Psi_{pqr}(x) = \Phi_{pq}(x)\Psi_{pq}(x^r). \quad (4.17)$$

Let us now write

$$\Phi_{pq}(x)(1 + x^r + \ldots + x^{(p-1)r}) = \sum_{j=0}^{\tau} e(j)x^j, \quad (4.18)$$

where $\tau = (p-1)(r+q-1)$ and when $j \not\in [0, \tau]$, we say $e(j) = 0$. Note that this polynomial is of degree $\tau$ and is self-reciprocal. The following lemma from [45] gives some formulas for computing $c_{pqr}(k)$, which are derived from equation (4.18).

**Lemma 4.5.2.** Let $p < q < r$ be odd primes and $\tau = (p-1)(r+q-1)$. If $k < qr$, then

$$c_{pqr}(k) = -e(k) = -\sum_{j=0}^{\left\lfloor \frac{k}{r} \right\rfloor} a_{pq}(k - jr).$$

If $k > \tau$, then

$$c_{pqr}(k) = e(k - qr) = \sum_{j=0}^{\left\lfloor \frac{k}{r} \right\rfloor - q} a_{pq}(k - (q + j)r),$$

if $k - qr \geq 0$ and 0 otherwise. If $qr \leq k \leq \tau$, then

$$c_{pqr}(k) = -e(k) + e(k - qr) = -\sum_{j=0}^{\left\lfloor \frac{k}{r} \right\rfloor} a_{pq}(k - jr) + \sum_{j=0}^{\left\lfloor \frac{k}{r} \right\rfloor - q} a_{pq}(k - (q + j)r).$$

If $qr > \tau$, then $c_{pqr}(k) = c_{pqr}(\tau - k)$. If $\tau < k < qr$, then $c_{pqr}(k) = 0$.

The main result from Moree in [45] is the following theorem.

**Theorem 4.5.3.** Let $p < q < r$ be odd primes. Then $C(pqr) = p - 1$ if and only if $q \equiv r \equiv \pm 1 \pmod{p}$ and $r < \frac{(p-1)}{(p-2)}(q - 1)$. In the remaining cases, $C(pqr) < p - 1$.

Consequently, for every prime $p \geq 3$, there are infinitely many pairs $(q, r)$ such that $C(pqr) = p - 1$. 

39
4.6 Pseudocyclotomic Polynomials

When constructing the cyclotomic polynomial whose index is square-free and odd, the formula in Proposition 1.3.4 can be rewritten in a way that applies to a more general family of polynomials. Let \( n = p_1 \cdots p_k \) for distinct prime factors in the set

\[
\rho = \{p_1, \ldots, p_k\},
\]

then, using the notation of Nagell [46], put

\[
\Pi_0(x) = x^n - 1
\]

and for \( 1 \leq v \leq k \)

\[
\Pi_v(x) = \prod \left( x^{p_i^{v_i}p_j} - 1 \right),
\]

the product extending over all the \( v \) indices \( i_k \) which satisfy the conditions

\[
1 \leq i_1 < i_2 < \cdots < i_v \leq r.
\]

Then we have the identity

\[
\Phi_n(x) = \frac{\Pi_0(x)\Pi_2(x)\cdots}{\Pi_1(x)\Pi_3(x)\cdots},
\]

where all the \( \Pi_v(x) \) with an even index occur in the numerator and all with an odd index in the denominator. From (4.20) we easily deduce Propositions 1.3.8 and 1.3.9.

This allows for a combinatorial approach to solving for the coefficients. The natural generalization of this approach is to define it for distinct, pairwise relatively prime integers. That is, if we consider the set \( \rho = \{p_1, \cdots, p_k\} \) of pairwise relatively prime integers, we can define the pseudocyclotomic polynomial \( \tilde{\Phi}_\rho(x) \) similarly to the identity in (4.20). Thus we have Elder’s [21] formula for the pseudocyclotomic polynomial of order \( k \)

\[
\tilde{\Phi}_{p_1,\ldots,p_k}(x) = \prod_{I \subseteq [k]} \left( x^{\prod_{i \in I} p_i} - 1 \right)^{(-1)^{|I|}}
\]

where \([k] = \{1, 2, \ldots, k\}\). Or, inductively as in Proposition 1.3.8, we can write \( \tilde{\Phi}_{p_1,\ldots,p_k}(x) \) as

\[
\tilde{\Phi}_{p_1,\ldots,p_k}(x) = \frac{\tilde{\Phi}_{p_1,\ldots,p_{k-1}}(x^{p_k})}{\tilde{\Phi}_{p_1,\ldots,p_{k-1}}(x)}.
\]

The name “Pseudocyclotomic polynomial” was coined by Elder in [21] and many of his results on cyclotomic polynomials applies to pseudocyclotomic polynomials just as well. The study of these polynomials was introduced by Bachman in [7] where he referred to the pseudocyclotomic polynomials as inclusion-exclusion polynomials for their combinatorial structure related to the inclusion-exclusion principle. Since we are interested in their relationship to the cyclotomic polynomials, we will adopt Elder’s terminology.
The main motivation behind studying the pseudocyclotomic polynomials is the realization that many of the results that have been formulated for $\Phi_n$, where $n$ is a product of distinct, odd primes, only use the fact that the prime divisors of $n$ are pairwise relatively prime and hence apply to a much larger class of polynomials than the cyclotomic polynomials.

To clarify the notation, consider the polynomials $\tilde{\Phi}_{pqr}(x)$ compared with $\tilde{\Phi}_{p,q,r}(x)$, where we see the commas are necessary, since we write

$$\tilde{\Phi}_{pqr}(x) = \frac{x^{pqr} - 1}{x - 1},$$

whereas

$$\tilde{\Phi}_{p,q,r}(x) = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x - 1)(x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)}.$$

The following facts that we have established for $\Phi_n(x)$ will also hold for the pseudocyclotomic polynomials:

**Proposition 4.6.1.**

(a) $\tilde{\Phi}_{p_1,\ldots,p_k}(x)$ has degree $(p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$.

(b) If $k > 0$, then $\tilde{\Phi}_{p_1,\ldots,p_k}(0) = 1$.

(c) If $k > 1$, then $\tilde{\Phi}_{p_1,\ldots,p_k}(1) = 1$, and $\tilde{\Phi}_{p}(1) = p$.

(d) If $p_i = 1$ for any $i$, then $\tilde{\Phi}_{p_1,\ldots,p_k}(x) = 1$.

(e) For pseudocyclotomic polynomials of order 1, we have

$$\tilde{\Phi}_{p}(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}.$$

(f) The same formula in (3.3) applies to pseudocyclotomic polynomials of order 2, where we let $\mu$ be the inverse of $q$ modulo $p$ and let $\lambda$ be the inverse of $p$ modulo $q$. Then we have

$$\tilde{\Phi}_{p,q}(x) = \left(\sum_{i=0}^{\mu-1} x^{ip}\right) \left(\sum_{j=0}^{\lambda-1} x^{jq}\right) - x \left(\sum_{i=0}^{q-\mu-1} x^{ip}\right) \left(\sum_{j=0}^{p-\lambda-1} x^{jq}\right).$$

**Example 4.6.1.** To see an example of a pseudocyclotomic polynomial which is not a cyclotomic polynomial, consider the relatively prime integers $p^2, q^2, r^2$, where $p, q, r$ are distinct primes. Therefore, we can use the formula in (4.21) to write the pseudocyclotomic polynomial

$$\tilde{\Phi}_{p^2,q^2,r^2}(x) = \frac{(x^{p^2q^2r^2} - 1)(x^{p^2} - 1)(x^{q^2} - 1)(x^{r^2} - 1)}{(x - 1)(x^{p^2q^2} - 1)(x^{p^2r^2} - 1)(x^{q^2r^2} - 1)}.$$
But if we let \( n = p^2q^2r^2 \), then the largest square-free factor of \( n \) is \( pqr \), so by Proposition 1.3.8 we have \( \Phi_n(x) = \Phi_{pqr}(x^{pqr}) \), thus we have the cyclotomic polynomial

\[
\Phi_n(x) = \frac{(x^{p^2q^2r^2} - 1)(x^{p^2q^2r^2q} - 1)(x^{p^2q^2r^2r} - 1)}{(x^{p^2q^2r^2} - 1)(x^{p^2q^2r^2q} - 1)(x^{p^2q^2r^2r} - 1)}.
\]

We also note that the pseudocyclotomic polynomial, \( \tilde{\Phi}_{p^2q^2r^2}(x) \) is a product of \( \Phi_n(x) \) with other cyclotomic polynomials of the form \( \Phi_{p^i q^j r^k}(x) \) for \( i, j, k = 0, 1, 2 \). Thus in general, the pseudocyclotomic polynomials are not irreducible, like the cyclotomic polynomials.

