# ABSTRACT

AL-KATEEB, ALA'A QASEM MOHAMMAD. Structures and Properties of Cyclotomic Polynomials. (Under the direction of Hoon Hong.)

The cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial in $\mathbb{Z}[x]$ whose zeros are the primitive $n$-th roots of unity. It has numerous application in number theory, abstract algebra and cryptography. Thus it is important to understand its structures and properties. In this dissertation, we report several newly found structures and properties of $\Phi_n$.

Let $n = mp$, where $m$ is an odd square-free integer and $p > m$ is a prime number. Let $q = \text{quo}(p, m)$ and $r = \text{rem}(p, m)$. Let $f_{m,p,i}$ be the $i$-th digit of $\Phi_{mp}$ in the radix $x^p$. Let $f_{m,p,i,j}$ be the $j$-th digit of $f_{m,p,i}$ in the radix $x^m$. Let $C_{m,p,i,j}$ be the list of coefficients of $f_{m,p,i,j}$.

The newly found structures are as follows:

1. $C_{m,p,i,0} = \cdots = C_{m,p,i,q-1}$.

2. $C_{m,p,i,q}$ is a truncation of $C_{m,p,i,0}$.

   $C_{m,p,i,q} = (1) \qquad \text{if } r = 1 \text{ and } i = 0$

   $C_{m,p,i,q} = (0) \qquad \text{if } r = 1 \text{ and } i > 0$

3. Let $p - \tilde{p} \equiv_m 0$. Then $C_{m,p,i,0} = C_{m,\tilde{p},i,0}$.

4. Let $p + \tilde{p} \equiv_m 0$. Then $C_{m,\tilde{p},i,0}$ is a negated/rotated version of $C_{m,p,i,0}$.

5. Let $i + \tilde{\imath} = \varphi(m) - 1$. Then $C_{m,p,\tilde{\imath},0}$ is a flipped/rotated version of $C_{m,p,i,0}$.

The newly found properties are as follows:

1. Norm:$\|\Phi_{mp}\|_k^k$ is linear over $p$'s that are equivalent modulo $m$. Moreover, $\|\Phi_{mp}\|_k^k$ and $\|\Phi_{m\tilde{p}}\|_k^k$ are parallel if $p+\tilde{p} \equiv_m 0$.

2. Middle term: Let $M(\Phi_{mp})$ denote the coefficient of the midterm of $\Phi_{mp}$. Then we have $M(\Phi_{mp}) = \pm M(\Phi_{m\tilde{p}})$ if $p \mp \tilde{p} \equiv_m 0$ and $M(\Phi_{mp}) = \pm 1$ if $p \equiv_m \pm 1$.

3. Number of terms: Let $\mathrm{Nt}_c(\Phi_{mp})$ denote the number of terms with the coefficient $c$ in $\Phi_{mp}$. Then $\mathrm{Nt}_c(\Phi_{mp})$ is linear over $p$'s that are equivalent modulo $m$. Moreover, $\mathrm{Nt}_c(\Phi_{mp})$ and $\mathrm{Nt}_{-c}(\Phi_{m\tilde{p}})$ are parallel if $p+\tilde{p} \equiv_m 0$.

4. Number of terms in $\Phi_{p_1p_2p_3}$: We provide explicit formulas for the number of terms in $\Phi_{p_1p_2p_3}$ for some special families of $p_1, p_2$ and $p_3$.

Structures and Properties of Cyclotomic Polynomials

by
Ala'a Qasem Mohammad Al-Kateeb

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Mathematics

Raleigh, North Carolina

2016

APPROVED BY:

| | |
|---|---|
| Eunjeong Lee | Ricky Liu |
| Seth Sullivant | Ernest Stitzinger |

Hoon Hong
Chair of Advisory Committee

# DEDICATION

I dedicate this work to my husband, Amer, who has been a constant source of support and encouragement during the challenges of graduate school, life and motherhood. I am very thankful to you for your help and constant support during that long and hard trip. I also dedicate it to my parents, my great father and my precious mother who have always loved me unconditionally, for their endless support and motivation. I dedicate it also to my siblings, and finally, to my three little angels: Sara, Mohammad and Salma.

# BIOGRAPHY

Al-Kateeb was born in Irbid a nice northern city in Jordan. She is a wife and a mother of three kids. She received her elementary and secondary education in Irbid, graduating in 2003. Al-Kateeb joined the math department at Yarmouk University in fall 2003. During her undergraduate studies she developed interests in Abstract algebra , number theory and the history of mathematics. Besides, Al-Kateeb has pursued interests in mathematics educational activities. In 2007, Al-Kateeb graduated with a B. S. in Mathematics and was on the top of her class. Al-Kateeb finished her master degree in Mathematic 2009 and then she worked as a mathematics teacher in a high school for one year. After that she worked as a mathematics lecturer in Yarmouk University in Jordan, the school that gave her a PhD scholarship. Al-Kateeb enrolled in the graduate program of NCSU in 2012. After graduation she will return back to Jordan to start her job as an assistant professor of mathematics.

## ACKNOWLEDGEMENTS

My utmost and most sincere gratitude goes to my advisor, Prof. Hoon Hong, for the continuous support of my Ph.D study and related research and for his patience, motivation, and immense knowledge. He helped me to learn how to think, organise my work and even more how to slowdown and control my stress.

My appreciation and utmost thanks goes to Prof. Eunjeong Lee whose help and collaborations was so precious and crucial in completing this dissertation and its related research.

My sincere thanks also goes to my doctoral committee, Prof. Ernie Stitzinger, Prof. Seth Sullivant, Dr. Ricky Liu and Prof. David Aspnes, for their insightful comments and encouragement.

I also would like to thank my friend and classmate Mary Ambrosino for the helpful discussions and also all my friends in the department especially Ranya Ali.

Finally, I would like to thank Yarmouk university for giving me the scholarship and supporting my study.

# TABLE OF CONTENTS

# LIST OF TABLES

# Chapter 1

# Introduction

In this dissertation, we study a fundamental family of polynomials in number theory, namely the family of cyclotomic polynomials. A cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial in $\mathbb{Z}[x]$ whose zeros are the primitive $n$-th roots of unity.

**Example 1.1.**

$$
\begin{aligned}
\Phi_1(x) &= -1 + x & \Phi_2(x) &= 1 + x \\
\Phi_3(x) &= 1 + x + x^2 & \Phi_4(x) &= 1 + x^2 \\
\Phi_5(x) &= 1 + x + x^2 + x^3 + x^4 & \Phi_6(x) &= 1 - x + x^2 \\
\Phi_7(x) &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 & \Phi_8(x) &= 1 + x^4 \\
\Phi_9(x) &= 1 + x^3 + x^6 & \Phi_{10}(x) &= 1 - x + x^2 - x^3 + x^4
\end{aligned}
$$

This set of polynomials has numerous application in number theory, abstract algebra and cryptography:

1. Some important theorems were proved using the properties of those polynomial

like:

   (a) Wedderburn's theorem for finite division rings (see [5]).

   (b) Proving a special case of Dirichlet's theorem on primes in arithmetic progressions (see [23]).

2. Some applications in cryptography:

   (a) investigating the efficiencies of certain class of cryptosystems (see[27])

   (b) constructing cryptosystems (see [34, 39])

Thus it is important to understand its structures and properties. In this dissertation, we report several newly found structures and properties.

In Chapter 2, we review the definition, various known structures and properties of cyclotomic polynomials. We also review the definition of inverse cyclotomic polynomials and summarize some of its basic properties needed in the subsequent chapters.

In Chapter 3, we investigate the structure of cyclotomic polynomials. Let $n = mp$ where $m$ is an odd square-free integer and $p > m$ is a prime number. Let $q = \mathrm{quo}(p, m)$ and $r = \mathrm{rem}(p, m)$. Let $f_{m,p,i}$ be the $i$-th"digit" of $\Phi_{mp}$ in the radix $x^p$. Let $f_{m,p,i,j}$ be the $j$-th "digit" of $f_{m,p,i}$ in the radix $x^m$. Let $C_{m,p,i,j}$ be the list of coefficients of $f_{m,p,i,j}$. Note that $C_{m,p,i,j}$ is a consecutive sub-list of the list of the coefficients of $\Phi_{mp}$. Hence they together form a partition of the list of the coefficients of $\Phi_{mp}$. We show the following structures on the partition (Theorem 3.1).

1. $C_{m,p,i,0} = \cdots = C_{m,p,i,q-1}$

2. $C_{m,p,i,q}$ is a truncation of $C_{m,p,i,0}$.

   $C_{m,p,i,q} = (1) \qquad \text{if } r = 1 \text{ and } i = 0$

$$C_{m,p,i,q} = (0) \qquad \text{if } r = 1 \text{ and } i > 0$$

3. Let $p - \tilde{p} \equiv_m 0$. Then $C_{m,p,i,0} = C_{m,\tilde{p},i,0}$.

4. Let $p + \tilde{p} \equiv_m 0$. Then $C_{m,\tilde{p},i,0}$ is a negated/rotated version of $C_{m,p,i,0}$.

5. Let $i + \tilde{\imath} = \varphi(m) - 1$. Then $C_{m,p,\tilde{\imath},0}$ is a flipped/rotated version of $C_{m,p,i,0}$.

We point out that the structural finding 1 was implicitly present in a recursive formula and resulting algorithms in Arnold and Monagan ([4] Section 4), but they did not make it explicit, maybe because their main concern was computational efficiency, not structural study. We have made it explicit because the explicit structure is useful for studying many other properties.

In Chapter 4, we investigate the norm of cyclotomic polynomial $\|\Phi_{mp}\|_k$. We show the following properties of norms (Theorem 4.1).

1. $\|\Phi_{mp}\|_k^k$ is linear over $p$'s that are equivalent modulo $m$.

2. $\|\Phi_{mp}\|_k^k$ and $\|\Phi_{m\tilde{p}}\|_k^k$ are parallel if $p + \tilde{p} \equiv_m 0$.

In Chapter 5, we investigate the middle term of a cyclotomic polynomial. Let $M(\Phi_{mp})$ denote the coefficient of the midterm of $\Phi_{mp}$. We show the following properties of midterms (Theorem 5.1).

1. $M(\Phi_{mp}) = \pm M(\Phi_{m\tilde{p}})$ if $p \mp \tilde{p} \equiv_m 0$.

2. $M(\Phi_{mp}) = \pm 1$ if $p \equiv_m \pm 1$.

In Chapter 6, we investigate the number of terms with prescribed coefficient in $\Phi_n$. Let $\mathrm{Nt}_c(\Phi_{mp})$ denote the number of terms with the coefficient $c$ in $\Phi_{mp}$. We show the following properties of number of terms (Theorem 6.1).

1. $\mathrm{Nt}_c(\Phi_{mp})$ is linear over $p$'s that are equivalent modulo $m$.

2. $\mathrm{Nt}_c(\Phi_{mp})$ and $\mathrm{Nt}_{-c}(\Phi_{m\tilde{p}})$ are parallel if $p + \tilde{p} \equiv_m 0$.

Finally, in Chapter 7, we study the number of terms in $\Phi_{p_1p_2p_3}$. We report the following findings on(Theorem 7.1). Suppose that $p_2 \equiv_{p_1} +1$ or $-1$. Then

1. $\mathrm{hw}(\Phi_{p_1p_2p_3}) = N \cdot (p_3 - 1) + 1 \qquad \text{if } p_3 \equiv_{p_1p_2} +1$

2. $\mathrm{hw}(\Phi_{p_1p_2p_3}) = N \cdot (p_3 + 1) - 1 \qquad \text{if } p_3 \equiv_{p_1p_2} -1$

where

$$N = \frac{2}{3}\frac{(p_1 - 1)\left((p_1 + 4)(p_2 - 1) - (r_2 - 1)\right)}{p_1p_2}$$

$$r_2 = \mathrm{rem}(p_2, p_1)$$

# Chapter 2

# Review

In this chapter we will review the definition and various known structures and properties of cyclotomic polynomials.

## 2.1 Cyclotomic polynomials

In this section we will define the cyclotomic polynomials and review some of their basic structures and properties.

Let $n$ be a positive integer. Then the zeros of $x^n - 1$ are all of the form $e^{\frac{2\pi ik}{n}}$ where $1 \leq k \leq n$,

$$x^n - 1 = \prod_{k=1}^{n}(x - e^{\frac{2\pi ik}{n}})$$

Let $R(n) = \{e^{\frac{2\pi ik}{n}}, k = 0, \cdots, n\}$ be the set of $n$-th roots of unity. Clearly $R(n)$ is an abelian group under multiplication. An $n$-th root of unity is called primitive if it is a generator of the group $R(n)$, i.e, $\gcd(k, n) = 1$.

**Definition 2.1** (Cyclotomic Polynomials)**.** *The cyclotomic polynomial* $\Phi_n$ *is defined to* *be the polynomial whose zeros are the primitive $n$-th roots of unity, i.e,*

$$\Phi_n = \prod_{\substack{\gcd(k,n)=1\\ 1\leq k\leq n}} (x - e^{\frac{2\pi i k}{n}})$$

**Example 2.1.** *Note*

| $n$ | $\Phi_n$ |
|---|---|
| 1 | $x - e^{2\pi i} = -1 + x$ |
| 2 | $x - e^{\frac{2\pi i}{2}} = x - (-1) = 1 + x$ |
| 3 | $(x - e^{\frac{\pi i}{3}}) \cdot (x - e^{\frac{2\pi i}{3}}) = (x + \frac{1}{2} - \frac{\sqrt{3}}{2}i) \cdot (x + \frac{1}{2} + \frac{\sqrt{3}}{2}i)) = 1 + x + x^2$ |
| 4 | $(x - e^{\frac{2\pi i}{4}}) \cdot (x - e^{\frac{6\pi i}{4}}) = (x - i) \cdot (x + i) = 1 + x^2$ |
| 5 | $(x - e^{\frac{2\pi i}{5}}) \cdot (x - e^{\frac{4\pi i}{5}}) \cdot (x - e^{\frac{6\pi i}{5}}) \cdot (x - e^{\frac{8\pi i}{5}}) = 1 + x + x^2 + x^3 + x^4$ |

Based on the last example, one might think that all coefficients of cyclotomic polynomials are either $\pm 1$ or 0, but this is not generally true. The first integer $n$ for which $\Phi_n$ has a coefficient different from $-1, 0$ or 1 is $n = 105$. That was found in 1883 by Migotti [35].

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

the coefficients of $x^7$ and $x^{41}$ equal $-2$.