We can also define an analogous inverse pseudocyclotomic polynomial by

\[
\tilde{\Psi}_{p_1, \ldots, p_k}(x) = \frac{x^{p_1 \cdots p_k}}{\Phi_{p_1, \ldots, p_k}(x)},
\]

where we see that if \( p < q \) are relatively prime positive integers, then we have

\[
\tilde{\Psi}_{p,q}(x) = x^{p+q-1} + \cdots + x^q + x^q - x^{p-1} - \cdots - x - 1.
\]
Chapter 5
Cyclotomic Polynomials of Order 4

Cyclotomic polynomials of order 4 are the next simplest case to study after the ternary case. Yet, there is a significant increase in complexity as we go from the order 3 to the order 4 case, as can be seen in the following formula for $\Phi_{pqrs}(x)$.

$$\Phi_{pqrs}(x) = \frac{(x^{pqrs} - 1)(x^{pq} - 1)(x^{ps} - 1)(x^{q} - 1)(x^{rs} - 1)(x - 1)}{(x^{pqr} - 1)(x^{pqs} - 1)(x^{qr} - 1)(x^{qs} - 1)(x - 1)}$$  \hspace{1cm} (5.1)

Bloom in [16] showed that if $p < q < r < s$ are odd primes, then

$$A(pqrs) \leq p(p - 1)(pq - 1).$$

This result, along with Bang’s [9] result in equation (4.2) suggest that if $n = p_1 \cdots p_k$ where $p_1 < \cdots < p_k$ are odd primes, then $A(n)$ can be bounded by a function of a proper subset of $\{p_1, \ldots, p_k\}$. That is, $A(n)$ depends only on the values of $p_1, \ldots, p_i$ where $i < k$.

5.1 Flat Cyclotomic Polynomials of Order 4

The study of the coefficients of cyclotomic polynomials of order 4 is a lesser-known area of study than the order 3 case. Nonetheless, we know of an infinite family of flat cyclotomic polynomials of order 4. The first known example was from Kaplan’s paper [33] in which he used the first flat cyclotomic polynomial of order 4 and generalized his previous result on periodicity stated in Theorem 4.4.2 to generate an infinite family of flat cyclotomic polynomials of order 4.

**Theorem 5.1.1.** Let $2 < p_1 < p_2, \cdots < p_r$ be primes and let $n = p_1 \cdots p_r$. Let $s, t$ be primes satisfying $n < s < t$ and $s \equiv t \pmod{n}$. Then $V(ns) = V(nt)$, i.e. $\Phi_{ns}(x)$ and $\Phi_{nt}(x)$ have the same set of coefficients.

We will prove this theorem in the next section using the methods of Sam Elder in [21] and we will use his techniques to further generalize the result.

An immediate consequence of Theorem 5.1.1 is $A(ns) = A(nt)$ when $n < s < t$ and $s \equiv t \pmod{n}$. In addition, note that $A(3 \cdot 5 \cdot 31 \cdot 929) = 1$. So we can generate infinitely many $s \equiv 929 \equiv -1 \pmod{465}$ by Dirichlet’s theorem for primes in arithmetic progressions. Hence, there are infinitely many flat cyclotomic polynomials of order 4 of the form $\Phi_{3 \cdot 5 \cdot 31 \cdot s}$.

Numerical evidence, however, suggested that this is incomplete. Arnold and Monagan have computed the height of $\Phi_n$ of order 4 for $n < 3 \cdot 10^8$ and made their data available in [1]. There are 1389 flat cyclotomic polynomials of order 4 among their calculations. All of
these are of the form $n = pqrs$ where $q \equiv -1 \pmod{p}$, $r \equiv \pm 1 \pmod{pq}$, and $s \equiv \pm 1 \pmod{pqr}$.

The following theorem, conjectured by Kaplan in [33] and proved in Elder’s paper [21], gives a more general family of flat cyclotomic polynomials of order 4.

**Theorem 5.1.2.** Let $p < q < r < s$ be odd primes such that $r \equiv \pm 1 \pmod{pq}$ and $s \equiv \pm 1 \pmod{pqr}$. Then $A(pqrs) = 1$ if and only if $q \equiv -1 \pmod{p}$.

Elder’s proof of this theorem and Theorems 4.4.4 and 4.4.5 used techniques which we outline in the next chapter.

One curious phenomenon that has appeared among the heights of cyclotomic polynomials transitioning from order 3 to order 4 is the reduction of height of certain $\Phi_{pn}(x)$. The case when $p = 3$ is the only known case where there exists $n$ such that $A(pn) < A(n)$. In other words, it is the only case where we have examples to show that an increase in order can possibly yield a reduction in height. There are 11 examples of this phenomenon for $n < 20000$.

**Table 5.1: Examples of the case $A(3n) < A(n)$ for $n < 20000$**

<table>
<thead>
<tr>
<th>$n$</th>
<th>$3n$</th>
<th>$A(n)$</th>
<th>$A(3n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$4745 = 5 \cdot 13 \cdot 73$</td>
<td>14235</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>$7469 = 7 \cdot 11 \cdot 97$</td>
<td>22407</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>$10439 = 11 \cdot 13 \cdot 73$</td>
<td>31317</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>$14231 = 7 \cdot 19 \cdot 107$</td>
<td>42693</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>$14443 = 11 \cdot 13 \cdot 101$</td>
<td>43329</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>$14707 = 7 \cdot 11 \cdot 191$</td>
<td>44121</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>$16027 = 11 \cdot 31 \cdot 47$</td>
<td>48081</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>$16523 = 13 \cdot 31 \cdot 41$</td>
<td>49569</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>$18791 = 19 \cdot 23 \cdot 43$</td>
<td>56373</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>$19129 = 11 \cdot 37 \cdot 47$</td>
<td>57387</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>$19499 = 17 \cdot 31 \cdot 37$</td>
<td>58497</td>
<td>8</td>
<td>7</td>
</tr>
</tbody>
</table>

By Kaplan’s general periodicity in Theorem 5.1.1, each of these examples generates infinitely many more examples. After establishing some relevant results in Chapter 6, we conjecture about this phenomenon in Conjecture 7.2.1.

### 5.2 Higher Order $\Phi_n(x)$

At present, there are no flat cyclotomic polynomials of order 5 or higher that we know about. We know of many cases where $A(n) = 2$, thanks to the results of Arnold and Monagan [2, 1]. We saw in Theorem 5.1.2 that the only known $\Phi_n(x)$ of order four for
which $A(n) = 1$ are the $n = p_1p_2p_3p_4$ satisfying

\[
\begin{align*}
p_2 &\equiv -1 \pmod{p_1} \\
p_3 &\equiv \pm 1 \pmod{p_1p_2} \\
p_4 &\equiv \pm 1 \pmod{p_1p_2p_3}.
\end{align*}
\]

Arnold and Monagan calculated $A(n)$ for $n = p_1p_2p_3p_4p_5 < 2^{63}$ such that $n/p_i$ satisfies the congruences above for $i = 1, 2, \ldots, 5$. That is,

\[
\begin{align*}
p_2 &\equiv -1 \pmod{p_1} \\
p_3 &\equiv -1 \pmod{p_1p_2} \\
p_4 &\equiv \pm 1 \pmod{p_1p_2p_3} \\
p_5 &\equiv \pm 1 \pmod{p_1p_2p_3p_4}.
\end{align*}
\]

They only considered $n = p_1p_2p_3p_4p_5$ for which, given $(p_1, p_2, p_3, p_4)$, $p_5$ is the minimal prime in its congruence class. Their computations showed that in this case we most frequently have $A(n) = 2$ or occasionally we have $A(n) = 3$, but no instances of $A(n) = 1$ occur.

In fact, Elder [21] proved that in the case that $2 < p < q < r < s < t$ are primes satisfying $t \equiv \pm 1 \pmod{pqrs}$, $s \equiv \pm 1 \pmod{pqr}$, and $r \equiv \pm 1 \pmod{pq}$, we must have $A(pqrst) > 1$. 
Chapter 6
The Structure of \( \Phi_{pn}(x) \)

Since we have a complete understanding of the structure of cyclotomic polynomials of orders 1 and 2, it would seem very useful to understand how the higher order cases are related to these lower order cases. For instance, we can look at cyclotomic polynomials of order 3 as a product of other, simpler polynomials:

\[
\Phi_{pqr}(x) = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)(x - 1)} \\
= \Phi_{pq}(x^r)\Psi_{pq}(x)/(x^{pq} - 1) \\
= -\Phi_{pq}(x^r)\Psi_{pq}(x)(1 + x^{pq} + x^{2pq} + \cdots).
\]

Or in a more general way, when \( p \nmid n \), we can write \( \Phi_{np}(x) \) as a product of simpler polynomials as

\[
\Phi_{np}(x) = -\Psi_n(x)\Phi_n(x^p)(1 + x^p + x^{2p} + \cdots).
\]

This does not necessarily simplify the calculation of \( \Phi_{np}(x) \) because we have to consider complicated counting arguments. But we can see that understanding the structure of the cyclotomic polynomial \( \Phi_{np}(x) \) and its relationship with the lower order cyclotomic polynomial \( \Phi_n(x) \) is ultimately the key to understanding the complicated structure of higher order cyclotomic polynomials.

In fact, we can begin to study those relationships while first reconsidering the structure of \( \Phi_{pq}(x) \) and how it can be used in the construction of \( \Phi_{pqr}(x) \). This structure is the basis of Elder’s arguments in [21] which he uses to prove several new families of flat cyclotomic polynomials.

Sam Elder’s methods in [21] are new and utilize several previously undiscovered results. In particular, Elder’s theory of flat cyclotomic polynomials views \( \Phi_{np} \) as the greatest common divisor of simpler polynomials, allowing it to be written as a linear combination of these simpler polynomials. Here, we will look at his methods under some scrutiny, reprove some results on periodicity, and then sketch outlines of his proofs for Theorems 4.4.4, 4.4.5, and 5.1.2.