Now review some basic structures and properties of $\Phi_n$. For this, we first recall two essential functions in number theory, Euler's and Möbius functions. Those functions are useful in proving many basic structures and properties of $\Phi_n$.

**Definition 2.2** (Euler's function)**.** *Let* $\varphi : \mathbb{Z} \to \mathbb{Z}$ *be the cardinality of* $\{k : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}$.

**Remark 2.1.** *From the definition of* $\varphi(n)$ *we can see that the degree of* $\Phi_n$ *is* $\varphi(n)$.

**Example 2.2.** *We have*

$$\begin{aligned} \varphi(1) &= 1, \ \varphi(2) &= 1 \\ \varphi(5) &= 4, \ \varphi(10) &= 8 \end{aligned}$$

**Lemma 2.1.** *Let* $n, m \in \mathbb{Z}$. *Then*

1. $n = \sum_{d|n} \varphi(d)$
2. *If* $\gcd(n, m) = 1$, *then* $\varphi(nm) = \varphi(n)\varphi(m)$
3. *If* $p$ *is prime, then* $\varphi(p^k) = p^k - p^{k-1}$
4. *If* $n = p_1^{e_1} \cdots p_k^{e_k}$ *is the prime factorization of* $n$, *then*

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

*Proof.* For proof see any elementary number theory textbook such as [15, 25, 37] $\square$

**Definition 2.3** (Möbius function $\mu$)**.** *The function* $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ *is defined by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 \cdots p_k \\ 0 & \text{otherwise} \end{cases}$$

*where* $p_i$*'s are distinct prime numbers.*

**Example 2.3.** *We have*

$$\begin{aligned}\mu(2) &= -1\\ \mu(6) &= 1\\ \mu(12) &= 0\end{aligned}$$

**Theorem 2.1** (Möbius Inversion Formula)**.** *Let $f, g : \mathbb{Z}^+ \to \mathbb{Z}^+$ be functions such that $f(n) = \prod_{d|n} g(d)$. Then $g(n) = \sum_{d|n} \left(f\left(\frac{n}{d}\right)\right)^{\mu(d)}$.*

*Proof.* Note

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

□

**Theorem 2.2.** *For $n \geq 1$,*

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

*Proof.* Let $\zeta$ be an $n$-th primitive root of unity such that $\zeta^d = 1$, then $\zeta$ is also a $d$-th root of unity and hence a root of $\Phi_d$. Since $d \mid n$ we have $\zeta$ is a root of $x^n - 1$. Since both polynomials $x^n - 1$ and $\prod_{d|n} \Phi_d(x)$ are monic and have same roots then they are equal. □

**Theorem 2.3.** *For $n \geq 1$ and $x \neq \pm 1$,*

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

*Proof.* We have from Theorem 2.2

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

Let $f(n) = x^n - 1$. Then by applying Theorem 2.1 on $f$ we have

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

□

**Example 2.4.** *Let $n = 45$. Then*

$$\begin{aligned}
\Phi_{45}(x) &= 1 - x^3 + x^9 - x^{12} + x^{15} + x^{24} \\
&= \prod_{d|45}(x^d - 1)^{\mu(\frac{45}{d})} \\
&= (x-1)^{\mu(45)}(x^3-1)^{\mu(15)}(x^5-1)^{\mu(9)}(x^9-1)^{\mu(5)}(x^{15}-1)^{\mu(3)}(x^{45}-1)^{\mu(1)} \\
&= (x^3-1)^1(x^9-1)^{-1}(x^{15}-1)^{-1}(x^{45}-1)
\end{aligned}$$

**Theorem 2.4.** *We have $\Phi_n = \Phi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})$.*

*Proof.*

$$\Phi_n = \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)} \qquad \text{by Theorem 2.3}$$

$$= \prod_{d|\mathrm{rad}(n)} (x^{\frac{n}{d}} - 1)^{\mu(d)} \qquad \text{since } \mu(k) = 0 \text{ if } \ k \text{ is not square free}$$

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

$$= \Phi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})$$

$\square$

**Theorem 2.5.** *If $n \geq 3$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$.*

*Proof.*

$$\begin{aligned}
\Phi_{2n}(x) &= \prod_{d|2n} (x^d - 1)^{\mu(\frac{2n}{d})} \\
&= \prod_{2|d} (x^d - 1)^{\mu(\frac{2n}{d})} \prod_{d|n} (x^d - 1)^{\mu(\frac{2n}{d})} && d \text{ is either odd or even} \\
&= \prod_{d|n} (x^d - 1)^{\mu(\frac{2n}{d})} (x^{2d} - 1)^{\mu(\frac{n}{d})} \\
&= \prod_{d|n} (x^d + 1)^{\mu(\frac{n}{d})} && \text{since } \mu(\frac{2n}{d}) = -\mu(\frac{n}{d}) \\
&= \prod_{d|n} (-x^d - 1)^{\mu(\frac{n}{d})} \\
&= \Phi_n(-x)
\end{aligned}$$

$\square$

**Theorem 2.6.** *Let $n \geq 2$ and $\Phi_n = \sum_{s=0}^{\varphi(n)} a_s x^s$. Then we have*

1. $\Phi_n = x^{\varphi(n)} \Phi_n(\frac{1}{x})$
2. $a_{\varphi(n)-s} = a_s$ *for* $0 \leq s \leq \varphi(n)$

*Proof.* Since complex roots are coming in pairs we can write

$$\Phi_n = \prod_{k=1}^{\lfloor \frac{n}{2} \rfloor} \left(x - e^{\frac{2\pi i k}{n}}\right) \cdot \left(x - e^{\frac{-2\pi i k}{n}}\right) = \prod_{k=1}^{\lfloor \frac{n}{2} \rfloor} (x^2 - 2x\cos\left(\frac{2\pi k}{n}\right) + 1)$$

Now

1. Note

$$\begin{aligned} x^{-\varphi(n)}\Phi_n(x) &= x^{-\varphi(n)} \prod_{k=1}^{\lfloor \frac{n}{2} \rfloor} (x^2 - 2x\cos\left(\frac{2\pi k}{n}\right) + 1) \\ &= \prod_{k=1}^{\lfloor \frac{n}{2} \rfloor} (x^{2-\varphi(n)} - 2x^{1-\varphi(n)}\cos\left(\frac{2\pi k}{n}\right) + x^{-\varphi(n)}) \\ &= \Phi_n(\frac{1}{x}) \end{aligned}$$

2. Note

$$\Phi_n = \sum_{s=0}^{\varphi(n)} a_s x^s = \sum_{s=0}^{\varphi(n)} a_s x^{\varphi(n)-s} = \sum_{s=0}^{\varphi(n)} a_{\varphi(n)-s} x^s$$

□

**Example 2.5.** *Let* $n = 15$*. Then* $\varphi(15) = 8$ *and*

$$\Phi_{15}(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8$$

*Note*

$$\begin{aligned} x^8\Phi_{15}(\frac{1}{x}) &= x^8(x^{-8} - x^{-7} + x^{-5} - x^{-4} + x^{-3} - x^{-1} + 1) \\ &= 1 - x + x^3 - x^4 + x^5 - x^7 + x^8 \\ &= \Phi_{15}(x) \end{aligned}$$

*Clearly*

$$a_0 = a_8 = 1 \qquad a_1 = a_7 = -1$$
$$a_2 = a_6 = 0 \qquad a_3 = a_5 = 1$$
$$a_4 = -1$$

**Example 2.6.** *We have*

1. $\Phi_3(x) = 1 + x + x^2$
2. $\Phi_9(x) = \Phi_3(x^3) = 1 + x^3 + x^6$
3. $\Phi_{18}(x) = \Phi_9(-x) = 1 - x^3 + x^6$

**Theorem 2.7.** $\Phi_n(x) \in \mathbb{Z}[x]$ *and monic.*

*Proof.* We prove the theorem by induction on $n$.

1. $\Phi_1 = x - 1 \in \mathbb{Z}[x]$.
2. Assume $\Phi_d \in \mathbb{Z}[x]$ and monic for all $d < n$.
3. Recall $x^n - 1 = \Phi_n \cdot (\prod_{d|n, d<n} \Phi_d)$. From the induction hypothesis, it follows that $\prod_{d|n,d<n} \Phi_d \in \mathbb{Z}$ and monic. From the definition of $\Phi_n$, obviously $\Phi_n$ a monic polynomial. Thus, $\Phi_n \in \mathbb{Q}[x]$ and monic. Since $x^n - 1 \in \mathbb{Z}[x]$ and monic, we conclude that $\Phi_n \in \mathbb{Z}[x]$.

$\square$

**Theorem 2.8.** $\Phi_n$ *is irreducible over* $\mathbb{Q}$.

*Proof.* There are many different proofs for this result. For $n$ is prime number there are proofs by Gauss (1801), Kronecter (1845) and Eisenstien (1850). For general integer $n$ there are Dedekind (1827), Landaue (1929) and Schure (1929). For more proofs and details one might see [41]. $\square$

**Theorem 2.9.** *For any $a \in \mathbb{Z}$ there exists $n \in \mathbb{N}$ such that $a$ is a coefficient of $\Phi_n$.*

*Proof.* Let $t$ be an odd integer such that $t > 2$. Then it is well known [38] that there exist $t$ distinct primes such that

$$p_1 < p_2 < \cdots < p_t$$

where $p_1 + p_2 > t$. Let $n = p_1 \cdots p_t$ and $p = p_t$. Then

$$\begin{aligned}
\Phi_n &= \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} \\
&= \prod_{i=1}^{t} \frac{(x^{p_1} - 1)}{(x - 1)} && \text{since } n \text{ is square free} \\
&\equiv_{x^{p+1}} \frac{(1 - x^p)}{(1 - x)} (1 - x^{p_1}) \cdots (1 - x^{p_{t-1}}) && t \text{ is odd} \\
&\equiv_{x^{p+1}} (1 + x + \cdots + x^{p-1})(1 - x^{p_1} - \cdots - x^{p_{t-1}}) && \text{since } p_j + p_k > p + 1
\end{aligned}$$

from the last product and the fact that each $p_i < p - 1$ we have $a_n(p) = -t + 1$, where $a_n(m)$ denotes the coefficient of $x^m$ in $\Phi_n(x)$. Let

$$S := \{a_n(m) |\ \forall\ n, m \in \mathbb{N}\}$$

Then we need to show that $S = \mathbb{Z}$. We do the following steps

1. Let $t = 2$, then $\{-1, 0, 1\} \subset S$.

2. For $t \geq 3$, we have $a_n(p) = -t + 1 \leq -2$. Thus $\{\ell \in \mathbb{Z}, \ell \leq -2\} \subset S$

3. Consider $\Phi_{2n}$ where $n$ is as defined above. Then $a_{2n}(p) = -a_n(p) = t - 1$. Thus since $t \geq 3$ we have $\{\ell \in \mathbb{Z}, \ell \geq 2\} \subset S$

Hence $S = \mathbb{Z}$ □

## 2.2 Structures of cyclotomic polynomials

Generally, there is no explicit non-recursive formula for computing the coefficients of $\Phi_n$. In this section we summarize some of the well-known formulas/descriptions for determining the structure of the polynomial $\Phi_n$.

**Definition 2.4.** *Let $n = p_1 \cdots p_k$ a product of $k$ distinct prime numbers. Then $\Phi_n$ is called a cyclotomic polynomial of order $k$.*

**Remark 2.2.** *$\Phi_{p_1p_2}$ and $\Phi_{p_1p_2p_3}$ are called binary $(k = 2)$ and ternary $(k = 3)$ cyclotomic polynomial respectively, the binary and ternary are the first non trivial cases that has been studied.*

The binary cyclotomic polynomial is the first non trivial case to be considered. There are many studies on these polynomials like [10, 13, 20, 26, 32]. The following theorem gives an explicit formula for $\Phi_{p_1p_2}$. It can be found in [32].

**Theorem 2.10.** *Let $s, r$ be integers such that $(p_1 - 1)(p_2 - 1) = rp_1 + sp_2$. Then*

$$\Phi_{p_1p_2} = \left(\sum_{i=0}^{r} x^{ip_1}\right)\left(\sum_{j=0}^{s} x^{jp_2}\right) - \left(\sum_{i=r+1}^{p_2-1} x^{ip_1}\right)\left(\sum_{j=s+1}^{p_1-1} x^{jp_2}\right) x^{-p_1p_2}$$

*Moreover, for any $0 \leq k \leq (p_1 - 1)(p_2 - 1)$ we have*

1. $a_k = 1$ *if and only if* $k = ip_1 + jp_2$ *for some* $i \in [0, r], j \in [0, s]$

2. $a_k = -1$ *if and only if* $k+p_1p_2 = ip_1+jp_2$ *for some* $i \in [r+1, p_2-1], j \in [s+1, p_1-1]$

3. $a_k = 0$ *otherwise*

*Proof.* Let

$$f(x) := \left(\sum_{i=0}^{r} x^{ip_1}\right)\left(\sum_{j=0}^{s} x^{jp_2}\right) - \left(\sum_{i=r+1}^{p_2-1} x^{ip_1}\right)\left(\sum_{j=s+1}^{p_1-1} x^{jp_2}\right) x^{-p_1p_2}$$

clearly $f \in \mathbb{Z}[x]$ is monic. We claim that $\deg(f) = \varphi(p_1p_2)$ and $f$ vanishes at each primitive $p_1p_2$-th root of unity.

The degree of the first product is $rp_1+sp_2 = \varphi(p_1p_2)$ and the degree of the second product is $(p_2-1)p_1 + (p_1-1)p_2 - p_1p_2 = p_1p_2 - p_1 - p_2 = \varphi(p_1p_2) - 1$ thus $\deg(f) = \varphi(p_1p_2)$. Let $\zeta$ be a primitive $p_1p_2$-th primitive root of unity. Then

$$\Phi_{p_1p_2}(\zeta) = 0 = \Phi_{p_1}(\zeta^{p_2}) = \Phi_{p_2}(\zeta^{p_1})$$

This implies that $\sum_{i=0}^{r}(\zeta^{p_1})^i = -\sum_{i=r+1}^{p_2-1}(\zeta^{p_1})^i$ and $\sum_{j=0}^{s}(\zeta^{p_2})^j = -\sum_{j=s+1}^{p_1-1}(\zeta^{p_2})^j$ Thus $f(\zeta) = 0$. Then $f(x) = \Phi_{p_1p_2}(x)$. All the monomials in $f$ are different to see that assume they are not different, then there exists $i_1, i_2 \in [0, p_2-1]$ and $j_1, j_2 \in [0, p_1-1]$ such that $i_1p_1 + j_1p_2 = i_2p_1 + j_2p_2$ or $i_2p_1 + j_2p_2 - p_1p_2$, then we have $p_2 \mid (i_1 - i_2)$. Hence $(i_1 = i_2)$, similarly $j_1 = j_2$. $\square$

Ternary cyclotomic polynomial is the second non trivial case to be considered. There are many studies on these polynomials like [6, 7, 12, 16, 18, 42] The following theorem gives some formulas for the coefficients $\Phi_{p_1p_2p_3}$. It can be found in [8, 14].