6.1 Re-examining \( \Phi_{pq}(x) \)

In Example 3.2.1, we computed the coefficients of \( \Phi_{5,11}(x) \) using the L diagram in Figure 3.2.1, as prescribed by Elder. One key realization was that the rows of this diagram are multiples of \( \Phi_{11}(x^5) \) and the columns are multiples of \( \Phi_{5}(x^{11}) \), or in general \( \Phi_p(x^q) \) and \( \Phi_q(x^p) \). In this particular case, we notice that \( \Phi_{5,11}(x) \) can be written as

\[
\Phi_{55}(x) = \Phi_{11}(x^5) - x(1 + x^5)\Phi_{5}(x^{11}),
\]

46
where we see that \( \Phi_{55}(x) \) is really some linear combination of \( \Phi_5(x^{11}) \) and \( \Phi_{11}(x^5) \). In fact, this notion generalizes to

\[
\Phi_{pq}(x) = (1 + x^p + x^{2p} + \cdots + x^{(\mu-1)p})\Phi_p(x^q) - x(1 + x^q + x^{2q} + \cdots + x^{(p-\lambda-1)q})\Phi_q(x^p),
\]

where as before, \( \mu \) is the inverse of \( q \) modulo \( p \) and \( \lambda \) is the inverse of \( p \) modulo \( q \).

Another key realization of Elder is that the polynomials \((1 + x + \cdots + x^{\ell-1})\Phi_{pq}(x)\) can also be plotted on the L diagram by placing the lines in different locations. For example, when \( \ell = 2 \), we have that \((1 + x)\Phi_{55}(x)\) can be obtained from the following L diagram.

**Figure 6.1: L diagram for \((1 + x)\Phi_{55}(x)\)**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
<th>45</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>16</td>
<td>21</td>
<td>26</td>
<td>31</td>
<td>36</td>
<td>41</td>
<td>46</td>
<td>51</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>27</td>
<td>32</td>
<td>37</td>
<td>42</td>
<td>47</td>
<td>52</td>
<td>2</td>
<td>7</td>
<td>12</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>38</td>
<td>43</td>
<td>48</td>
<td>53</td>
<td>3</td>
<td>8</td>
<td>13</td>
<td>18</td>
<td>23</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>49</td>
<td>54</td>
<td>4</td>
<td>9</td>
<td>14</td>
<td>19</td>
<td>24</td>
<td>29</td>
<td>34</td>
<td>39</td>
<td></td>
</tr>
</tbody>
</table>

Notice that the lines are placed above and to the left of the \( \ell = 2 \) location in the L diagram. So, we can similarly plot \((1 + x + x^2)\Phi_{55}(x)\) using the diagram with the lines above and to the left of \( \ell = 3 \) as we see below.

**Figure 6.2: L diagram for \((1 + x + x^2)\Phi_{55}(x)\)**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
<th>45</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>16</td>
<td>21</td>
<td>26</td>
<td>31</td>
<td>36</td>
<td>41</td>
<td>46</td>
<td>51</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>27</td>
<td>32</td>
<td>37</td>
<td>42</td>
<td>47</td>
<td>52</td>
<td>2</td>
<td>7</td>
<td>12</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>38</td>
<td>43</td>
<td>48</td>
<td>53</td>
<td>3</td>
<td>8</td>
<td>13</td>
<td>18</td>
<td>23</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>49</td>
<td>54</td>
<td>4</td>
<td>9</td>
<td>14</td>
<td>19</td>
<td>24</td>
<td>29</td>
<td>34</td>
<td>39</td>
<td></td>
</tr>
</tbody>
</table>

Thus we have the following generalization of equation (3.3).

**Lemma 6.1.1.** Let \( p < q \) be primes and let \( \ell \) be an integer such that \( 1 \leq \ell \leq p + q - 1 \). Let \( 1 \leq \mu \leq q \) and \( 1 \leq \lambda \leq p \) be such that \( pq + \ell = \mu p + \lambda q \). Then

\[
(1 + x + \cdots + x^{\ell-1})\Phi_{pq}(x) = (1 + x^p + \cdots + x^{p(\mu-1)}) (1 + x^q + \cdots + x^{q(\lambda-1)}) - x^\ell (1 + x^p + \cdots + x^{p(q-\mu-1)}) (1 + x^q + \cdots + x^{q(p-\lambda-1)}). \quad (6.1)
\]

**Proof.** Let \( R(x) \) be the right side of equation (6.1). Then if we multiply by \((1 - x^p)(1 - x^q)\)
we get
\[
(1 - x^p)(1 - x^q)(R(x)) = (1 - x^{p\mu})(1 - x^{q\lambda}) - x^\ell(1 - x^{(p-\mu)}(1 - x^{q(p-\lambda)})
\]
\[
= 1 - x^{p\mu} - x^{q\lambda} + x^{pq+\ell} - x^\ell + x^{\ell+pq-p\mu} + x^{\ell+pq-q\lambda} - x^{pq}
\]
\[
= 1 - x^\ell - x^{pq} + x^{pq+\ell} = (1 - x^\ell)(1 - x^{pq})
\]
\[
= (1 + x + \cdots + x^{\ell-1})(1 - x^p)(1 - x^q)\Phi_{pq}(x).
\]

Another key realization of Elder is that the polynomials of the form \(\Phi_{np}(x)\) for \(p \nmid n\) can be constructed by dividing up the coefficients into families of polynomials \(\{F_j(x)\}\) according to the residue of their exponents modulo \(p\). For example, consider the polynomial \(\Phi_{30}(x)\) for \(n = 10, p = 3\). We have
\[
\Phi_{30}(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.
\]
(6.2)

Then we have \(F_j(x)\) for \(j = 0, 1, 2\) given by
\[
F_0(x) = 1 - x
\]
\[
F_1(x) = 1 - x + x^2
\]
\[
F_2(x) = -x + x^2,
\]
with the original polynomial written \(\Phi_{3,10}(x) = F_0(x^3) + xF_1(x^3) + x^2F_2(x^3)\).

So for the general case, using \(\Phi_{np}(x) = \sum_{j=0}^{p-1} x^jF_j(x^p)\), we have the coefficients of \(\Phi_{np}(x)\) are determined by the coefficients of the \(F_j(x)\). These polynomials have quite a bit of structure to them which uniquely defines the \(F_j(x)\). It is now our goal to establish the structure and properties of these \(F_j(x)\) in the construction of \(\Phi_{np}(x)\). As we prove results on these polynomials, we will also point out that there are pseudocyclotomic analogs for these polynomials, which have similar structure. There will be several results which rely on the use of pseudocyclotomics.

### 6.2 Redefining \(\Phi_{np}\)

Now, we will attempt to generalize our observations in the examples above.

**Proposition 6.2.1.** Let \(m\) and \(n\) be relatively prime positive integers. Then
\[
\Phi_m(x^n) = \prod_{d|n} \Phi_{md}(x).
\]

**Proof.** Let \(n = p_1^{e_1} \cdots p_k^{e_k}\) be the prime factorization of \(n\). Then through repeated application of Proposition 1.3.9, we have
\[
\Phi_m(x^{p_1^{e_1} \cdots p_k^{e_k}}) = \prod_{d|p_1^{e_1} \cdots p_k^{e_k}} \Phi_{md}(x^{p_1^{e_1-1} \cdots p_k^{e_k-1}})
\]
and subsequently applying Proposition 1.3.8 yields

\[
\prod_{d \mid p_1 \cdots p_k} \Phi_{md}(x^{p_1^{e_1-1} \cdots p_k^{e_k-1}}) = \prod_{d \mid n} \Phi_{md}(x).
\]

**Proposition 6.2.2.** Let \(d_1, d_2, \ldots, d_k\) be relatively prime positive integers with \(d_1 d_2 \cdots d_k = n\). Then,

\[
\Phi_n(x) = \gcd\{\Phi_{d_i}(x^{n/d_i})\}_{i=1}^k.
\]

**Proof.** The previous result in Proposition 6.2.1 shows that

\[
\Phi_{d_i}(x^{n/d_i}) = \prod_{d \mid (n/d_i)} \Phi_{d, d}(x) = \Phi_{n}(x) \prod_{d \mid (n/d_i), d \neq n/d_i} \Phi_{d, d}(x)
\]

where we see that

\[
\gcd\left\{ \prod_{d \mid (n/d_i), d \neq n/d_i} \Phi_{d, d}(x), \prod_{d \mid (n/d_j), d \neq n/d_j} \Phi_{d, d}(x) \right\}_{i \neq j} = 1,
\]

and hence \(\gcd\{\Phi_{d_i}(x^{n/d_i})\}_{i=1}^k = \Phi_n(x)\). ■

**Corollary 6.2.3.** If \(n > 1\), then \(\Phi_n\) is the greatest common divisor of all the polynomials of the form \(1 + x^{n/p} + \cdots + x^{(p-1)n/p}\) where \(p\) is a prime dividing \(n\).

**Proof.** Let \(d_i\) in Proposition 6.2.2 be prime. Then \(1 + x^{n/p} + \cdots + x^{(p-1)n/p} = \Phi_p(x^{n/p})\) and the result follows from the statement of Proposition 6.2.2 ■

**Corollary 6.2.4.** If \(p \nmid n\), then

\[
\Phi_{np}(x) = \gcd(1 + x^n + \cdots + x^{n(p-1)}, \Phi_n(x^n))
\]

**Proof.** In Proposition 6.2.2, let \(k = 2, d_1 = n,\) and \(d_2 = p\) and the result follows from the statement of Proposition 6.2.2. ■

By the extended Euclidean Algorithm in the Euclidean domain \(\mathbb{Z}[x]\), we can write the greatest common divisor as a linear combination of the given polynomials. That is, for each \(n\) and prime \(p\) where \(p \nmid n\), there exist unique polynomials \(a(x)_{n,p}, b_{n,p}(x) \in \mathbb{Z}[x]\) of minimal degree such that

\[
\Phi_{np}(x) = a_{n,p}(x)\Phi_p(x^n) + b_{n,p}(x)\Phi_n(x^p).
\]

(6.3)

The polynomials \(a(x)\) and \(b(x)\) here will be uniquely defined if either

\[
\deg(a(x)) < \deg(\Phi_n(x^p)/\Phi_{np}(x)) = \varphi(n)
\]
or
\[ \deg(b(x)) < \deg(\Phi_p(x^n)/\Phi_{np}(x)) = (n - \varphi(n))(p - 1) \]

hold.

### 6.3 Reconstructing \( V(np) \)

Since the degrees of the terms of \( \Phi_n(x^p) \) are multiples of \( p \), we can arrange the terms on either side of equation (6.3) according to the residue class of their exponents modulo \( p \). Thus we can define the families of polynomials \( \{F_{n,p,j}(x)\}_{j=0}^{p-1} \) and \( \{G_{n,p,j}(x)\}_{j=0}^{p-1} \) by

\[ F_j(x) = \sum_{i \geq 0} x^i a_{np}(ip + j) \quad \text{and} \quad G_j(x) = \sum_{i \geq 0} x^i [x^{ip+j}](a(x)\Phi_p(x^n)), \]

so we have

\[ \Phi_{np}(x) = \sum_{j=0}^{p-1} x^j F_j(x^p) \quad \text{and} \quad a(x)\Phi_p(x^n) = \sum_{j=0}^{p-1} x^j G_j(x^p). \]

It is worth noting that we can define pseudocyclotomic analogs as follows:

\[ \tilde{F}_j(x) = \sum_{i \geq 0} x^i [x^{ip+j}][\Phi_{p_1,\ldots,p_k}_p(x)], \quad \tilde{G}_j(x) = \sum_{i \geq 0} x^i [x^{ip+j}][\Phi_{p_1,\ldots,p_k}_p(x)]. \]

If we write \( b(x)\Phi_n(x^p) = \Phi_{np}(x) - a(x)\Phi_p(x^n) = \sum_{j=0}^{p-1} x^j(F_j(x^p) - G_j(x^p)) \) and collect the terms with exponent congruent to \( j \) modulo \( p \), where \( 0 \leq j \leq p - 1 \), we have

\[ \left( \sum_{i \geq 0} x^{ip}[x^{ip+j}]b(x) \right) x^j \Phi_n(x^p) = x^j(F_j(x^p) - G_j(x^p)), \]

therefore, we can say \( F_j(x^p) \equiv G_j(x^p) \pmod{\Phi_n(x^p)} \), or if we change variables, we can say

\[ F_j(x) \equiv G_j(x) \pmod{\Phi_n(x)}. \quad (6.4) \]

And we consider the degree conditions on \( F_j \), since \( \deg(\Phi_{np}(x)) = \varphi(n)(p - 1) \), we have \( \deg(x^jF_j(x^p)) = j + p \deg(F_j(x)) \leq \varphi(n)(p - 1) \), or

\[ \deg(F_j(x)) \leq \varphi(n) - \frac{\varphi(n) + j}{p}, \quad 0 \leq j \leq p - 1. \quad (6.5) \]

In particular, we have \( \deg(F_j(x)) < \varphi(n) = \deg(\Phi_n(x)) \). Therefore, we have the following proposition.

**Proposition 6.3.1.** \( F_j(x) \) is the unique polynomial with degree less than \( \varphi(n) \) congruent.
to \( G_j(x) \) modulo \( \Phi_n(x) \).

In the case that \( p > \varphi(n) \), the inequality in (6.5) simplifies to

\[
\deg(F_j(x)) \leq \begin{cases} 
\varphi(n) - 1 & \text{if } 0 \leq j \leq p - \varphi(n), \\
\varphi(n) - 2 & \text{if } p - \varphi(n) + 1 \leq j \leq p - 1.
\end{cases} \tag{6.6}
\]

For the case when \( p > n \), we see a periodic structure that develops in the \( G_j(x) \). After establishing the structure of the \( G_j(x) \) for \( p < n \), we will extend it to handle all \( p \).

**Proposition 6.3.2.** For all \( 0 \leq j < p - n \), we have \( G_j(x) = G_{n+j}(x) \).

**Proof.** Since \( \deg(a(x)) < \varphi(n) \), \([x^k]a(x) = 0\) for \( k \geq n \). Then we have by definition,

\[
x^{n+j}G_{n+j}(x^p) = \sum_{k \equiv n+j \pmod{p}} x^k[x^k](a(x) + a(x)x^n + \cdots + a(x)x^{n(p-1)})
\]

Similarly, we have that \([x^k](a(x)x^{n(p-1)}) = 0\) unless \( n(p-1) \leq k \leq n(p-1) + \varphi(n) - 1 \). Reducing modulo \( p \) as \( p > n \), we have \( \sum_{k \equiv j \pmod{p}} x^k[x^k](a(x)x^{n(p-1)}) \neq 0 \) implies \( j \in \{p - n, p - n + 1, \ldots, p - n + \varphi(n) - 1\} \pmod{p} \). But since \( j < p - n \) and \( p - n + \varphi(n) - 1 < p \), \( j \not\in \{p - n, p - n + 1, \ldots, p - n + \varphi(n) - 1\} \pmod{p} \) hence \( \sum_{k \equiv j \pmod{p}} x^k[x^k](a(x)x^{n(p-1)}) = 0 \). Therefore,

\[
x^{n+j}G_{n+j}(x^p) = \sum_{k \equiv j \pmod{p}} x^k[x^k](a(x) + a(x)x^n + \cdots + a(x)x^{n(p-2)}),
\]

\[
x^{n+j}G_j(x^p) = \sum_{k \equiv j \pmod{p}} x^{n+k}[x^{n+k}](a(x)x^n + \cdots + a(x)x^{n(p-1)})
\]

\[
= \sum_{k \equiv n+j \pmod{p}} x^k[x^k](a(x)x^n + \cdots + a(x)x^{n(p-1)}) = x^{n+j}G_{n+j}(x^p). \quad \blacksquare
\]

Now we apply Proposition 6.3.1 to get the following:

**Corollary 6.3.3.** For all \( 0 \leq j < p - n \), we have \( F_j(x) = F_{n+j}(x) \).

We now wish to exclude the condition that \( p > n \). To extend this to all \( j \) and include the case \( p < n \), we can define inductively for \( j < 0 \)

\[
G_j(x) = xG_{j+p}(x), \tag{6.7}
\]

\[
F_j(x) = xF_{j+p}(x). \tag{6.8}
\]
This way we have \( x^jG_j(x^p) = x^{j+p}G_{j+p}(x^p) \) and \( x^jF_j(x^p) = x^{j+p}F_{j+p}(x^p) \). While equations (6.4) and (6.5) still hold, we no longer have \( \deg(F_j(x)) < \varphi(n) \) for \( j \leq -\varphi(n) \). Thus we can generalize these results with the following.

**Proposition 6.3.4.** For all \( j < p - n \),

\[
\begin{align*}
G_j(x) &\equiv G_{n+j}(x) \pmod{x^n - 1}, & (6.9) \\
F_j(x) &\equiv F_{n+j}(x) \pmod{\Phi_n(x)}. & (6.10)
\end{align*}
\]

**Proof.** For any \( j < p - n \),

\[
x^{n+j}G_{n+j}(x^p) = \sum_{k=n+j} x^k [x^k](a(x)\Phi_p(x^n)),
\]

\[
x^{n+j}G_j(x^p) = \sum_{k=j} x^k [x^k](a(x)\Phi_p(x^n))
\]

\[
= \sum_{k=n+j} x^k [x^k](a(x)x^n\Phi_p(x^n))
\]

\[
= \sum_{k=n+j} x^k [x^k](a(x)\Phi_p(x^n) + a(x)(x^{pn} - 1))
\]

\[
= x^{n+j}G_{n+j}(x^p) + \sum_{k=n+j} x^k [x^k](a(x)x^{pn}) - \sum_{k=n+j} x^k [x^k]a(x)
\]

where in the third line we use the fact that \( (x^n - 1)\Phi_p(x^n) = x^{pn} - 1 \). Thus we have

\[
x^{n+j}(G_j(x^p) - G_{n+j}(x^p)) = (x^{pn} - 1) \sum_{k=n+j} x^k [x^k]a(x),
\]

giving \( G_j(x^p) \equiv G_{n+j}(x^p) \pmod{x^{pn} - 1} \), hence \( G_j(x) \equiv G_{n+j}(x) \pmod{x^n - 1} \).

So we have shown the congruence in (6.9) holds. To get the second congruence in (6.10), we apply the congruence in (6.4) to the congruence in (6.9) and the fact \( \Phi_n(x)|(x^n - 1) \) to get \( F_j(x) \equiv G_j(x) \equiv G_{n+j}(x) \equiv F_{n+j}(x) \pmod{\Phi_n(x)}. \)

This shows that from a single \( F_j(x) \), we can generate all the \( F_j(x) \) up to congruence modulo \( \Phi_n(x) \). Since the \( F_j(x) \) with non-negative \( j \) have degree less than \( \Phi_n(x) \), this determines all of them. The following lemma gives a set of properties that will define \( F_j(x) \).