**Theorem 2.11.** *Let* $\Phi_n = \sum_{m=0}^{\varphi(n)} c_m x^m$ *. Then* $c_m$ *is determined by the number of partitions of* $m$ *of the form:*

$$m = a + \alpha p_1 p_2 + \beta p_1 p_3 + \gamma p_2 p_3 + \delta_1 p_2 + \delta_2 p_3$$

*where* $0 \leq a < p_1, \alpha, \beta, \gamma \geq 0$ *and* $\delta_i \in \{0, 1\}$*. If* $m$ *has no such partition, then* $c_m = 0$*. Each partition of* $m$ *in the given form contributes* $+1$ *to the value of* $c_m$ *if* $\delta_1 = \delta_2$*, but* $-1$ *if* $\delta_1 \neq \delta_2$*.*

In [1, 3, 4, 2], Arnold and Monagan gave recursive formulas for the coefficients of arbitrary cyclotomic polynomials. Using them, they also gave several algorithms. Below we review a recursive formula.

**Notation 2.1.** *Let*

$$\Phi_m = \sum_i b_i x^i \qquad \Psi_m = \sum_j c_j x^j \qquad \Phi_{mp} = \sum_k a_k x^k$$

**Theorem 2.12.** *We have*

$$a_k - a_{k-m} = -\sum_{ip+j=k} b_i c_j$$

*Proof.* Note

$$\begin{aligned}
\Phi_{mp}(x) &= \frac{\Phi_m(x^p)}{\Phi_m(x)} \\
&= \Phi_m(x^p)\Psi_m(x)(x^m - 1)^{-1} \\
&= -\Phi_m(x^p)\Psi_m(x)(1 - x^m)^{-1} \\
&= -\Phi_m(x^p)\Psi_m(x)\sum_{l \geq 0} x^{lm}
\end{aligned}$$

Thus

$$\sum_k a_k x^k = -\sum_i b_i x^{ip} \sum_j c_j x^j \sum_{l\geq 0} x^{lm} = -\sum_{\substack{i,j\\ l\geq 0}} b_i c_j x^{ip+j+lm} = -\sum_k \sum_{\substack{ip+j+lm=k\\ l\geq 0}} b_i c_j x^k$$

Thus

$$a_k = -\sum_{\substack{ip+j+lm=k\\ l\geq 0}} b_i c_j$$

Note

$$a_{k-m} = -\sum_{\substack{ip+j+lm=k-m\\ l\geq 0}} b_i c_j = -\sum_{\substack{ip+j+(l+1)m=k\\ l\geq 0}} b_i c_j = -\sum_{\substack{ip+j+lm=k\\ l\geq 1}} b_i c_j$$

Thus

$$a_k - a_{k-m} = -\sum_{\substack{ip+j+lm=k\\ l\geq 0}} b_i c_j + \sum_{\substack{ip+j+lm=k\\ l\geq 1}} b_i c_j = -\sum_{\substack{ip+j+lm=k\\ l=0}} b_i c_j = -\sum_{ip+j=k} b_i c_j$$

□

## 2.3 Property: norm

The Norm of a mathematical object (polynomial, matrix , vector, etc) is a measuring tool for the size or length of that object, in this section we will define the norm for $\Phi_n$.

**Notation 2.2** (Norm of a polynomial)**.** *Let $f = a_0 + \cdots + a_n x^n$. Then the k-norm of $f$ is defined by*

$$\|f\|_k = \begin{cases} \left(\sum_{j=0}^{n} |a_j|^k\right)^{\frac{1}{k}} & \text{if } k < \infty \\ \max\{|a_j|, j = 0, \cdots, n\} & \text{if } k = \infty \end{cases}$$

**Example 2.7.** *Let $f = x^3 - 2x^2 + 5x - 3$. Then*

1. $\|f\|_1 = |1| + |-2| + |5| + |-3| = 11$

2. $\|f\|_2 = (|1|^2 + |-2|^2 + |5|^2 + |-3|^2)^{\frac{1}{2}} = (39)^{\frac{1}{2}} = 6.245$

**Remark 2.3** (Height). *Note that $\|\Phi_n\|_\infty = h(\Phi_n) = \max\{|a_j|, j = 0, \cdots, n\}$, the height of $\Phi_n$. $\Phi_n$ is called flat when $h(\Phi_n) = 1$. The flatness of cyclotomic polynomial has been studied heavily and there are many open problems in that area [11, 17, 29, 31, 42], also there are many studies regarding the height of $\Phi_n$ such as [7, 9, 16, 22, 30, 33, 40, 43].*

In [21], Carlitz proved the following theorem for $\|\Phi_{np}\|_2^2$, where $n$ is a square-free odd integer and $p$ is a prime number. We will extend this result to $\|\Phi_{np}\|_k^k$ in Chapter 4

**Theorem 2.13** (Carlitz). *Let $r = \mathrm{rem}(p, n)$. Then*

$$\|\Phi_{np}\|_2^2 = A_{n,r}p + B_{n,r}$$

*where $A_{n,r}, B_{n,r} \in \mathbb{Q}$ and depends only on $n$ and $r$.*

## 2.4 Property: middle term

In this section we define the middle term of $\Phi_n$ and present its well-known properties

**Notation 2.3.** *$M(\Phi_n) =$ the coefficient of $x^{\frac{\varphi(n)}{2}}$ in $\Phi_n$, middle term of $\Phi_n$.*

**Example 2.8.** *Note*

| $n$ | $\Phi_n$ | $M(\Phi_n)$ |
|---|---|---|
| $p$ | $1 + \cdots + x^{p-1}$ | 1 |
| 8 | $1 + x^4$ | 0 |
| 15 | $1 - x + x^3 - x^4 + x^5 - x^7 + x^8$ | $-1$ |
| 21 | $1 - x + x^3 - x^4 + x^6 - x^8 + x^9 - x^{11} + x^{12}$ | 1 |

It has been shown that $M(\Phi_{p_1p_2}) = \pm 1$ this result can be found in [10, 32], however, this is not true when $n$ is a multiple of three primes or more, for example $M(\Phi_{385}) = -3, M(\Phi_{4785}) = 5$ and $M(\Phi_{7735}) = -7$.

**Theorem 2.14.** *$M(\Phi_{p_1p_2}) = (-1)^r$, where $r$ is $(p_1-1)(p_2-1) = rp_1 + sp_2$.*

*Proof.* Let $(p_1-1)(p_2-1) = rp_1 + sp_2$, $r$ and $s$ are both even or both odd otherwise $rp_1 + sp_2 = (p_1-1)(p_2-1)$ will be odd. Let $\ell = \frac{(p_1-1)(p_2-1)}{2}$. Then we consider the following cases:

1. If $r$ and $s$ are even, then $\ell = (\frac{r}{2})p_1 + (\frac{s}{2})p_2$ and then by theorem 2.10 on page 14 we have $a_\ell = 1 = (-1)^r$.

2. If $r$ and $s$ are odd, then we can write $\ell + p_1p_2 = rp_1 + sp_2 + p_1p_2 = (\frac{r+p_2}{2})p_1 + (\frac{s+p_1}{2})p_2$, now $\frac{r+p_2}{2} \in [r+1, p_2-1]$ and $\frac{s+p_1}{2} \in [s+1, p_1-1]$ since $r \leq p_2 - 1$ and $s \leq p_1 - 2$. Thus by theorem 2.10 on page 14 $a_\ell = -1 = (-1)^r$.

3. If $p_1 = 2$, then $r = \frac{p_2-1}{2} = \ell$ and $s = 0$. $\Phi_{2p_2} = \Phi_{p_2}(-x) = \sum_{i=0}^{p_2-1}(-x)^i$, here $a_\ell = (-1)^\ell = (-1)^r$

$\square$

Generally, the value of $M(\Phi_n)$ is a point of interest. It has been shown in [24] that $M(\Phi_n)$ is either zero or an odd integer.

**Theorem 2.15** (Dredsen)**.** *For $n \geq 3$ the middle coefficient of $\Phi_n$ is either zero (when $n$ is a power of 2) or an odd integer.*

## 2.5 Property: number of terms

In this section we will discuss the number of terms with prescribed coefficient in $\Phi_n$

**Notation 2.4.** *Let $f$ be a polynomial. Then $\mathrm{Nt}_c(f)$ denotes the number of terms with the coefficient $c$ in $f$.*

**Example 2.9.** *Note*

| $c$ | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $\mathrm{Nt}_c(\Phi_5)$ | 0 | 0 | 0 | 5 | 0 |
| $\mathrm{Nt}_c(\Phi_7)$ | 0 | 0 | 0 | 7 | 0 |
| $\mathrm{Nt}_c(\Phi_{15})$ | 0 | 3 | 2 | 4 | 0 |
| $\mathrm{Nt}_c(\Phi_{35})$ | 0 | 8 | 8 | 9 | 0 |
| $\mathrm{Nt}_c(\Phi_{105})$ | 2 | 13 | 16 | 18 | 0 |
| $\mathrm{Nt}_c(\Phi_{165})$ | 0 | 33 | 24 | 14 | 10 |

**Notation 2.5.** *Let $\Phi_n = \sum_{s=0}^{\varphi(n)} a_s x^s$. Then we denote*

1. *$C(\Phi_n) = \{a_s : s = 0, \ldots, \varphi(n)\}$, that is, the set of all the coefficients of $\Phi_n$.*

2. *$\mathrm{hw}(\Phi_n)$ be the number of nonzero terms of $\Phi_n$.*

**Remark 2.4.** $\mathrm{hw}(\Phi_\mathrm{n}) = \sum_{0 \neq c \in C(\Phi_n)} \mathrm{Nt_c}(\Phi_n) = \varphi(n) + 1 - \mathrm{Nt}_0(\Phi_n)$.

$\mathrm{hw}(\Phi_{p_1 p_2})$ has been found by Carlitz [20] but $\mathrm{hw}(\Phi_n)$ where $n$ is a product of three primes or more is still an open problem.

**Theorem 2.16** (Carlitz)**.** *Let* $n = p_1 \cdot p_2$. *Then*

$$\mathrm{hw}(\Phi_{p_1 p_2}) = 2\bar{p_1} \cdot \bar{p_2} - 1.$$

*where* $p_1 \cdot \bar{p_1} \equiv_{p_2} p_2 - 1$ *and* $p_2 \cdot \bar{p_2} \equiv_{p_1} p_1 - 1$.

*Proof.* Let $\theta(p_1p_2) = \#\{0 \leq i \leq \varphi(p_1p_2) : c_i = 1\}$. Since all the coefficients of $\Phi_{p_1p_2}$ are either $-1, 0$ or $1$ and $\Phi_{p_1p_2}(1) = 1$, we have

$$\theta(p_1p_2) = 1 + \#\{0 \leq i \leq \varphi(p_1p_2) : c_i = -1\}$$

Now

$$\begin{aligned}
\Phi_{p_1p_2} &= \frac{(1-x)(1-x^{p_1p_2})}{(1-x^{p_1})(1-x^{p_2})} \\
&= \frac{1-x}{1-x^{p_1}} \sum_{j=0}^{p_1-1} x^{jp_2} \\
&= \frac{1}{1-x^{p_1}} \left( \sum_{j=0}^{p_1-1} x^{jp_2} - \sum_{i=0}^{p_1-1} x^{ip_2+1} \right)
\end{aligned}$$

Since $\Phi_{p_1p_2}$ is a polynomial then each $x^{jp_2}$ associate a term $x^{ip_2+1}$ such that $ip_2+1 \equiv_{p_1} jp_2$ in other words

$$(x^{p_1} - 1) \mid (x^{jp_2} - x^{ip_2+1})$$

Hence

$$(i-j)p_2 \equiv_{p_1} -1$$

so $i - j = -\bar{p_2}$. Then

$$\begin{aligned}
\Phi_{p_1p_2} &= \frac{1}{1-x^{p_1}} \left( \sum_{j=0, j-\bar{p_2}<p_1}^{p_1-1} \left(x^{jp_2} - x^{(j-\bar{p_2})p_2+1}\right) - \sum_{j=0, j-\bar{p_2}\geq p_1}^{p_1-1} \left(x^{jp_2} - x^{(j-\bar{p_2}-p_1)p_2+1}\right) \right) \\
&= \frac{1}{1-x^{p_1}} \left( \left(1 - x^{\bar{p_2}p_2+1}\right) \sum_{j=0}^{p_1-1+\bar{p_2}} x^{jp_2} - \left(1 - x^{(p_1+\bar{p_2})p_2-1}\right) \sum_{i=0}^{p_1-1+\bar{p_2}} x^{ip_2+1} \right)
\end{aligned}$$

the first part gives the positive terms and the second one gives the negative ones, clearly

$$\theta(p_1p_2) = \frac{(p_1+\bar{p_2})(1-p_2\bar{p_2})}{p_1}$$

Hence

$$\begin{aligned}\mathrm{hw}(\Phi_{p_1p_2}) &= 2\theta(p_1p_2) - 1\\ &= 2\frac{(p_1+\bar{p_2})(1-p_2\bar{p_2})}{p_1} - 1\\ &= 2\cdot\bar{p_1}\cdot\bar{p_2} - 1\end{aligned}$$

since $p_2\cdot(p_1+\bar{p_2}) \equiv_{p_1} p_1 - 1$ and $p_1\cdot\frac{1-p_2\bar{p_2}}{p_1} \equiv_{p_2} p_2 - 1$. □

**Example 2.10.** *Let* $p_1 = 3$. *Then*

$$\begin{aligned}\mathrm{hw}(\Phi_{3p_2}) &= 2\cdot\bar{3}\cdot\bar{p_2} - 1\\ &= \begin{cases} 2\cdot\bar{3}-1 & p_2 \equiv_3 1\\ 4\cdot\bar{3}-1 & p_2\equiv_3 2\end{cases}\end{aligned}$$

## 2.6 Inverse cyclotomic polynomials

In this section we define the inverse cyclotomic polynomial $\Psi_n$ and present some of its basic properties. As $\Phi_n$ is defined as the monic polynomial whose zeros are the primitive $n$-th roots of unity, $\Psi_n$ is defined to be the monic polynomial whose zeros are the non primitive $n$-th roots of unity. There are some recent studies on the inverse cyclotomic polynomials [19, 28, 36].