**Lemma 6.3.5.** Extend the family \( \{F_j(x)\}_{j=0}^{p-1} \) of polynomials in \( \mathbb{Z}[x] \) by letting \( F_j(x) = xF_{j+p}(x) \) for all \( j < 0 \). If each of the following conditions hold:

1. \( F_{j-n}(x) \equiv F_j(x) \pmod{\Phi_n(x)} \) for all \( 0 \leq j < p \);
2. Inequality (6.5) holds for the original \( F_j(x) \);
(c) \( F_0(0) = 1; \)

then \( \Phi_{np}(x) = \sum_{j=0}^{p-1} x^j F_j(x^p). \)

Proof. Let \( f'(x) = \sum_{j=0}^{p-1} x^j F_j(x^p), \) and suppose that (a) holds. First note that when \( j < 0, \) we have \( F_{j-n}(x) = xF_{j-n+p}(x) \equiv xF_{j+p}(x) = F_j(x) \pmod{\Phi_n(x)}, \) we have \( F_{j-n}(x) \equiv F_j(x) \pmod{\Phi_n(x)} \) for all \( j < p. \) Recall that \( F_j(x) = xF_{j+p}(x) \) implies that \( x^jF_j(x^p) = x^{j+p}F_{j+p}(x^p), \) so we can choose any set of representatives of the \( p \) congruence classes modulo \( p \) to express \( f'(x). \) Since \( \gcd(n, p) = 1, \) the numbers \( \{-in\}_{i=0}^{p-1} \) are representatives of the \( p \) congruence classes modulo \( p, \) and hence

\[
\begin{align*}
f'(x) &= \sum_{j=0}^{p-1} x^j F_j(x^p) = \sum_{i=0}^{p-1} x^{-in} F_{-in}(x^p) \\
&\equiv x^{-n(p-1)}(1 + x^n + \cdots + x^{n(p-1)})F_0(x^p) \pmod{\Phi_n(x^p)} \\
&\equiv x^n \Phi_{p}(x^n)F_0(x^p) \pmod{\Phi_n(x^p)}.
\end{align*}
\]

Since \( \Phi_{np}(x) | \Phi_{p}(x^n) \) and \( \Phi_{np}(x) \bmod{\Phi_n(x^p)}, \) this congruence implies that \( \Phi_{np}(x) \mid f'(x). \)

Now with the condition given in (b) that the inequality in (6.5) holds for the original \( F_j(x), \) we have for \( 0 \leq j \leq p - 1, \)

\[
\deg(f'(x)) = \max\{\deg(x^j F_j(x^p))\} = \max\{j + p \cdot \deg(F_j(x))\} \\
\leq \varphi(n)(p-1) = \deg(\Phi_{np}(x)).
\]

So we see that \( f'(x) = c\Phi_{np}(x) \) for some constant \( c. \) Assuming the condition in (c), we evaluate both sides of the equation at \( x = 0 \) to get \( c = 1. \) So if all three conditions are satisfied, we have \( \Phi_{np}(x) = f'(x). \) \[ \square \]

Condition (b) in Lemma 6.3.5 requires that inequality (6.5) hold for \( F_j(x) \) where \( j \geq 0 \) and when \( p > n, \) equation (6.6) gives the condition. And with the extension, \( \deg(F_{j-p}(x)) = 1 + \deg(F_j(x)), \) we get \( \deg(F_{j-p}(x)) \leq \varphi(n) - \frac{\varphi(n)+j-p}{p} \) if and only if \( \deg(F_j(x)) \leq \varphi(n) - \frac{\varphi(n)+j}{p}. \) Therefore, inequality (6.5) for \( 0 \leq j < p \) is equivalent to inequality (6.5) for \( 1 - \varphi(n) \leq j \leq p - \varphi(n). \) So for the latter range, since \( 0 < (\varphi(n) + j)/p \leq 1, \) we can write equation (6.5) as

\[
\deg(F_j(x)) \leq \varphi(n) - 1 \quad \text{for} \quad 1 - \varphi(n) \leq j \leq p - \varphi(n). \tag{6.11}
\]

Therefore, for the degree requirements in Lemma 6.3.5, we have the inequalities given in (6.5),(6.11), and when \( p > n \) we have (6.6). Since all three conditions hold when \( \Phi_{np}(x) = \sum_{j=0}^{p-1} x^j F_j(x^p), \) we can extend Corollary 6.3.3 to

\[
F_j(x) = F_{n+j}(x) \quad \text{when} \quad 1 - \varphi(n) \leq j \leq p - \varphi(n). \tag{6.12}
\]
So we have at this point a general method for proving facts about \( F_j(x) \) and hence \( \Phi_{np}(x) \) by verifying that any solution satisfies the three conditions of Lemma 6.3.5. And in examining the set of coefficients of \( \Phi_{np}(x) \), we have partitioned \( V(np) \) so that \( V(np) = \bigcup_{j=0}^{n-1} V(F_j(x)) \). Moreover, we have that \( V(F_j(x)) = V(F_{j-p}(x)) \), so we can write \( V(np) = \bigcup_{j < p} V(F_j(x)) \). In the case that \( p > n \), Corollary 6.3.3 gives

\[
V(np) = \bigcup_{j=0}^{n-1} V(F_j(x)) = \bigcup_{j=p-n}^{p-1} V(F_j(x)). \tag{6.13}
\]

So in determining \( V(np) \) we only need to look at the coefficients of \( n \) consecutive \( F_j(x) \).

### 6.4 Revisiting Periodicity

One of the most useful and revealing results on the coefficients of \( \Phi_n \) are those concerning the periodicity of the set of coefficients of \( \Phi_n \). Here we will revisit some of these concepts and show how Elder’s methods provide a simple proof of Kaplan’s general periodicity in Theorem 5.1.1.

First, we prove the following lemma.

**Lemma 6.4.1.** Let \( s, t \) be primes satisfying \( n < s < t \) and \( s \equiv t \pmod{n} \). Then for \( 0 \leq j < s \), we have \( F_{s,j}(x) = F_{t,j}(x) \).

**Proof.** Let us define \( F'_{s,j}(x) = F_{t,j}(x) \) for \( 0 \leq j < s \) and its extension \( F_{s,j}(x) = x^{F'_{s,j+k}(x)} \) for \( j < 0 \). We will verify the conditions of Lemma 6.3.5 with \( p = s \) for the functions \( F'_{s,j}(x) \).

(a) First, consider \( n \leq j < s \) and note that \( F'_{s,j-n}(x) = F_{t,j-n}(x) \equiv F_{t,j}(x) = F'_{s,j}(x) \) (mod \( \Phi_n(x) \)). Now, for \( 0 \leq j < n \), define the unique integer \( k \) such that \( 0 \leq j - n + ks < s \). Then we have

\[
F'_{s,j-n}(x) = x^k F'_{s,j-n+ks}(x) = x^k F_{t,j-n+ks}(x) = F_{t,j-n+k(s-t)}(x) \equiv F_{t,j}(x) = F'_{s,j}(x) \pmod{\Phi_n(x)}
\]

where we use the fact that \( n|(-n + k(s-t)) \).

(b) We will use the condition prescribed in (6.11). So if we have \( 1 - \varphi(n) \leq j \leq s - \varphi(n) \) and let \( k \) be an integer satisfying \( 0 \leq j + ks < s \), then we have \( F'_{s,j}(x) = x^k F'_{s,j+ks}(x) = x^k F_{t,j+ks}(x) \). Then for \( 0 \leq l < k \), since \( 1 - \varphi(n) \leq j + ls < s \), we can apply equation (6.12) to get \( F_{t,j+ls}(x) = F_{t,j+(l-1)s+t}(x) \). Thus applying equation (6.8) we have \( x^l F_{t,j+ls}(x) = x^l F_{t,j+(l-1)s+t}(x) = x^{l-1} F_{t,j+(l-1)s}(x) \). So we have shown \( F'_{s,j}(x) = x^k F_{t,j+ks}(x) = F_{t,j}(x) \), hence \( \deg(F'_{s,j}(x)) = \deg(F_{t,j}(x)) \leq \varphi(n) - 1 \) for all \( 1 - \varphi(n) \leq j \leq s - \varphi(n) \), satisfying the condition.

(c) Finally, \( F_{t,0}(0) = F_{s,0}(0) = 1 \).

\[54\]
The proof of Theorem 5.1.1 requires we assume \( n < s < t \), thus we can apply equation (6.13) to get

\[
V(nt) = \bigcup_{j=t-n}^{t-1} V(F_{t,j}(x)) = \bigcup_{j=0}^{n-1} V(F_{t,j}(x))
\]

\[
= \bigcup_{j=0}^{n-1} V(F_{s,j}(x)) = \bigcup_{j=s-n}^{s-1} V(F_{s,j}(x)) = V(ns).
\]

Elder proves more results like this, including the case when \( s \equiv -t \pmod{n} \).

**Theorem 6.4.2.** Let \( n \) be a positive integer and let \( s \) and \( t \) be primes satisfying \( n < s < t \) with \( s \equiv -t \pmod{n} \). Then \( V(ns) = -V(nt) \).