**Definition 2.5** (Inverse cyclotomic polynomial)**.** *The inverse cyclotomic polynomial*

$\Psi_n(x)$ *is defined to be the monic polynomial of degree* $\psi(n)$ *such that*

$$\Psi_n = \prod_{\substack{gcd(k,n)>1 \\ 1\le k\le n}} (x - e^{\frac{2\pi ik}{n}})$$

**Example 2.11.** *Consider some cases with small values of* $n$*.*

- $n = 1 : \Psi_1 = \frac{x-1}{\Phi_1} = 1$
- $n = 2 : \Psi_2 = \frac{x^2-1}{x+1} = -1 + x$
- $n = 4 : \Psi_4 = \frac{x^4-1}{x^2+1} = -1 + x^2$
- $n = 3 : \Psi_3 = \frac{x^3-1}{x^2+x+1} = -1 + x$

**Lemma 2.2.** *We have*

$$\Psi_n = -\prod_{\substack{k|n \\ k<n}} (1 - x^k)^{-\mu(\frac{n}{k})}$$

**Lemma 2.3.** *We have*

1. $\Psi_{2n} = (1 - x^n) \cdot \Psi_n(-x)$ *if* $n$ *is odd.*
2. $\Psi_{np} = \Psi_n(x^p)$ *if* $p \mid n$*.*
3. $\Psi_{np} = \Psi_n(x^p) \cdot \Phi_n$ *if* $p \nmid n$*.*
4. $\Psi_n = \Psi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})$*.*
5. $\Psi_n = -\Psi_n(\frac{1}{x}) \cdot x^{n-\varphi(n)}$*.*

*Proof.*

1. $\Psi_{2n} = \frac{x^{2n}-1}{\Phi_{2n}} = \frac{x^{2n}-1}{\Phi_n(-x)} = (x^{2n} - 1)\frac{\Psi_n(-x)}{-(x^n+1)} = (1 - x^n)\Psi_n(-x)$.

2. $\Psi_{np} = \frac{x^{np}-1}{\Phi_{np}} = \frac{x^{np}-1}{\Phi_n(x^p)} = \frac{(x^p)^n-1}{\Phi_n(x^p)} = \Psi_n(x^p)$.

3. $\Psi_{np} = \frac{x^{np}-1}{\Phi_{np}} = \frac{x^{np}-1}{\Phi_n(x^p)}\Phi_n = \Psi_n(x^p)\Phi_n$.

4. $\Psi_n = \frac{x^n-1}{\Phi_n} = \frac{x^n-1}{\Phi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})} = \frac{(x^{\frac{n}{\mathrm{rad}(n)}})^{\mathrm{rad}(n)}-1}{\Phi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})} = \Psi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}})$.

5. $\Psi_n(\frac{1}{x}) = \frac{(\frac{1}{x})^n-1}{\Phi_n(\frac{1}{x})} = \frac{1-x^n}{x^n\Phi_n(\frac{1}{x})} = \frac{1-x^n}{x^{n-\varphi(n)}\Phi_n} = -\frac{\Psi_n}{x^{n-\varphi(n)}}$, hence $\Psi_n = -\Psi_n(\frac{1}{x}) \cdot x^{n-\varphi(n)}$

$\square$

**Proposition 2.1.** *We have*

*1.* $\Psi_p = -1 + x$.

*2.* $\Psi_{p_1p_2} = (-1 + x^{p_2}) \cdot \Phi_{p_1}$.

# Chapter 3

# Structures

## Introduction

In this chapter, we investigate the structure of cyclotomic polynomials.

Let $m$ be an odd square-free positive integer and $p$ be a prime number such that[1] $p > m$. Let $q = \mathrm{quo}(p, m)$ and $r = \mathrm{rem}(p, m)$, the quotient and the reminder of $p$ divided by $m$ respectively. Let $f_{m,p,i}$ be the $i$-th"digit" of $\Phi_{mp}$ in the radix $x^p$. Let $f_{m,p,i,j}$ be the $j$-th "digit" of $f_{m,p,i}$ in the radix $x^m$. Let $C_{m,p,i,j}$ be the list of coefficients of $f_{m,p,i,j}$. Note that $C_{m,p,i,j}$ is a consecutive sub-list of the list of the coefficients of $\Phi_{mp}$. Hence they together form a partition of the list of the coefficients of $\Phi_{mp}$. We show the following structures on the partition (Theorem 3.1).

1. $C_{m,p,i,0} = \cdots = C_{m,p,i,q-1}$

2. $C_{m,p,i,q}$ is a truncation of $C_{m,p,i,0}$.

   $C_{m,p,i,q} = (1) \qquad \text{if } r = 1 \text{ and } i = 0$

[1] The case $p < m$ turns out to be uninteresting from certain structural point of view.

$C_{m,p,i,q} = (0) \qquad \text{if } r = 1 \text{ and } i > 0$

3. Let $p - \tilde{p} \equiv_m 0$. Then $C_{m,p,i,0} = C_{m,\tilde{p},i,0}$.

4. Let $p + \tilde{p} \equiv_m 0$. Then $C_{m,\tilde{p},i,0}$ is a negated/rotated version of $C_{m,p,i,0}$.

5. Let $i + \tilde{\imath} = \varphi(m) - 1$. Then $C_{m,p,\tilde{\imath},0}$ is a flipped/rotated version of $C_{m,p,i,0}$.

We point out that the structural finding 1 was implicitly present in a recursive formula and resulting algorithms in Arnold and Monagan ([4] Section 4), but they did not make it explicit, maybe because their main concern was computational efficiency, not structural study. We have made it explicit because the explicit structure is useful for studying many other properties.

## 3.1 Main results

In this section, we will state the main results of this chapter precisely. We will use the following notations.

**Notation 3.1** (Partition)**.** *Let* $\Phi_{mp} = \sum_{v\geq 0} c_v x^v$. *For* $0 \leq i \leq \varphi(m) - 1$ *and* $0 \leq j \leq q$, *let*

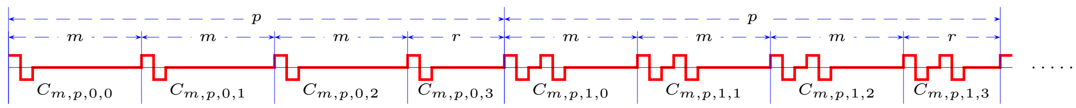
$$C_{m,p,i,j} := (c_{ip+jm}, \ldots, c_{ip+jm+l})$$

*where if* $j < q$ *then* $l = m - 1$ *else* $l = r - 1$.

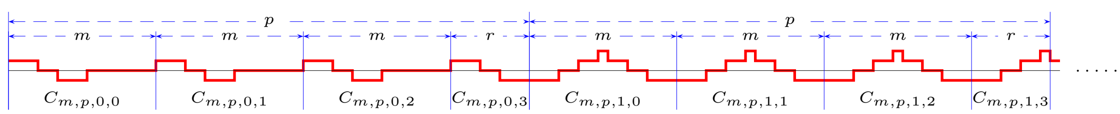
We will illustrate the idea of partition by the following two examples.

**Example 3.1.** *We will visualize a polynomial by a graph where the horizonal axis stands for the exponents and the vertical axis stands for the corresponding coefficients.*

*Let $m = 11$ and $p = 41$. Then $\phi(m) - 1 = 9$, $q = 3$ and $r = 8$. The partition of the list of the coefficients of $\Phi_{mp}$ into $C_{m,p,i,j}$'s is illustrated by the following diagram.*




**Example 3.2.** *We will visualize a polynomial by a graph where the horizonal axis stands for the exponents and the vertical axis stands for the corresponding coefficients.*
*Let $m = 15$ and $p = 53$. Then $\phi(m) - 1 = 7$, $q = 3$ and $r = 8$. The partition of the list of the coefficients of $\Phi_{mp}$ into $C_{m,p,i,j}$'s is illustrated by the following diagram.*




We need to define some operations on $C_{m,p,i,j}$'s.

**Notation 3.2** (Operation)**.** *For $A = (a_0, \ldots a_{m-1})$ and $0 \leq s < m$, let*

1. $\mathcal{T}_s A := (a_0, \ldots, a_{s-1})$ *"Truncate from the s-th element"*

2. $\mathcal{N} A := (-a_0, \ldots, -a_{m-1})$ *"Negate"*

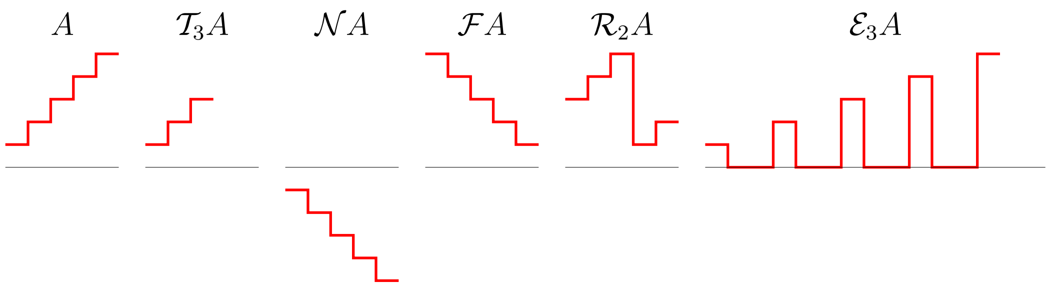
3. $\mathcal{F} A := (a_{m-1}, \ldots, a_0)$ *"Flip"*

4. $\mathcal{R}_s A := (a_s, \ldots, a_{m-1}, a_0, \ldots, a_{s-1})$ *"Rotate by s"*

5. $\mathcal{E}_s A := (a_0, 0, \ldots, 0, a_1, 0, \ldots, 0, \ldots, a_{m-1})$ *"Expand by s"*

   *where $s - 1$ zeros are padded between two consecutive elements*

**Example 3.3** (Operation). *Let* $A = (1, 2, 3, 4, 5)$. *Then*




We can now state the main theorem of this chapter regarding $C_{m,p,i,j}$'s.

**Theorem 3.1** (Structure). *We have*

1. $C_{m,p,i,0} = \cdots = C_{m,p,i,q-1}$

2. $C_{m,p,i,q} = \mathcal{T}_r C_{m,p,i,0}$

   $C_{m,p,i,q} = (1)$ *if* $r = 1$ *and* $i = 0$

   $C_{m,p,i,q} = (0)$ *if* $r = 1$ *and* $i > 0$

3. $C_{m,\tilde{p},i,0} = C_{m,p,i,0}$ *if* $\tilde{p} - p \equiv_m 0$

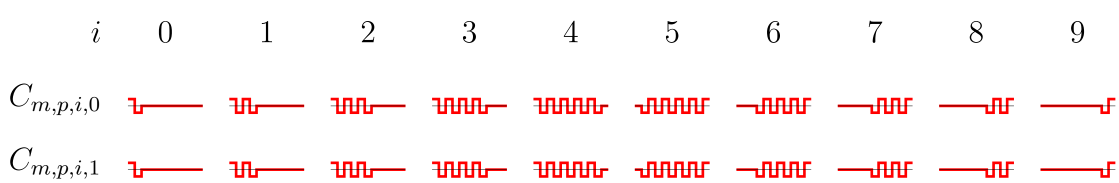
4. $C_{m,\tilde{p},\tilde{\imath},0} = \mathcal{R}_r \mathcal{N} C_{m,p,i,0}$ *if* $\tilde{p} + p \equiv_m 0$ *and* $\tilde{\imath} + i = \varphi(m) - 1$

5. $C_{m,p,\tilde{\imath},0} = \mathcal{R}_{\tilde{r}} \mathcal{F} C_{m,p,i,0}$ *if* $\tilde{\imath} + i = \varphi(m) - 1$ *and* $\tilde{r} + r \equiv_m \varphi(m) - 1$, $0 \le \tilde{r} < m$

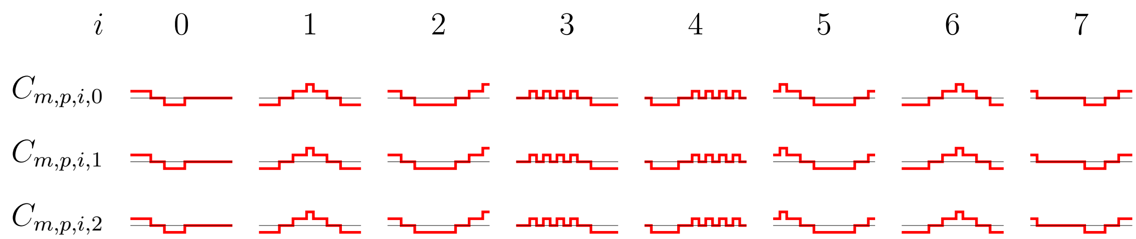
Now we present a set of examples to illustrate the main theorem.