**Sketch of Proof.** The proof amounts to verifying the following relationship among the \( F_j(x) \):

For \( 0 \leq j < s \),

\[
F_{s,j}(x) = \begin{cases} 
-F_{t,t+s-\varphi(n)-j}(x) & \text{if } s - \varphi(n) + 1 \leq j \leq s - 1, \\
-F_{t,t-n+s-\varphi(n)-j}(x) & \text{if } s - n \leq j \leq s - \varphi(n), \\
F_{s,j+n}(x) & \text{if } 0 \leq j \leq s - n - 1.
\end{cases}
\] (6.14)

Again, as in the previous result, the proof will go through and verify that the right side of equation (6.14) satisfies the conditions of Lemma 6.3.5. Once this is established, we simply apply equation (6.13) and we have

\[
V(ns) = \bigcup_{j=0}^{n-1} V(F_{s,j}(x)) = \bigcup_{j=s-n}^{s-1} V(F_{s,j}(x))
\]

\[
= \bigcup_{j=t-n}^{t-1} -V(F_{t,j}(x)) = -\bigcup_{j=0}^{n-1} V(F_{t,j}(x)) = -V(ns). \quad \blacksquare
\]

These results on periodicity may also be extended to the case when \( n - \varphi(n) < s < t \).

**Theorem 6.4.3.** Let \( n \) be a positive integer and let \( s \) and \( t \) be primes satisfying \( n - \varphi(n) < s < t \) and \( s \equiv \pm t \pmod{n} \). Then \( V(ns) = \pm V(nt) \).

**Proof.** Suppose \( s \equiv t \pmod{n} \). Recall that we can write \( V(ns) = \bigcup_{j=0}^{s-1} V(F_{s,j}(x)) \) and \( V(nt) = \bigcup_{j=0}^{t-1} V(F_{t,j}(x)) \). Also, recall that \( F_{t,j+t}(x) = xF_{t,j}(x) \) if \( j < 0 \), therefore \( V(F_{t,j+t}(x)) = V(F_{t,j}(x)) \). And since \( \gcd(n,t) = 1 \), we have \( V(nt) = \bigcup_{j=0}^{t-1} V(F_{t,j+t}(x)) \).

Now, by equation (6.12) and the fact that \( V(F_{t,j+t}(x)) = V(F_{t,j}(x)) \), we have the equation \( F_{t,-in}(x) = F_{t, -(i-1)n}(x) \) holds when \( 1 - \varphi(n) \leq -in \leq t - \varphi(n) \). So \( F_{t,-in}(x) = F_{t, -(i-1)n}(x) \) unless \( t - n \leq k \leq t - \varphi(n) \) where \( k \equiv -in \pmod{t} \) for some \( 0 \leq k <
When \( F_{t \cdot \cdot n}(x) = F_{t \cdot \cdot (j-1)n}(x) \), we can leave out \( F_{\cdot \cdot n}(x) \) from the calculation of \( V(nt) \). Since \( V(F_{t \cdot \cdot n}(x)) = V(F_{t \cdot j}(x)) \) when \( j \equiv \pm in \pmod{t} \), we can write \( V(nt) = \bigcup_{j=\pm n} V(F_{t \cdot j}(x)) \).

The \( F_{t \cdot j}(x) \) are built from the coefficients of \( \Phi_{nt} \), which are palindromic from equation (2.1), thus we have

\[
V(F_{t \cdot j}(x)) = \{a_{nt}(j + kt) : k \in \mathbb{Z}\} = \{a_{nt}((t - 1) \phi(n) - j - kt) : k \in \mathbb{Z}\} = \{a_{nt}((t - j - \phi(n)) + t(\phi(n) - k - 1)) : k \in \mathbb{Z}\} = \{a_{nt}(t - j - \phi(n) + kt) : k \in \mathbb{Z}\} = V(F_{t \cdot t - j - \phi(n)}).
\]

Since \( 0 \leq t - \phi(n) - j \leq n - \phi(n) \) implies that \( t - n \leq j \leq t - \phi(n) \), we have \( V(nt) = \bigcup_{j=0}^{n - \phi(n)} V(F_{t \cdot j}(x)) \). So when \( n - \phi(n) < s \), we have

\[
V(nt) = \bigcup_{j=0}^{n - \phi(n)} V(F_{t \cdot j}(x)) = \bigcup_{j=0}^{n - \phi(n)} V(F_{s \cdot j}(x)) \subseteq \bigcup_{j=0}^{n - \phi(n)} V(F_{s \cdot j}(x)) = V(ns), \tag{6.15}
\]

and

\[
V(ns) = \bigcup_{j=0}^{s - 1} V(F_{s \cdot j}(x)) = \bigcup_{j=0}^{s - 1} V(F_{t \cdot j}(x)) \subseteq \bigcup_{j=0}^{s - 1} V(F_{t \cdot j}(x)) = V(nt). \tag{6.16}
\]

So we have shown that \( V(ns) = V(nt) \).

In the case when \( s \equiv -t \pmod{n} \), we apply Dirichlet’s theorem on primes in arithmetic progressions to get some prime \( s' > n \) with \( s \equiv s' \pmod{n} \) and some prime \( t' > s' > n \) with \( t \equiv t' \pmod{n} \). By the result we have just shown, since \( s \equiv s' \pmod{n} \) and \( t \equiv t' \pmod{n} \), we have \( V(ns) = V(ns') \) and \( V(nt) = V(nt') \). Since we have \( t' \equiv -s' \pmod{n} \) and \( n < s' < t' \), we can apply the result from Theorem 6.4.2 to get \( V(nt') = -V(ns') \). Thus \( V(ns) = -V(nt) \).

We should also mention that the notion of periodicity applies to the pseudocyclotomic analogs just as well. We will state the following analogs of Lemma 6.4.1 and Theorem 6.4.3, the proofs of which are identical.

**Proposition 6.4.4.** Let \( p_1, \ldots, p_k \) be pairwise relatively prime positive integers and \( n = p_1 \cdot \ldots \cdot p_k \). Let \( s < t \) be positive integers relatively prime to \( n \) such that \( s \equiv t \pmod{n} \). Then for \( 0 \leq j < s \), \( \bar{F}_{p_1 \cdot \ldots \cdot p_k, s \cdot j}(x) = \bar{F}_{p_1 \cdot \ldots \cdot p_k, t \cdot j}(x) \).

**Proposition 6.4.5.** Let \( p_1, \ldots, p_k \) be pairwise relatively prime positive integers and \( n = p_1 \cdot \ldots \cdot p_k \). Let \( s, t \) be positive integers relatively prime to \( n \) such that \( s \equiv \pm t \pmod{n} \) and \( n - (p_1 - 1)(p_2 - 1) \cdot \ldots \cdot (p_k - 1) < s < t \). Then \( V(\bar{F}_{p_1 \cdot \ldots \cdot p_k, s}(x)) = \pm V(\bar{F}_{p_1 \cdot \ldots \cdot p_k, t}(x)) \), taking the same signs.

The following corollary will be particularly useful in the proof of Theorem 4.4.5.
Corollary 6.4.6. Let \( p_1, \ldots, p_k \) be primes and \( n = p_1 \cdots p_k \). Let \( p > n \) be another prime such that \( p \equiv w \pmod{n} \) where \( 0 < w < n \). Then for \( 0 \leq j < w \), \( F_{n,p,j}(x) = \bar{F}_{p_1,\ldots,p_k,w,j}(x) \).

This will be particularly useful as a way of computing \( F_{n,p,0}(x) \) since it does not require us to compute \( \Phi_{np}(x) \).

6.5 Proving Flatness

The structure of the \( F_j(x) \) is the main argument used in Elder’s proofs of Theorems 4.4.4, 4.4.5, and 5.1.2, so we first establish some properties that will be particularly useful in showing cyclotomic polynomials to be flat.

Proposition 6.5.1. Let \( p \) be a prime such that \( p \equiv 1 \pmod{n} \). Then \( F_{n,p,j}(x) \equiv x^{-j} \pmod{\Phi_n(x)} \).

The proof of this Proposition will follow from checking the conditions of Lemma 6.3.5 applied to the polynomial of degree less than \( \varphi(n) \) congruent to \( x^{-j} \) modulo \( \Phi_n(x) \). In the case when \( p \equiv -1 \pmod{n} \), we have the following.

Proposition 6.5.2. Let \( p \) be a prime such that \( p \equiv -1 \pmod{n} \). Then \( F_{n,p,j}(x) \equiv -x^{j+\varphi(n)} \pmod{\Phi_n(x)} \).

Proof. We can find prime \( q \) such that \( q \equiv 1 \pmod{n} \) and hence \( F_{q,j}(x) \equiv x^{-j} \pmod{\Phi_n(x)} \) by Proposition 6.5.1. Also, we have \( p \equiv -q \pmod{n} \), so we can apply the formula from equation (6.14) to get

\[
F_{p,j}(x) = -F_{q,q+p-\varphi(n)-j}(x) \equiv -x^{-q-p+\varphi(n)+j} \\
\equiv -x^{\varphi(n)+j} \pmod{\Phi_n(x)} \text{ if } p - \varphi(n) + 1 \leq j \leq p - 1,
\]

\[
F_{p,j}(x) = -F_{q,q-n+p-\varphi(n)-j}(x) \equiv -x^{-q+n-p+\varphi(n)+j} \\
\equiv -x^{\varphi(n)+j} \pmod{\Phi_n(x)} \text{ if } p - n \leq j \leq p - \varphi(n),
\]

\[
F_{p,j}(x) = F_{p,j+n}(x) \equiv -x^{\varphi(n)+j+n} \\
\equiv -x^{\varphi(n)+j} \pmod{\Phi_n(x)} \text{ if } 0 \leq j \leq p - n - 1,
\]

since \( x^n \equiv 1 \pmod{\Phi_n(x)} \).

In the case that \( p < q < r \) are primes with \( r \equiv \pm 1 \pmod{pq} \), we have \( r \geq pq - 1 > p + q - 1 = n - \varphi(n) \) for \( n = pq \). Therefore, periodicity applies and we can consider the case when \( r \equiv 1 \pmod{pq} \). So we have \( F_{n,r,0}(x) = \bar{F}_{p,q,1,0}(x) = 1 \) and

\[
F_j(x) = x^{-j}F_{j(1-r)}(x) \equiv x^{-j}F_0(x) \equiv x^{-j} \pmod{\Phi_{pq}(x)}.
\]

So in order to establish Kaplan’s family of flat cyclotomic polynomials of order 3, differently from how we proved Theorem 4.4.1, we must show these \( F_j(x) \) are flat. In particular,
we can show for all integers \( k \), that \( x^k \) is congruent to a flat polynomial with degree less than \( (p-1)(q-1) \) modulo \( \Phi_{pq}(x) \). This approach is simpler than the approach from Kaplan and does not rely on counting arguments.

Note that we have pseudocyclotomic analogs to Propositions 6.5.1 and 6.5.2.

**Proposition 6.5.3.** Let \( p_1, \ldots, p_k \) be pairwise relatively prime positive integers and \( p \equiv 1 \pmod{p_1 \cdots p_k} \) a positive integer. Then \( \tilde{F}_{p_1, \ldots, p_k, p, j}(x) \equiv x^{-j} \pmod{\Phi_{p_1, \ldots, p_k}(x)} \).

**Proposition 6.5.4.** Let \( p_1, \ldots, p_k \) be pairwise relatively prime positive integers and \( p \equiv -1 \pmod{p_1 \cdots p_k} \) a positive integer. Then

\[
\tilde{F}_{p_1, \ldots, p_k, p, j}(x) \equiv -x^{j+(p_1-1)\cdots(p_k-1)} \pmod{\Phi_{p_1, \ldots, p_k}(x)}.
\]

### 6.5.1 Proof of Theorem 4.4.4

The next simplest case to prove is Theorem 4.4.4, in which case we have \( p < q < r \). Since periodicity applies here, we need to consider \( r \equiv 2 \pmod{pq} \). From Lemma 6.4.1 we have \( F_{pq, r, j}(x) = F_{pq, 2, j}(x) \) for \( j = 0, 1 \). We know that

\[
F_{pq, 2, 0}(x^2) + xF_{pq, 2, 1}(x^2) = \Phi_{2pq}(x) = \Phi_{pq}(-x) \]

hence \( F_{pq, r, 0}(x^2) = F_{pq, 2, 0}(x^2) - xF_{pq, 2, 1}(x^2) \), so

\[
F_{pq, 2, 0}(x^2) = \frac{1}{2}(\Phi_{pq}(x) + \Phi_{pq}(-x)) = \sum_{k \geq 0} a_{pq}(2k)x^{2k}. \tag{6.17}
\]

Similarly,

\[
x F_{pq, 2, 1}(x^2) = \frac{1}{2}(\Phi_{pq}(-x) - \Phi_{pq}(x)) = -\sum_{k \geq 0} a_{pq}(2k+1)x^{2k+1}, \tag{6.18}
\]

From \( F_{pq, r, 0}(x) \) and \( F_{pq, r, 1}(x) \), we can generate all \( F_{pq, r, j}(x) \). We have

\[
F_{pq, r, -2}(x) = F_{pq, r, -2}(x) = xF_{pq, r, 0}(x),
\]

\[
F_{pq, r, -1}(x) = xF_{pq, r, 1}(x),
\]

and

\[
F_{pq, r, j-2}(x) \equiv xF_{pq, r, j}(x) \pmod{\Phi_{pq}(x)},
\]

with \( \deg F_{pq, r, j}(x) < (p-1)(q-1) \), for \( 4 \leq j < r \).

This forms the basis of the argument. Recall from equation (3.3) that if \( \mu \) is the inverse of \( p \) modulo \( q \) and \( \lambda \) is the inverse of \( q \) modulo \( p \), we have

\[
\Phi_{pq}(x) = \left( \sum_{i=0}^{\mu-1} x^{ip} \right) \left( \sum_{j=0}^{\lambda-1} x^{jq} \right) - x \left( \sum_{i=0}^{q-\mu-1} x^{ip} \right) \left( \sum_{j=0}^{p-\lambda-1} x^{jq} \right).
\]

58
where we know that $\mu > 1$ since $p < q$ and we know that $\lambda = 1$ if and only if $q \equiv 1 \pmod{p}$. So if we suppose that $q \not\equiv 1 \pmod{p}$, then $\lambda > 1$. It can easily be shown that $F_{pq,r,r^{-}(p-1)(q-1)}(x)$ is not flat by showing that either the coefficient on $x^{(p-1)(q-1)/2}$ or $x^{(p-1)(q-1)/2+(p+q)/2}$ is 2. This shows that in the original $\Phi_{pq}(x)$, either

\[ a_{pq}(r - (p - 1)(q - 1) + r(p - 1)(q - 1)/2) = 2 \]

or

\[ a_{pq}(r - (p - 1)(q - 1) + r(p + 1)/2) = 2, \]

when $q \not\equiv 1 \pmod{p}$.

To prove the other direction, we can use the $F_{pq,r,0}(x)$ and $F_{pq,r,1}(x)$ to compute the rest of the $F_{pq,r,j}(x)$ and demonstrate that they must all be flat. See [21] for the details.

### 6.5.2 Proof of Theorem 4.4.5

The next case generalizes one direction of Theorem 4.4.4. That is, Theorem 4.4.5 generalizes the notion that in Theorem 4.4.4, if $q \equiv 1 \pmod{p}$, then $A(pqr) = 1$. The statement of Theorem 4.4.5 says that if $p < q < r$ are primes with $r \equiv w \pmod{pq}$ for some positive integer $w$ with $p \equiv 1 \pmod{w}$ and $q \equiv 1 \pmod{pw}$, then we have $A(pqr) = 1$.

Elder’s proof of Theorem 4.4.5 utilizes a pseudocyclotomic polynomial. He proves that each of the $F_{pq,r,j}(x)$ is flat by an explicit computation. The pseudocyclotomic polynomial $\tilde{\Phi}_{w,p,q}(x)$ is used to calculate $\tilde{F}_{p,q,w,j}(x)$, which is the same as $F_{pq,r,j}(x)$ for $0 \leq j < w$. The $\tilde{F}_{p,q,w,j}(x)$ are computed by extracting the coefficients from $\tilde{\Phi}_{w,p,q}(x)$. And since $q \equiv 1 \pmod{pq}$, we can compute $\tilde{\Phi}_{w,p,q}(x)$ which is the same as $\Phi_{p,q,w}(x)$.

So, starting with the computation of $\tilde{F}_{w,p,q,j}(x)$, from Proposition 6.5.3, we have

\[
\tilde{F}_{w,p,q,j}(x) \equiv x^{-j} \pmod{\tilde{\Phi}_{w,p}(x)}.
\]

We consider the case $0 \leq j < wp$ and calculate

\[
\tilde{F}_{w,p,q,j}(x) = \begin{cases} 
1 & \text{if } j = 0, \\
x^{-j}(1 - (1 + x + \cdots + x^{j-1})\tilde{\Phi}_{w,p}(x)) & \text{if } 1 \leq j < w, \\
x^{-j}(1 - \tilde{\Phi}_{w}(x^{p})) & \text{if } w \leq j < p, \\
x^{wp-j} - (1 + x + \cdots + x^{wp-p-1-j})\tilde{\Phi}_{w,p}(x) & \text{if } p < j \leq w + p - 1, \\
x^{wp-j} & \text{if } w + p \leq j < wp.
\end{cases}
\]

(6.19)

We use this to then construct

\[
\tilde{\Phi}_{w,p,q}(x) = \sum_{j=0}^{q-1} x^j \tilde{F}_{w,p,q,j}(x^q) = \sum_{j=0}^{w-1} x^j \tilde{F}_{p,q,w,j}(x^w).
\]
In particular, for \( f \) term besides \( x \) from Proposition 1.3.9. So we define in each separate case. We can consider some of the simpler cases first. We must examine several cases with various conditions on \( j \) and construct the \( f'(x) \) in each separate case. We can consider some of the simpler cases first.

For the case \( (p - 1)(q + r - 1) < j \leq qr \), we can use the fact that \( \Phi_{pq}(x) \mid \Phi_p(x^{qr}) \) from Proposition 1.3.9. So we define

\[
f'(x) = x^{qr-j} \Phi_p(x^{qr}) = x^{qr-j} + x^{2qr-j} + \cdots + x^{(p-1)qr-j} + x^{pqr-j}.
\]

It is divisible by \( \Phi_p(x^{qr}) \) since \( j \leq qr \). And the other condition on \( j \), \( (p - 1)(q + r - 1) < j \), gives that \( (p - 1)qr - j < (p - 1)(qr - q - r + 1) = (p - 1)(q - 1)(r - 1) \). Therefore, no term besides \( x^{pqr-j} \) has degree bigger than \( \varphi(pqr) \). And clearly this \( f'(x) \) is flat, therefore \( F_j(x) \) is flat for \((p - 1)(q + r - 1) < j \leq qr \).