**Example 3.4** (Structure 1). *Let* $m = 11$ *and* $p = 31$. *Then* $\varphi(m) - 1 = 9$

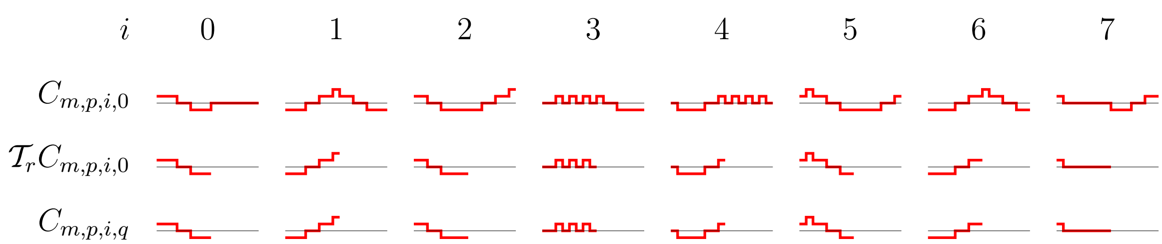
*and* $q = 2$. *Note*



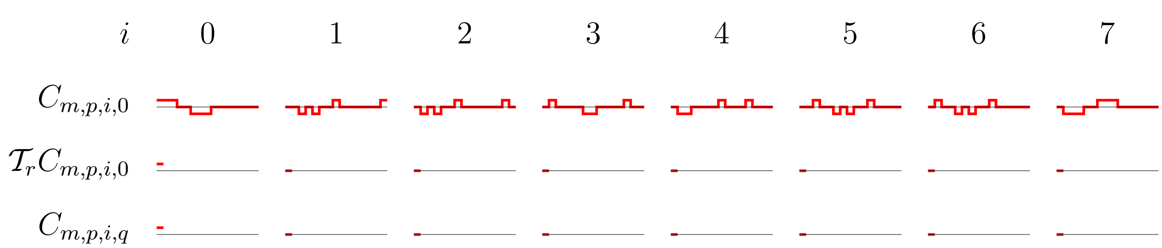
**Example 3.5** (Structure 1)**.** *Let* $m = 15$ *and* $p = 53$*. Then* $\varphi(m) - 1 = 7$ *and* $q = 3$*. Note*




**Example 3.6** (Structure 2)**.** *Let* $m = 15$ *and* $p = 53$*. Then* $\varphi(m) - 1 = 7$*,* $q = 3$ *and* $r = 8$*. Note*

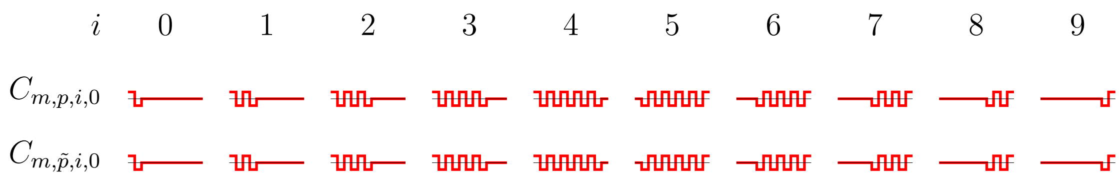



**Example 3.7** (Structure 2)**.** *Let* $m = 15$ *and* $p = 31$*. Then* $\varphi(m) - 1 = 7$*,* $q = 2$ *and* $r = 1$*. Note*



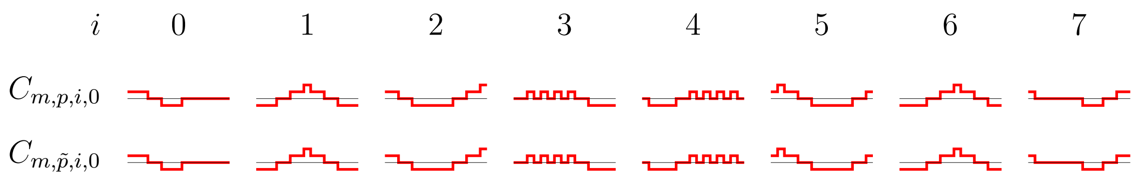

**Example 3.8** (Structure 3)**.** *Let* $m = 11$*,* $p = 31$ *and* $\tilde{p} = 53$*.*

*Then* $\varphi(m) - 1 = 9$*. Note*



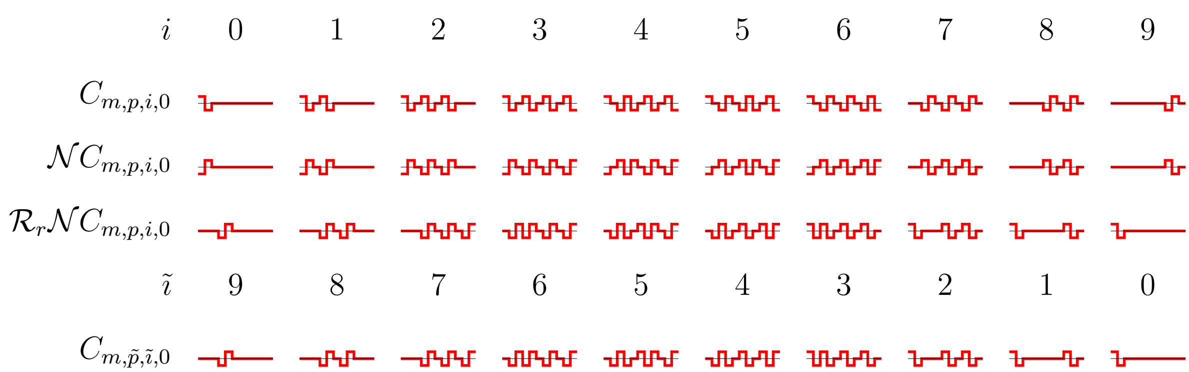

**Example 3.9** (Structure 3)**.** *Let* $m = 15$*,* $p = 53$ *and* $\tilde{p} = 83$*.*

*Then* $\varphi(m) - 1 = 7$*. Note*



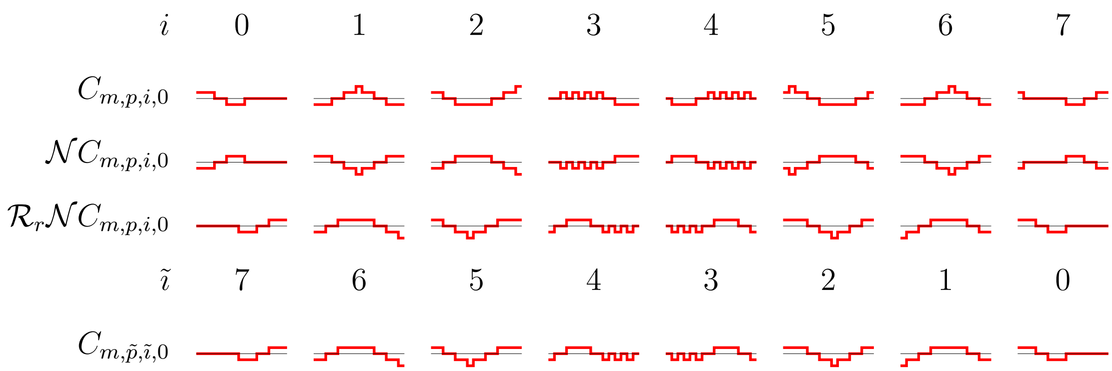

**Example 3.10** (Structure 4)**.** *Let* $m = 11$*,* $p = 41$ *and* $\tilde{p} = 47$*.*

*Then* $\varphi(m) - 1 = 9$ *and* $r = 8$*. Note*



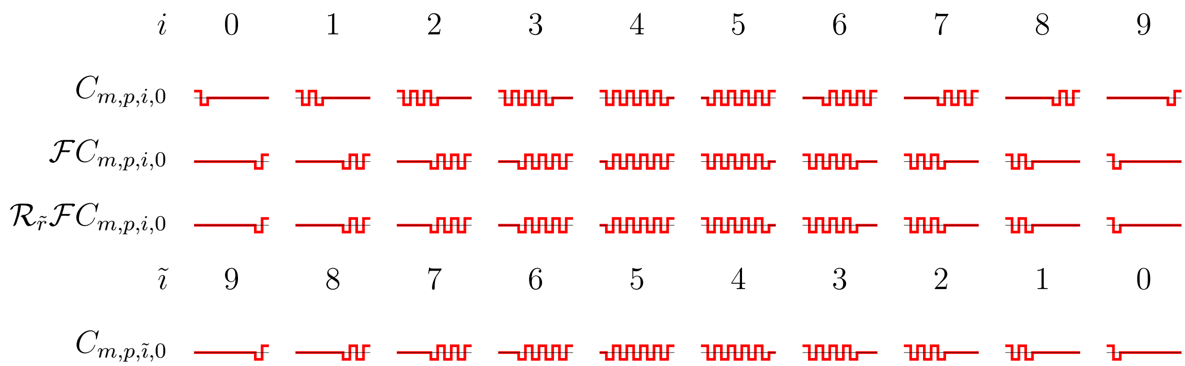

**Example 3.11** (Structure 4)**.** *Let* $m = 15$*,* $p = 53$ *and* $\tilde{p} = 37$*.*

*Then $\varphi(m) - 1 = 7$ and $r = 8$. Note*



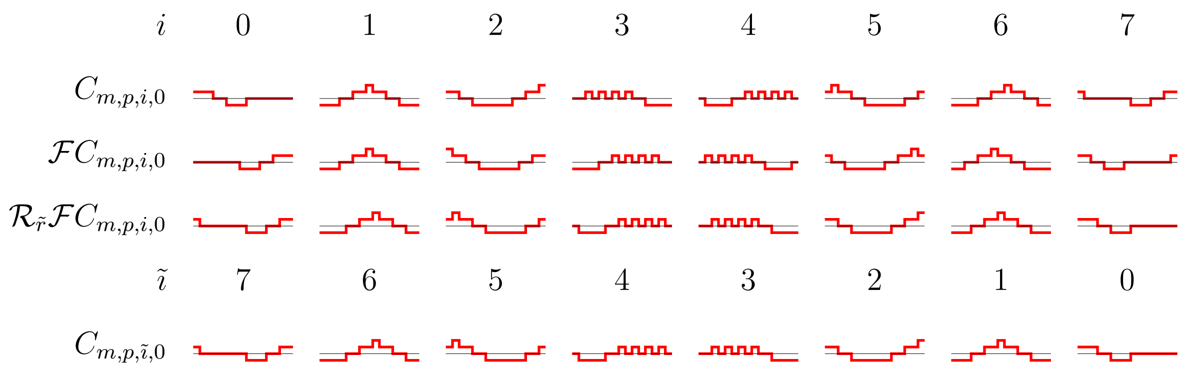

**Example 3.12** (Structure 5)**.** *Let $m = 11$ and $p = 31$.*

*Then $\varphi(m) - 1 = 9$, $r = 9$ and $\tilde{r} = 0$. Note*




**Example 3.13** (Structure 5)**.** *Let $m = 15$ and $p = 53$.*

*Then* $\varphi(m) - 1 = 7$*,* $r = 8$ *and* $\tilde{r} = 14$*. Note*




## 3.2 Proofs

In this section we prove Theorem 3.1. Previously we defined $C_{m,p,i,j}$ as a list of coefficients. However, it will be useful to have them in polynomial format, because it is easier to work with polynomials rather than lists. Hence we begin by reformulating Notations 3.1 and 3.2 in terms of polynomials.

**Notation 3.3** (Partition)**.** *Let* $f_{m,p,i}$ *be the* $i$*-th digit of* $\Phi_{mp}$ *in the radix* $x^p$ *and let* $f_{m,p,i,j}$ *be the* $j$*-th digit of* $f_{m,p,i}$ *in the radix* $x^m$*, that is,*

$$\Phi_{mp} = \sum_{i=0}^{\varphi(m)-1} f_{m,p,i}\ x^{ip}$$

$$f_{m,p,i} = \sum_{i=0}^{q} f_{m,p,i,j}\ x^{jm}$$

**Lemma 3.1.** $C_{m,p,i,j}$ *is the list of the coefficients of* $f_{m,p,i,j}$*, that is,*

$$f_{m,p,i,j} = \sum_{k=0}^{l} c_{ip+mj+k} x^k$$

*where if $j < q$ then $l = m - 1$ else $l = r - 1$.*

*Proof.* Immediate from comparing Notations 3.1 and 3.3. $\square$

**Example 3.14.** *Let $m = 5$ and $p = 13$. Then*

$$\begin{aligned}\Phi_{5\cdot 13} = 1 &- x + x^5 - x^6 + x^{10} - x^{11} + x^{13} - x^{14} + x^{15} - x^{16} + x^{18} - x^{19} \\ &+ x^{20} - x^{21} + x^{23} - x^{24} + x^{25} - x^{27} + x^{28} - x^{29} + x^{30} - x^{32} + x^{33} \\ &- x^{34} + x^{35} - x^{37} + x^{38} - x^{42} + x^{43} - x^{47} + x^{48}\end{aligned}$$

*Hence*

$$\begin{aligned} f_{5,13,0,0} &= 1 - x & f_{5,13,0,2} &= 1 - x \\ f_{5,13,1,0} &= 1 - x + x^2 - x^3 & f_{5,13,1,2} &= 1 - x + x^2 \\ f_{5,13,2,0} &= -x + x^2 - x^3 + x^4 & f_{5,13,2,2} &= -x + x^2 \\ f_{5,13,3,0} &= -x^3 + x^4 & f_{5,13,3,2} &= 0 \end{aligned}$$

**Notation 3.4** (Operation)**.** *For $f = a_0 + \cdots + a_{m-1}x^{m-1}$ and $0 \le s < m$, let*

1. $\mathcal{T}_s f := a_0x^0 + \cdots + a_{s-1}x^{s-1}$
2. $\mathcal{N} f := -a_0x^0 - \cdots - a_{m-1}x^{m-1}$
3. $\mathcal{F} f := a_{m-1}x^0 + \cdots + a_0x^{m-1}$
4. $\mathcal{R}_s f := a_sx^0 + \cdots + a_{m-1}x^{(m-1-s)} + a_0x^{(m-s)} + \cdots + a_{s-1}x^{m-1}$
5. $\mathcal{E}_s f := a_0x^0 + a_1x^s + \cdots + a_{m-1}x^{s(m-1)}$

**Lemma 3.2.** *Let $f$ be a polynomial of degree less than $m$ and $0 \leq s < m$. Then we have*

1. $\mathcal{T}_s f = \mathrm{rem}(f, x^s)$

2. $\mathcal{N} f = -f$

3. $\mathcal{F} f = x^{m-1} f\left(x^{-1}\right)$

4. $\mathcal{R}_s f = \mathrm{rem}(x^{m-s} f, x^m - 1)$

5. $\mathcal{E}_s f = f(x^s)$

*Proof.* Immediate from Notation 3.4. $\square$

**Example 3.15.** *Let $f = 1 - 3x + x^2 - 2x^3 + x^5, m = 6$ and $s = 3$. Then we have*

1. $\mathcal{T}_3 f = \mathrm{rem}(f, x^3) = 1 - 3x^2 + x^2$

2. $\mathcal{N} f = -f = -1 + 3x - x^2 + 2x^3 - x^5$

3. $\mathcal{F} f = x^5 f\left(x^{-1}\right) = 1 - 2x^2 + x^3 - 3x^4 + x^5$

4. $\mathcal{R}_3 f = \mathrm{rem}(x^3 f, x^6 - 1) = -2 + x^2 + x^3 - 3x^4 + x^5$

5. $\mathcal{E}_3 f = f(x^3) = 1 - 3x^3 + x^6 - 2x^9 + x^{15}$

**Proposition 3.1.**

1. $\mathrm{rem}\left(i(m-r), m\right) = m - \mathrm{rem}\left(ir, m\right)$

2. $x^{\mathrm{rem}(\square, m)} = \mathrm{rem}\left(x^{\square}, x^m - 1\right)$

*Proof.* Obvious. $\square$

**Lemma 3.3.** *We have*

$$\Phi_{mp} = -\ \Phi_m\left(x^p\right)\ G$$

*where*

$$G = \Psi_m\ \sum_{u\geq 0} x^{um}$$

*Proof.* Note

$$\begin{aligned}
\Phi_{mp} &= \frac{\Phi_m\left(x^p\right)}{\Phi_m} && \text{from } p \nmid m \\
&= \Phi_m\left(x^p\right)\ \frac{\Psi_m}{x^m - 1} && \text{from Definition 2.5} \\
&= -\Phi_m\left(x^p\right)\ \Psi_m\ \frac{1}{1 - x^m} && \text{by rearranging} \\
&= -\ \Phi_m\left(x^p\right)\ \Psi_m\ \sum_{u\geq 0} x^{um} && \text{by carrying out a formal expansion of } \frac{1}{1-x^m} \\
&= -\ \Phi_m\left(x^p\right)\ G
\end{aligned}$$

□

**Notation 3.5.** *Let*

$$G = \Psi_m \sum_{u\geq 0} x^{um} = \sum_{t\geq 0} e_t x^t$$

*For* $0 \leq i \leq \varphi(m) - 1$ *and* $0 \leq j \leq q$, *let*

$$g_{m,p,i,j} = \sum_{k=0}^{l} e_{ip+mj+k} x^k$$

*where if* $j < q$ *then* $l = m - 1$ *else* $l = r - 1$.

**Lemma 3.4.** *For all* $0 \leq i \leq \varphi(m) - 1$, *we have*

1. $g_{m,p,i,0} = \cdots = g_{m,p,i,q-1} = \mathcal{R}_{\mathrm{rem}(ir,m)} \Psi_m$

*2.* $g_{m,p,i,q} = \mathcal{T}_r \; g_{m,p,i,0}$

*Proof.* Let $0 \le j \le q$. Let $\Psi_m = \sum_{s\ge 0} b_s x^s$. Since $\deg \Psi_m < m$, we see immediately that $e_t = b_{\mathrm{rem}(t,m)}$ for $0 \le t$. We consider two cases:

1. $j < q$

$$
\begin{aligned}
g_{m,p,i,j} &= \sum_{k=0}^{m-1} e_{ip+mj+k}\; x^k && \text{from Notation 3.5}\\
&= \sum_{k=0}^{m-1} b_{\mathrm{rem}(ir+k,m)}\; x^k && \text{since } e_{ip+jm+k} = b_{\mathrm{rem}(ip+jm+k,m)}\\
& && \qquad = b_{\mathrm{rem}(ir+k,m)}\\
&= \sum_{s=0}^{m-1} b_s\; x^{\mathrm{rem}(s+i(m-r),m)} && \text{by re-indexing } k \text{ with}\\
& && s = \mathrm{rem}(ir+k,m) \text{ which can be easy}\\
& && \text{shown to be a bijection}\\
& && \mathbb{N}_{\le m-1} \to \mathbb{N}_{\le m-1} \text{ with the inverse}\\
& && \text{map } k = \mathrm{rem}(s+i\,(m-r)\,,m)\\
&= \sum_{s=0}^{m-1} b_s\; \mathrm{rem}\left(x^{s+i(m-r)}, x^m - 1\right) && \text{by Proposition 3.1}\\
&= \mathrm{rem}\left(\sum_{s=0}^{m-1} b_s\; x^{s+i(m-r)}, x^m - 1\right) && \text{since } b_s \text{ does not depend on } x\\
&= \mathrm{rem}\left(x^{i(m-r)} \sum_{s=0}^{m-1} b_s x^s, x^m - 1\right) && \text{by factoring out } x^{i(m-r)}\\
&= \mathrm{rem}(x^{i(m-r)} \Psi_{m,} x^m - 1) && \text{by recalling } \Psi_m = \sum_{s\ge 0} b_s x^s\\
&= \mathrm{rem}(x^{\mathrm{rem}(i(m-r),m)} \Psi_{m,} x^m - 1) && \text{by Proposition 3.1}
\end{aligned}
$$

$$= \mathrm{rem}(x^{m-\mathrm{rem}(ir,m)}\Psi_{m,}x^m - 1) \qquad \text{by Proposition 3.1}$$

$$= \mathcal{R}_{\mathrm{rem}(ir,m)}\Psi_m \qquad \text{from Lemma 3.2}$$

2. $j = q$

$$\begin{aligned}
g_{m,p,i,q} &= \sum_{k=0}^{r-1} e_{ip+mq+k}\ x^k && \text{from Notation 3.5} \\
&= \sum_{k=0}^{r-1} b_{\mathrm{rem}(ir+k,m)}\ x^k && \text{since } e_{ip+jm+k} = b_{\mathrm{rem}(ip+jm+k,m)} = b_{\mathrm{rem}(ir+k,m)} \\
&= \mathcal{T}_r\ g_{m,p,i,0} && \text{from the second line in the previous case.}
\end{aligned}$$

□

**Lemma 3.5.** *For all $0 \le i \le \varphi(m) - 1$ and $0 \le j \le q$, we have*

$$f_{m,p,i,j} = -\sum_{s=0}^{i} a_s g_{m,p,(i-s),j}$$

*where $\Phi_m = \sum_{s\ge 0} a_s x^s$.*

*Proof.* Note

$$\begin{aligned}
\Phi_{mp} &= -\Phi_m\left(x^p\right)\ G && \text{from Lemma 3.3} \\
&= -(\sum_{s\ge 0} a_s x^{sp})\ G && \text{from } \Phi_m = \sum_{s\ge 0} a_s x^s \\
&= -\sum_{s\ge 0} a_s x^{sp} \quad \sum_{k\ge 0} e_k x^k && G = \sum_{k\ge 0} e_k x^k \\
&= -\sum_{s\ge 0} a_s x^{sp} \quad \sum_{i\ge 0}\sum_{j=0}^{q} g_{m,p,i,j}\ x^{jm}\ x^{ip} && \text{from Notation 3.5 and } q = \frac{p-r}{m}
\end{aligned}$$

$$
\begin{aligned}
&= -\sum_{s\geq 0}\sum_{i\geq 0}\sum_{j=0}^{q} a_s\ g_{m,p,i,j}\ x^{jm+(s+i)p} && \text{by collecting the exponents of } x\\
&= -\sum_{i\geq 0}\sum_{\substack{s,i\geq 0\\ s+\bar{s}=i}}\sum_{j=0}^{q} a_s g_{m,p,\bar{s},j}\ x^{jm+ip} && \text{by re-indexing}\\
&= -\sum_{i\geq 0}\sum_{s=0}^{i}\sum_{j=0}^{q} a_s g_{m,p,(i-s),j} x^{jm+ip} && \text{by re-indexing and } \bar{s}=i-s\\
&= -\sum_{i\geq 0}\sum_{j=0}^{q}\sum_{s=0}^{i} a_s g_{m,p,(i-s),j} x^{jm+ip} && \text{by changing the summation order}\\
&= \sum_{i\geq 0}\left(\sum_{j=0}^{q}\left(-\sum_{s=0}^{i} a_s g_{m,p,(i-s),j}\right) x^{jm}\right) x^{ip} && \text{by grouping}
\end{aligned}
$$

Recall that $\deg g_{m,p,i,j} < m$. Thus

$$\deg \sum_{s=0}^{i} a_s g_{m,p,(i-s),j} < m$$

Furthermore deg $g_{m,p,i,q} < r$. Recall that $p = qm + r$. Thus

$$\deg \sum_{j=0}^{q}\left(-\sum_{s=0}^{i} a_s g_{m,p,(i-s),j}\right) x^{jm} < p$$

Thus finally from Notation 3.3, we have

$$f_{m,p,i,j} = -\sum_{s=0}^{i} a_s g_{m,p,(i-s),j}$$

$\square$

**Lemma 3.6.** *For* $0 \le i \le \varphi(m) - 1$ *and* $0 \le j \le q$,

$$f_{m,p,i,j} = \begin{cases} \mathcal{N}\mathcal{R}_{\mathrm{rem}(ir,m)}(\Psi_m \cdot \mathcal{E}_r \mathcal{T}_{i+1} \Phi_m) & 0 \le j \le q-1 \\ \mathcal{T}_r f_{m,p,i,0} & j = q \end{cases}$$

*Proof.* We consider two cases:

1. $j < q$

$$\begin{aligned} f_{m,p,i,j} &= -\sum_{s=0}^{i} a_s g_{m,p,(i-s),j} && \text{from Lemma 3.5} \\ &= -\sum_{s=0}^{i} a_s \mathcal{R}_{\mathrm{rem}((i-s)r,m)} \Psi_m && \text{from Lemma 3.4} \\ &= -\sum_{s=0}^{i} a_s \mathrm{rem}(x^{m-\mathrm{rem}((i-s)r,m)} \Psi_m, x^m - 1) && \text{from Lemma 3.2} \\ &= -\mathrm{rem}(x^{\mathrm{rem}(m-ir,m)} \Psi_m \sum_{s=0}^{i} a_s x^{sr}, x^m - 1) && \text{by Proposition 3.1} \\ &= -\mathrm{rem}(x^{m-\mathrm{rem}(ir,m)} \Psi_m \sum_{s=0}^{i} a_s x^{sr}, x^m - 1) && \text{by Proposition 3.1} \\ &= \mathcal{N}\mathcal{R}_{\mathrm{rem}(ir,m)}(\Psi_m \cdot \mathcal{E}_r \mathcal{T}_{i+1} \Phi_m) \end{aligned}$$

2. $j = q$

$$\begin{aligned} f_{m,p,i,q} &= -\sum_{s=0}^{i} a_s g_{m,p,(i-s),q} \\ &= -\sum_{s=0}^{i} a_s \mathcal{T}_r g_{m,p,(i-s),0} \\ &= -\mathcal{T}_r \sum_{s=0}^{i} a_s g_{m,p,(i-s),0} && \text{from Lemma 3.4} \end{aligned}$$

$$= \mathcal{T}_r f_{m,p,i,0} \qquad \text{from Lemma 3.5}$$

$\square$

**Lemma 3.7.** *We have* $\mathrm{rem}(\Psi_m \Phi_m(x^r), x^m - 1) = 0$

*Proof.* Note

$$\begin{aligned}
\mathrm{rem}(\Psi_m \Phi_m(x^r), x^m - 1) &= \mathrm{rem}(\Psi_m \Phi_m(x^p), x^m - 1) && \Phi_m(x^p) \equiv_{x^m-1} \Phi_m(x^r) \\
&= \mathrm{rem}(\Psi_m \Phi_m \Phi_{mp}, x^m - 1) && \Phi_m(x^p) = \Phi_m \Phi_{mp} \\
&= \mathrm{rem}((\Phi_{mp})(x^m - 1), x^m - 1) && \Psi_m \Phi_m = x^m - 1 \\
&= 0 && \mathrm{rem}(x^m - 1, x^m - 1) = 0
\end{aligned}$$

$\square$

Finally we are ready to prove Theorem 3.1.

*Proof of Theorem 3.1 (Structure 1).* From Lemma 3.6 on page 38 we see that $f_{m,p,i,j}$ does not depend on $j$. Hence

$$C_{m,p,i,0} = \cdots = C_{m,p,i,q-1}$$

$\square$

*Proof of Theorem 3.1 (Structure 2).* From Lemma 3.6 it is immediate that

$$C_{m,p,i,q} = \mathcal{T}_r C_{m,p,i,0}$$

From now on, let $r = 1$. Note

$$
\begin{aligned}
f_{m,p,i,q} &= \mathcal{T}_1 \mathcal{N} \mathcal{R}_{\mathrm{rem}(i \cdot 1, m)} (\Psi_m \cdot \mathcal{E}_1 \mathcal{T}_{i+1} \Phi_m) && \text{Lemma 3.6} \\
&= \mathrm{rem}\left( -\mathrm{rem}\left( x^{m-i} \sum_t b_t x^t \sum_{s \le i} a_s x^s,\ x^m - 1 \right), x^1 \right) \\
&= \mathrm{rem}\left( - \sum_{\substack{0 \le t \le m - \varphi(m) \\ 0 \le s \le i}} b_t a_s x^{\mathrm{rem}(m-i+t+s, m)}, x^1 \right) \\
&= - \sum_{\substack{0 \le t \le m - \varphi(m) \\ 0 \le s \le i \\ \mathrm{rem}(m-i+t+s, m) = 0}} b_t a_s \\
&= - \sum_{\substack{0 \le t \le m - \varphi(m) \\ 0 \le s \le i \\ m-i+t+s = m}} b_t a_s \\
&\qquad \text{since } 0 < m - i + t + s < 2m \\
&= - \sum_{t+s=i} b_t a_s \\
&= -\mathrm{coeff}_i \left( \Psi_m \Phi_m \right) \\
&= -\mathrm{coeff}_i \left( x^m - 1 \right) \\
&= \begin{cases} 1 & i = 0 \\ 0 & i \ne 0 \end{cases}
\end{aligned}
$$

Thus

$$
C_{m,p,i,q} = \begin{cases} (1, 0, \ldots, 0) & i = 0 \\ (0, 0, \ldots, 0) & i \ne 0 \end{cases}
$$

$\square$

*Proof of Theorem 3.1 (Structure 3).* Note

$$f_{m,\tilde{p},i,0} = \mathcal{N}\mathcal{R}_{\mathrm{rem}(ir,m)}(\Psi_m \cdot \mathcal{E}_r \mathcal{T}_{i+1} \Phi_m)$$