That leaves two remaining cases to consider: \( 1 \leq j \leq (p - 1)(q + r - 1) \) and \( qr + 1 \leq j \leq pqr - \varphi(pqr) \). We can use the general reciprocity of \( F_j(x) \) to get

\[
\{ V(F_j(x)) \}_{j=1}^{(p-1)(q+r-1)} = \{ V(F_j(x)) \}_{j=qr+1}^{pqr-\varphi(pqr)},
\]

so we have these two cases will come out to be the same. Thus, we only need to consider the case \( qr + 1 \leq j \leq pqr - \varphi(pqr) \).

Now, we must construct a new \( f'(x) \) for these constraints on \( j \). Let \( m = pqr - j \), so that in our construction of \( f'(x) \), we must have a leading term of \( x^m \) for \( \varphi(pqr) \leq m < (p - 1)qr \). Now, let \( m - \varphi(pqr) = ar + b \), where \( 0 \leq b \leq r \) and \( 0 \leq a \leq p \). The remainder of the proof will examine different cases of the parameters \( a \) and \( b \).

A simple case will be the case when \( b \geq 0 \). Let \( \ell = a + 1 < p + 1 < p + q - 1 \) then we can define

\[
f'(x) = x^{b-(p-1)(q-1)}(1 + x^r + \cdots + x^{r(t-1)}) \Phi_p(x^r).
\]

Since \( \Phi_{pq}(x) \mid \Phi_{pq}(x^r) \), we have \( \Phi_{pq}(x) \mid f'(x) \). Then we must consider the terms of
highest degree. Through a direct computation it can be shown that the leading term has
degree $m$, and the next highest degree terms will have degree less than $\varphi(pqr)$.
See [21] for the computations. This $f'(x)$ is clearly flat and satisfies the appropriate conditions, so
we have established the case when $b \geq 0$.

That covers the relatively simple cases. The next case to consider is the case when
$b < (p - 1)(q - 1)$ and $a = 0$, which will be more complicated, so we will give a simple
breakdown of the proof strategy. By defining

$$f'(x) = \Phi_{pqr}(x) \sum_{i=0}^{b} a_{pq}(i)x^{b-i},$$

we can show it satisfies the usual properties. Its monic with $\deg f'(x) = \varphi(pqr) + b = m$.
A direct computation will show that no other terms will have degree higher than $\varphi(pqr)$; see [21].

In order to investigate the coefficients of $f'(x)$ and show its flat, we can define a new
family of polynomials $\{F'_j(x)\}_{j=0}^{r-1}$ from $f'(x)$ in the way we did for $\Phi_{np}$. Here we let

$$F'_j(x) = \sum_{i \geq 0} x^i[x^{j+ir}]f'(x),$$

so that $f'(x) = \sum_{j=0}^{r-1} x^j F'_j(x^r).$ From here, we can use the fact that the structure of the $F'_j(x)$ are similar to the $F_{pq,r,j}(x)$. In fact, the $F'_j(x)$ can be
computed in terms of $F_{pq,r,j}(x)$ based on whether we have $r \equiv 1 \pmod{pq}$ or $r \equiv -1 \pmod{pq}$. See [21] for the complete proof that the $F'_j(x)$ are flat, which requires breaking
the values of $j$ into different intervals and computing each case separately.

The final case to consider is the case when $a > 0$. Here, we can consider the polynomial

$$f'_{a,b}(x)$$

which we will define as the multiple of $\Phi_{pqr}(x)$ with leading term $x^{\varphi(pqr)+ar+b}$ and
no other terms of degree at least $\varphi(pqr)$. The case when $b \geq (p - 1)(q - 1)$ was discussed
earlier, as well as the case $f'_{0,b}$ for $0 \leq b < (p - 1)(q - 1).$ Thus the claim now is that the polynomial

$$f'_{a,b}(x) = f'_{0,b}(x) + x^{r-(p-1)(q-1)+b} \Phi_{pq}(x^r)$$
is flat for $0 < a < p$ and $b \leq (p - 1)(q - 1)$. Again, this will boil down to showing
the appropriate $F'_j(x)$ are flat. In this case, since every exponent added is congruent to
$r - (p - 1)(q - 1) + b$ modulo $r$, we must show that when $j = r - (p - 1)(q - 1) + b$, the
polynomial $F'_j(x) + (1 + x + \cdots + x^{a-1})\Phi_{pq}(x)$ is flat. For the computations, see [21].

So we have a very basic overview of Elder’s strategy, which for the most part relies
heavily on computing the polynomials $F_j(x)$ and its various relatives. But in doing so, we
can establish several very general families of flat cyclotomic polynomials. To date, these
are the most general. However, we still have some way to go before we have a complete
characterization of all flat cyclotomic polynomials.
Chapter 7
Open Questions

7.1 Classifying Flat Cyclotomic Polynomials

Several questions naturally arise from studying flat cyclotomic polynomials. For example, it is not clear whether or not we have discovered all the types of flat cyclotomic polynomials. It is clear, from the conjectures of Broadhurst in Conjecture 4.4.3, that there is at least one family of flat ternary cyclotomic polynomials which we have yet to establish, namely Broadhurst’s Type 3 ternary cyclotomic polynomials. The question remains whether or not Broadhurst’s Type 1, 2, and 3 completely characterize all flat cyclotomic polynomials of order three. Part (b) of Conjecture 4.4.3 would settle this fact.

The same question arises in the order 4 case, that is, have we found all the flat cyclotomic polynomials of order 4? Theorem 5.1.2 covers all the cases that we have observed from computational data. Therefore, it is reasonable to assume that no other flat cyclotomic polynomials of order 4 exist.

Conjecture 7.1.1. Let \( p < q < r < s \) be odd primes with \( r \not\equiv \pm 1 \mod pq \) and \( s \not\equiv \pm 1 \mod pqr \). Then \( A(pqrs) > 1 \).

We have observed that none of the obvious candidates for flat cyclotomic polynomials of order 5 have height 1, but have relatively small height of 2 or 3. In fact, Elder [21] proved that the obvious candidates for \( \Phi_n \) of order 5 with potentially low height must be such that \( A(n) > 1 \). So we conjecture the following.

Conjecture 7.1.2. If \( p, q, r, s, t \) are distinct, odd primes, then \( A(pqrst) > 1 \).

On the other hand, higher order cases have not been attempted. One fact that could potentially settle this would be proving the observation that if \( A(n) > 1 \), then \( A(pn) > 1 \) for all prime \( p \nmid n \). That is, there are no primes \( p \) that would have the effect of “flattening” \( \Phi_n \).

Conjecture 7.1.3. If \( p \) is prime with \( p \nmid n \) and \( A(n) > 1 \), then \( A(pn) > 1 \).

If Conjectures 4.4.3, 7.1.1, 7.1.2, 7.1.3 can be proved true, then we have a complete characterization of all flat cyclotomic polynomials.

7.2 Height Reduction

It would seem reasonable to assume that an increase in order should lead to an increase in height, as has broadly been the situation observed in the data. However, as we have observed in the case when \( p = 3 \), there exist numbers \( n \) such that \( A(pn) < A(n) \), as in Table 5.1, so the slightly stronger statement that \( A(n) \leq A(pn) \) is false, in general. It is
not clear if this is possible for other primes $p$, but there are no known occurrences of this phenomenon for $p \neq 3$.

This may be an observation that holds for other primes $p$, but we have not found any that are small enough to compute. One observation that appears to hold for all the values in Table 5.1, is the following conjecture, which may partially explain this phenomenon.

**Conjecture 7.2.1.** Let $p < q < r < s$ be odd primes, let $u, v$ be such that $r \equiv u \pmod{pq}$ and $s \equiv v \pmod{qr}$ with $|u| \leq (pq - 1)/2$ and $|v| \leq (qr - 1)/2$. If $A(pqrs) < A(qrs)$, then $|u| < |v|$.

This conjecture is based on the observation that $A(pqrs)$ seems to take on smaller values when $s$ is in a smaller congruence class modulo $pqr$. Thus we may have a particular value of $n = qrs$ for which $A(n)$ is unusually large, for instance if $s$ is in a relatively large congruence class modulo $qr$; whereas if we consider its congruence class modulo $pqr$, there may be a reduction in its value modulo $pqr$ compared to its value modulo $qr$, hence a reduction in $A(pn)$.

While Conjecture 7.2.1 clearly holds for the values in Table 5.1, the converse does not hold in general. For instance, let $pqrs = 3 \cdot 11 \cdot 37 \cdot 53$, where we see $u = 4 \equiv 37 \pmod{3 \cdot 11}$ and $v = 53 \equiv 53 \pmod{11 \cdot 37}$, so we have $|u| < |v|$. But in this case, their heights are $A(11 \cdot 37 \cdot 53) = 3$ and $A(3 \cdot 11 \cdot 37 \cdot 53) = 7$. So their must be some extra conditions on the values $p, q, r, s$ in order to have $A(pqrs) < A(qrs)$. 

63
References


[9] A.S. Bang. Om lingingen \( \Phi_n(x) = 0 \). Nyt Tidsskrift for Matematik, 6:6–12, 1895.