Thus

$$f_{m,\tilde{p},i,0} = f_{m,p,i,0}$$

Hence

$$C_{m,\tilde{p},i,0} = C_{m,p,i,0}$$

□

*Proof of Theorem 3.1 (Structure 4).* Note

$$\begin{aligned}
f_{m,\tilde{p},\tilde{\imath},0} &= \mathcal{N}\mathcal{R}_{\mathrm{rem}(\tilde{\imath}\tilde{r},m)}(\Psi_m \cdot \mathcal{E}_{\tilde{r}} \mathcal{T}_{\tilde{\imath}+1} \Phi_m) && \text{from Lemma 3.6} \\
&= -\mathrm{rem}(\Psi_m \; x^{m-rem(\tilde{\imath}\tilde{r},m)} \sum_{s=0}^{\tilde{\imath}} a_s \; x^{s\tilde{r}}, x^m - 1) && \text{from Lemma 3.2} \\
&= -\mathrm{rem}(x^{\mathrm{rem}(\tilde{\imath}(m-\tilde{r}),m)} \; \Psi_m \; \sum_{s=0}^{\tilde{\imath}} a_s \; x^{s\tilde{r}}, x^m - 1) && \text{by Proposition 3.1} \\
&= -\mathrm{rem}(x^{\tilde{\imath}(m-\tilde{r})} \; \Psi_m \; \sum_{s=0}^{\tilde{\imath}} a_s \; x^{s\tilde{r}}, x^m) && \text{by Proposition 3.1} \\
&= \mathrm{rem}(-x^{\tilde{\imath}(m-\tilde{r})} \; \Psi_m \; \sum_{s=0}^{\tilde{\imath}} a_{\varphi(m)-s} \; x^{s\tilde{r}}, x^m - 1) && \text{since } a_{\varphi(m)-s} = a_s \\
&= \mathrm{rem}(-x^{(\varphi(m)-1-i)r} \; \Psi_m \; \sum_{s=0}^{\tilde{\imath}} a_{\varphi(m)-s} \; x^{s(m-r)}, x^m - 1) && \tilde{\imath} = \varphi(m) - 1 - i \\
& && \text{and } \tilde{r} = m - r \\
&= \mathrm{rem}(-x^{(m-1-i)r} \; \Psi_m \; \sum_{s=0}^{\tilde{\imath}} a_{\varphi(m)-s} \; x^{r(\varphi(m)-s)}, x^m - 1) && \text{by rearranging}
\end{aligned}$$

$$= \mathrm{rem}(-x^{\mathrm{rem}(m-(1+i)r,m)}\ \Psi_m \sum_{t=i+1}^{\varphi(m)} a_t x^{tr}, x^m - 1) \qquad \text{by re-indexing with } t = \varphi(m) - s$$

$$= \mathrm{rem}(-x^{\mathrm{rem}(m-(1+i)r,m)}\ \Psi_m\ (\Phi_m(x^r) - \sum_{t=0}^{i} a_t x^{tr}), x^m - 1) \qquad \text{since } \Phi_m(x^r) = \sum_{t=0}^{\varphi(m)} a_t x^{tr}$$

$$= \mathrm{rem}(x^{\mathrm{rem}(m-(1+i)r,m)} \Psi_m \sum_{t=0}^{i} a_t x^{tr}, x^m - 1) \qquad \text{by Lemma 3.7}$$

$$= \mathrm{rem}(x^{\mathrm{rem}(m-r,m)} \cdot x^{\mathrm{rem}(m-ir,m)} \Psi_m \sum_{t=0}^{i} a_t x^{tr}, x^m - 1)$$

$$= \mathrm{rem}(x^{\mathrm{rem}(m-r,m)} \left(\mathcal{N}\ f_{m,p,i,0}\right), x^m - 1) \qquad \text{by Lemma 3.6}$$

$$= \mathrm{rem}(x^{m-r} \left(\mathcal{N}\ f_{m,p,i,0}\right), x^m - 1)$$

$$= \mathcal{R}_r \mathcal{N} f_{m,p,i,0}$$

Hence

$$C_{m,\tilde{p},\tilde{\imath},0} = \mathcal{R}_r \mathcal{N} C_{m,p,i,0}$$

□

*Proof of Theorem 3.1 (Structure 5).* From Lemma 3.6 on page 38,

$$f_{m,p,\tilde{\imath},0} = \mathcal{N}\mathcal{R}_{\mathrm{rem}(\tilde{\imath}r,m)}(\Psi_m \cdot \mathcal{E}_r \mathcal{T}_{\tilde{\imath}+1} \Phi_m)$$

$$= -\mathrm{rem}(x^{m-\mathrm{rem}(\tilde{\imath}r,m)} \Psi_m \sum_{s=0}^{\tilde{\imath}} a_s x^{sr}, x^m - 1) \qquad \text{by Lemma 3.2}$$

$$= -\mathrm{rem}(x^{m-\mathrm{rem}(\tilde{\imath}r,m)} \Psi_m \Phi_m(x^r)$$

$$
\begin{aligned}
& - x^{m-\mathrm{rem}(\tilde{\imath}r,m)}\Psi_m \sum_{s=\tilde{\imath}+1}^{\varphi(m)} a_s x^{sr}), x^m - 1) && \Phi_m(x^r) = \sum_{s=0}^{\varphi(m)} a_s x^{sr} \\
= \ & \mathrm{rem}(x^{m-\mathrm{rem}(\tilde{\imath}r,m)}\Psi_m \sum_{s=\tilde{\imath}+1}^{\varphi(m)} a_s x^{sr}, x^m - 1) && \text{by Lemma 3.7} \\
= \ & \mathrm{rem}(x^{\mathrm{rem}(\tilde{\imath}(m-r),m)}\Psi_m \sum_{s=\tilde{\imath}+1}^{\varphi(m)} a_s x^{sr}, x^m - 1) && \text{by Proposition 3.1} \\
= \ & \mathrm{rem}(x^{\tilde{\imath}(m-r)}\Psi_m \sum_{s=\tilde{\imath}+1}^{\varphi(m)} a_s x^{sr}, x^m - 1) && \text{by Proposition 3.1} \\
= \ & \mathrm{rem}(\Psi_m \sum_{s=\tilde{\imath}+1}^{\varphi(m)} a_s x^{(s-\tilde{\imath})r}, x^m - 1) && \text{by distributing and} \\
& && x^m \equiv_{x^m-1} 1 \\
= \ & \mathrm{rem}(\Psi_m \sum_{w=0}^{i} a_{\varphi(m)-(i-w)} x^{(w+1)r}, x^m - 1) && w = s - \tilde{\imath} - 1 \\
= \ & \mathrm{rem}(\Psi_m \sum_{w=0}^{i} a_{i-w} x^{(w+1)r}, x^m - 1) && \text{since } a_{\varphi(m)-s} = a_s \\
= \ & \mathrm{rem}(x^r\Psi_m \sum_{w=0}^{i} a_{i-w} x^{wr}, x^m - 1) && \text{by factoring } x^r \\
= \ & \mathrm{rem}(x^r\Psi_m \sum_{t=0}^{i} a_t x^{(i-t)r}, x^m - 1) && t = i - w \\
= \ & \mathrm{rem}(-x^r x^{\psi(m)}\Psi_m(x^{-1}) \sum_{t=0}^{i} a_t x^{(i-t)r}, x^m - 1) && \Psi_m = -x^{\psi(m)}\Psi_m(x^{-1}) \\
= \ & \mathrm{rem}(-x^r x^{\psi(m)} x^{ir-m}\Psi_m(x^{-1}) \sum_{t=0}^{i} a_t x^{-tr}, x^m - 1) && \\
= \ & \mathrm{rem}(x^{r+m-\varphi(m)} f_{m,p,i,0}(x^{-1}), x^m - 1) && \psi(m) = m - \varphi(m) \\
= \ & \mathrm{rem}(x^{r+m-\varphi(m)+1} \mathcal{F} f_{m,p,i,0}, x^m - 1) && \mathcal{F} f_{m,p,i,0} = x^{m-1} f_{m,p,i,0}(x^{-1}) \\
= \ & \mathrm{rem}(x^{m-\tilde{r}} \mathcal{F} f_{m,p,i,0}, x^m - 1) && \text{by Proposition 3.1} \\
= \ & \mathcal{R}_{\tilde{r}} \mathcal{F} f_{m,p,i,0} && \text{by Lemma 3.2}
\end{aligned}
$$

Hence $C_{m,p,\tilde{i},0} = \mathcal{R}_{\tilde{r}}\mathcal{F}C_{m,p,i,0}$ $\square$

# Chapter 4

# Property: Norm

## Introduction

In this chapter we study the norm of $\Phi_{mp}$. Recall

**Notation 4.1** (Norm of a polynomial)**.** *Let $f = a_0 + \cdots + a_n x^n$. Then the k-norm of $f$ is defined by*

$$\|f\|_k = \begin{cases} \left(\sum_{j=0}^{n} |a_j|^k\right)^{\frac{1}{k}} & \text{if } k < \infty \\ \max\{|a_j|\,, j = 0, \cdots, n\} & \text{if } k = \infty \end{cases}$$

There have been intensive research on the norms of cyclotomic polynomials.

1. Numerous works on the infinity norm [7, 9, 11, 16, 17, 22, 29, 30, 31, 33, 40, 42, 43]

2. Carlitz's [21] showed that $\|\Phi_{mp}\|_2^2$ is linear over $p$'s that are equivalent modulo $m$.

We show the following newly found properties of norms (Theorem 4.1).

1. $\|\Phi_{mp}\|_k^k$ is linear over $p$'s that are equivalent modulo $m$.

2. $\|\Phi_{mp}\|_k^k$ and $\|\Phi_{m\tilde{p}}\|_k^k$ are parallel if $p + \tilde{p} \equiv_m 0$.

## 4.1 Main Results

In this section state the main result of this chapter. We start by the following notation.

**Notation 4.2.** *Let $p \in P_{m,r}$ and $k$ is finite. Then let*

$$\begin{aligned} \|a_{m,r}\|_k &= \sum_{i=0}^{\varphi(m)-1} \|f_{m,p,i,0}\|_k^k \\ \|b_{m,r}\|_k &= \sum_{i=0}^{\varphi(m)-1} \|f_{m,p,i,q}\|_k^k \\ \|A_{m,r}\|_k &= \frac{\|a_{m,r}\|_k}{m} \\ \|B_{m,r}\|_k &= \|b_{m,r}\|_k - r\,\|A_{m,r}\|_k \end{aligned}$$

We can now state the main Theorem of this chapter.

**Theorem 4.1** (Norm). *Let $p \in P_{m,r}$ and $k$ is finite. Then*

1. *[Linear]* $\|\Phi_{mp}\|_k^k = \|A_{m,r}\|_k\ p + \|B_{m,r}\|_k$

2. *[Parallel]* $\|A_{m,m-r}\|_k = \|A_{m,r}\|_k \qquad \|B_{m,m-r}\|_k = -\|B_{m,r}\|_k$

**Example 4.1.** *Let $m = 15$.*

1. *Let $p_1 = 17$ and $p_2 = 47$. Then $r = 2$*

| $k$ | 1 | 2 | $\infty$ |
|---|---|---|---|
| $\|\Phi_{15p_1})\|_k^k$ | 75 | 79 | 2 |
| $\|\Phi_{15p_2})\|_k^k$ | 211 | 223 | 2 |
| $\|\Phi_{15p})\|_k^k$ | $\frac{68}{15}p - \frac{31}{15}$ | $\frac{72}{15}p - \frac{39}{15}$ | 2 |
| $\|\Phi_{15p}\|_k$ | $\frac{68}{15}p - \frac{31}{15}$ | $\sqrt{\frac{72}{15}p - \frac{39}{15}}$ | 1 |

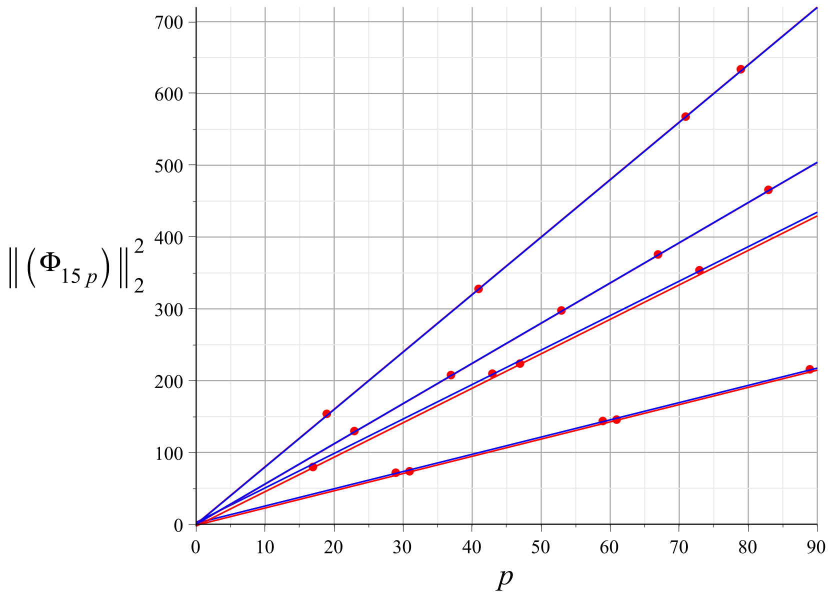
*2. Let $p_1 = 43$ and $p_2 = 73$. Then $r = 13$*

| $k$ | 1 | 2 | $\infty$ |
|---|---|---|---|
| $\lVert\Phi_{15p_1})\rVert_k^k$ | 197 | 209 | 2 |
| $\lVert\Phi_{15p_2})\rVert_k^k$ | 333 | 353 | 2 |
| $\lVert\Phi_{15p})\rVert_k^k$ | $\frac{68}{15}p + \frac{31}{15}$ | $\frac{72}{15}p + \frac{39}{15}$ | 2 |
| $\lVert\Phi_{15p})\rVert_k$ | $\frac{68}{15}p + \frac{31}{15}$ | $\sqrt{\frac{72}{15}p + \frac{39}{15}}$ | 1 |

**Example 4.2.** *Let $m = 15$. Then we have*

$$\lVert\Phi_{15p}\rVert_2^2 = \begin{cases} \frac{36}{15}p - \frac{21}{15} & \textit{if} \quad p \equiv_{15} 1 \\ \frac{72}{15}p - \frac{39}{15} & \textit{if} \quad p \equiv_{15} 2 \\ \frac{120}{15}p + \frac{4}{15} & \textit{if} \quad p \equiv_{15} 4 \\ \frac{84}{15}p - \frac{3}{15} & \textit{if} \quad p \equiv_{15} 7 \\ \frac{84}{15}p + \frac{3}{15} & \textit{if} \quad p \equiv_{15} 8 \\ \frac{120}{15}p - \frac{4}{15} & \textit{if} \quad p \equiv_{15} 11 \\ \frac{72}{15}p + \frac{39}{15} & \textit{if} \quad p \equiv_{15} 13 \\ \frac{36}{15}p + \frac{21}{15} & \textit{if} \quad p \equiv_{15} 14 \end{cases}$$

*The following figure shows the relationship between $p$ and $\lVert\Phi_{15p}\rVert_2^2$.*




## 4.2 Proofs

*Proof of Theorem 4.1.*

1. (Linear)

$$
\begin{aligned}
\|\Phi_{mp}\|_k^k &= \sum_{i=0}^{\varphi(m)-1} \sum_{j=0}^{q} \|f_{m,p,i,j}\|_k^k && \text{from Notation 3.1} \\
&= \sum_{i=0}^{\varphi(m)-1} q \ \|f_{m,p,i,0}\|_k^k + \sum_{i=0}^{\varphi(m)-1} \|f_{m,p,i,q}\|_k^k && \text{Theorem 3.1 (Structures 1, 2)} \\
&= q \ \|a_{m,r}\|_k + \ \|b_{m,r}\|_k && \text{from Notation 4.2} \\
&= \|a_{m,r}\|_k \frac{(p-r)}{m} + \ \|b_{m,r}\|_k && q = \frac{p-r}{m} \\
&= \ \|A_{m,r}\|_k \, p + \|B_{m,r}\|_k && \text{from Notation 4.2}
\end{aligned}
$$

2. (Parallel) For $\tilde{p} \in P_{m,m-r}$, without loss of generality we may assume $\tilde{p} > m$. Then

we have $\gcd(m, m-r) = \gcd(m, r) = 1$ because $\tilde{p}$ is prime and $\tilde{p} \nmid m$. Therefore, we have

$$
\begin{aligned}
\|\Phi_{m\tilde{p}}\|_k^k &= \sum_{i=0}^{\varphi(m)-1} \sum_{j=0}^{\tilde{q}} \|f_{m,\tilde{p},\tilde{\imath},j}\|_k^k && \text{from Notation 3.1} \\
&= \sum_{i=0}^{\varphi(m)-1} \tilde{q}\ \|f_{m,\tilde{p},\tilde{\imath},0}\|_k^k + \sum_{i=0}^{\varphi(m)-1} \|f_{m,\tilde{p},\tilde{\imath},\tilde{q}}\|_k^k && \text{from Theorem 3.1} \\
& && \text{(Structures 1, 2)} \\
&= \tilde{q} \sum_{i=0}^{\varphi(m)-1} \|f_{m,\tilde{p},\tilde{\imath},0}\|_k^k + \sum_{i=0}^{\varphi(m)-1} \|f_{m,p,i,0}\|_k^k - \|f_{m,p,i,q}\|_k^k && \text{from Lemma 6.1} \\
&= \tilde{q}\ \|a_{m,r}\|_k + \|a_{m,r}\|_k - \ \|b_{m,r}\|_k && \text{from Notation 4.2} \\
&= \|a_{m,r}\|_k \left( \frac{\tilde{p} - m + \tilde{r}}{m} \right) - \|b_{m,r}\|_k && \tilde{q} = \frac{\tilde{p} - (m-r)}{m} \\
&= \|A_{m,r}\|_k\ \tilde{p} - \|B_{m,r}\|_k && \text{from Notation 4.2}
\end{aligned}
$$

□

## 4.3 Application

In this section we provide a fast algorithm for computing $\|\Phi_{mp}\|_k$.

**Algorithm 4.1** (Norm).

**Input** *$m$, $p$ and $k$ such that $p \gg m$ and $k \geq 1$*

**Output** $\|\Phi_{mp}\|_k$

1. *Find small primes $p_1, p_2 > m$ such that $p \equiv_m p_1 \equiv_m p_2$*
2. $N_1 \leftarrow \|\Phi_{mp_1}\|_k^k$

   $N_2 \leftarrow \|\Phi_{mp}\|_k^k$ *through direct computation*
3. $\|A_{m,r}\|_k \leftarrow \frac{N_2 - N_1}{p_2 - p_1}$

   $\|B_{m,r}\|_k \leftarrow N_1 - \|A_{m,r}\|_k p_1$
4. *return* $\left(\|A_{m,r}\|_k p + \|B_{m,r}\|_k\right)^{\frac{1}{k}}$

**Remark 4.1.** *The algorithm depends on the linear property of $\|\Phi_{mp}\|_k^k$*

We implement the last algorithm in the following two examples to show how fast and useful it is. In the next example we fix the values of $r$ and change the values of $k$.

**Example 4.3.** *Let $m = 105, r = 1$. In Step 1, we used $p_1 = 211, p_2 = 421$. We compare the time needed to find $\|\Phi_{mp}\|_1$ and $\|\Phi_{mp}\|_2$ by Algorithm 4.1 and direct computation. All calculations were made using Maple 18 and the time is in seconds.*

Table 4.1: Norms of $\Phi_{mp}$, where $m = 105$ and $r = 1$

| $p$ | $\|\Phi_{mp}\|_1$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|
| 10501 | 114401 | 0.984 | 0.031 |
| 10711 | 116689 | 0.990 | 0.039 |
| 12391 | 134993 | 1.178 | 0.040 |

*Table 4.1(continued)*

| | | | |
|---|---|---|---|
| 15121 | 16473 | 1.373 | 0.037 |
| 16381 | 178465 | 1.484 | 0.036 |
| 17011 | 185329 | 1.563 | 0.034 |
| 20161 | 219649 | 2.038 | 0.039 |
| 200341 | 2182753 | 17.781 | 0.043 |
| 200971 | 2189617 | 17.346 | 0.037 |
| 300301 | 3271841 | 34.446 | 0.043 |

Table 4.2: Norms of $\Phi_{mp}$, where $m = 105$ and $r = 1$

| $p$ | $\|\Phi_{mp}\|_2$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|
| 10501 | 340.5892 | 0.992 | 0.036 |
| 10711 | 343.978 | 1.012 | 0.047 |
| 12391 | 369.974 | 1.217 | 0.043 |
| 15121 | 402.706 | 1.452 | 0.040 |
| 16381 | 402.706 | 1.452 | 0.040 |
| 17011 | 433.499 | 1.644 | 0.042 |
| 20161 | 471.933 | 1.946 | 0.038 |
| 200341 | 1487.710 | 17.735 | 0.039 |
| 200971 | 1490.047 | 18.314 | 0.039 |
| 300301 | 1821.428 | 42.18 | 0.047 |

**Example 4.4.** *In this example we fix $k$ and change the values of $r$. Let $m = 165$. We compare the time needed to find $\|\Phi_{mp}\|_2$ by Algorithm 4.1 and direct computation. All calculations were made using Maple* 18 *and the time is in seconds.*

Table 4.3: $\|\Phi_{mp}\|_2$ where $m = 165$

| $p$ | $r$ | $p_1$ | $p_2$ | $\|\Phi_{mp}\|_2$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|---|---|---|
| 80527 | 7 | 337 | 997 | 2871.585451 | 16.161 | 0.238 |
| 81517 | 7 | 337 | 997 | 2889.183103 | 17.168 | 1.983 |
| 81847 | 7 | 337 | 997 | 2895.025216 | 17.346 | 0.212 |
| 82507 | 7 | 337 | 997 | 2906.674216 | 17.915 | 0.200 |
| 82837 | 7 | 337 | 997 | 2912.481245 | 17.719 | 0.300 |
| 81203 | 23 | 353 | 683 | 3582.830307 | 18.447 | 0.204 |
| 81533 | 23 | 353 | 863 | 3590.103202 | 17.592 | 0.193 |
| 82193 | 23 | 353 | 683 | 3604.604971 | 16.999 | 0.183 |
| 83843 | 23 | 353 | 683 | 3640.606680 | 17.142 | 0.189 |
| 84503 | 23 | 353 | 683 | 3654.908070 | 17.176 | 0.192 |
| 80621 | 101 | 431 | 761 | 6629.918930 | 21.089 | 0.261 |
| 81281 | 101 | 431 | 761 | 6657.001202 | 18.969 | 0.210 |
| 81611 | 101 | 431 | 761 | 6670.501106 | 25.286 | 0.229 |
| 82601 | 101 | 431 | 761 | 64710.837876 | 21.929 | 0.234 |
| 83591 | 101 | 431 | 761 | 6750.933639 | 21.875 | 0.243 |
| 80177 | 152 | 317 | 647 | 4571.239329 | 19.188 | 0.201 |
| 82487 | 152 | 317 | 647 | 4636.624311 | 19.269 | 0.187 |
| 83477 | 152 | 317 | 647 | 4664.365873 | 19.778 | 0.185 |
| 84137 | 152 | 317 | 647 | 4682.768946 | 19.891 | 0.200 |
| 84467 | 152 | 317 | 647 | 4691.943414 | 20.140 | 0.185 |

# Chapter 5

# Property: Middle term

## Introduction

In this chapter we investigate the middle term of a cyclotomic polynomial.

**Notation 5.1.** *Let* $\Phi_n = \sum_{s=0}^{\varphi(n)} a_s x^s$*. Then* $M(\Phi_n) = a_{\frac{\varphi(n)}{2}}$*, that is, the coefficient of the middle term of* $\Phi_n$*.*

There have been some research on the middle term of cyclotomic polynomials.

1. Clearly, $M(\Phi_p) = 1$
2. In [24], Dredsen proved that $M(\Phi_{2^k}) = 0$, and $M(\Phi_n)$ is odd if $n \neq 2^k$.
3. In [10, 32], Beiter and (Lam and Leung) gave a formula for $M(\Phi_{pq})$.

We show the following newly found properties of midterms (Theorem 5.1).

1. $M(\Phi_{mp}) = \pm M(\Phi_{m\tilde{p}})$ if $p \mp \tilde{p} \equiv_m 0$.
2. $M(\Phi_{mp}) = \pm 1$ if $p \equiv_m \pm 1$.

## 5.1 Main results

**Theorem 5.1** (Middle term). *We have*

1. $M(\Phi_{mp}) = +M(\Phi_{m\tilde{p}})$ *if* $p - \tilde{p} \equiv_m 0$

2. $M(\Phi_{mp}) = -M(\Phi_{m\tilde{p}})$ *if* $p + \tilde{p} \equiv_m 0$

**Example 5.1.** *Let* $m = 15$. *Then*

| $p \equiv_m 1$ | $\tilde{p} \equiv_m 14$ | $M(\Phi_{pm})$ | $M(\Phi_{\tilde{p}m})$ | $p \equiv_m 2$ | $\tilde{p} \equiv_m 13$ | $M(\Phi_{pm})$ | $M(\Phi_{\tilde{p}m})$ |
|---|---|---|---|---|---|---|---|
| 31 | 29 | 1 | $-1$ | 17 | 43 | $-1$ | 1 |
| 61 | 59 | 1 | $-1$ | 47 | 73 | $-1$ | 1 |
| 151 | 89 | 1 | $-1$ | 107 | 103 | $-1$ | 1 |

**Theorem 5.2** (Middle term). *We have*

1. $M(\Phi_{mp}) = +1$ *if* $p \equiv_m +1$

2. $M(\Phi_{mp}) = -1$ *if* $p \equiv_m -1$

## 5.2 Proofs

**Lemma 5.1.** *We have*

$$\left(\frac{\varphi(m)}{2} - 1\right) p \leq \frac{\varphi(mp)}{2} \leq p \left(\frac{\varphi(m)}{2}\right) - 1$$

*Proof.* Note

$$\left(\frac{\varphi(m)}{2} - 1\right) p = \frac{\varphi(m)p}{2} - p$$

$$
\begin{aligned}
&= \frac{\varphi(m)p}{2} - p + \frac{\varphi(m)}{2} - \frac{\varphi(m)}{2} \\
&= \frac{\varphi(mp)}{2} + \left(\frac{\varphi(m)}{2} - p\right) \\
&\leq \frac{\varphi(mp)}{2}
\end{aligned}
$$

On the other hand

$$
\begin{aligned}
\left(\frac{\varphi(m)}{2}\right)p - 1 &= \frac{\varphi(m)}{2}p - 1 + \frac{\varphi(m)}{2} - \frac{\varphi(m)}{2} \\
&= \frac{\varphi(mp)}{2} + \frac{\varphi(m)}{2} - 1 \\
&\geq \frac{\varphi(mp)}{2}
\end{aligned}
$$

$\square$

*Proof of Theorem 5.1.* Let $I = \frac{\varphi(m)}{2} - 1$

1. In order to show that $M(\Phi_{mp}) = M(\Phi_{m\tilde{p}})$ we need to show that $c_{\frac{\varphi(m\tilde{p})}{2}} = c_{\frac{\varphi(mp)}{2}}$. Note

$$
\begin{aligned}
M(\Phi_{m\tilde{p}}) &= c_{\frac{\varphi(m\tilde{p})}{2}} && \text{by Notation 5.1} \\
&= c_{\frac{\varphi(m)(\tilde{p}-1)}{2}} && \text{by distribution} \\
&= c_{I\tilde{p}+\tilde{p}-\frac{\varphi(m)}{2}} && \text{from Lemma 5.1} \\
&= c_{I\tilde{p}+\tilde{q}m+r-\frac{\varphi(m)}{2}} && \tilde{p} = \tilde{q}m + r \\
&= \begin{cases} c_{I\tilde{p}+(\tilde{q}-1)m+(m+r-\frac{\varphi(m)}{2})} & r < \frac{\varphi(m)}{2} \\ c_{I\tilde{p}+\tilde{q}m+(r-\frac{\varphi(m)}{2})} & r \geq \frac{\varphi(m)}{2} \end{cases}
\end{aligned}
$$

$$= \begin{cases} c_{Ip+(q-1)m+(m+r-\frac{\varphi(m)}{2})} & r < \frac{\varphi(m)}{2} \\ c_{Ip+qm+(r-\frac{\varphi(m)}{2})} & r \geq \frac{\varphi(m)}{2} \end{cases} \quad \text{Theorem 3.1 (Structures 1, 3)}$$

$$= c_{Ip+p-\frac{\varphi(m)}{2}}$$

$$= c_{\frac{\varphi(mp)}{2}}$$

$$= M(\Phi_{mp})$$

2. Note

$$C_{m,\tilde{p},I,0} = \mathcal{R}_r \mathcal{N} C_{m,p,I+1,0} \qquad \text{by Theorem 3.1(Structure 4)}$$

Then we have

$$M(\Phi_{m\tilde{p}}) = \begin{cases} c_{I\tilde{p}+(\tilde{q}-1)m+(m+\tilde{r}-\frac{\varphi(m)}{2})} & \tilde{r} < \frac{\varphi(m)}{2} \\ c_{I\tilde{p}+\tilde{q}m+(\tilde{r}-\frac{\varphi(m)}{2})} & \tilde{r} \geq \frac{\varphi(m)}{2} \end{cases}$$

$$= \begin{cases} c_{I\tilde{p}+(\tilde{q}-1)m+(m+m-r-\frac{\varphi(m)}{2})} & \tilde{r} < \frac{\varphi(m)}{2} \\ c_{I\tilde{p}+\tilde{q}m+(m-r-\frac{\varphi(m)}{2})} & \tilde{r} \geq \frac{\varphi(m)}{2} \end{cases}$$

$$= \begin{cases} c_{I\tilde{p}+(m+m-r-\frac{\varphi(m)}{2})} & m-r < \frac{\varphi(m)}{2} \\ c_{I\tilde{p}+(m-r-\frac{\varphi(m)}{2})} & m-r \geq \frac{\varphi(m)}{2} \end{cases} \quad \begin{matrix} \text{by Theorem 3.1} \\ \text{(Structure 1)} \end{matrix}$$

$$= \begin{cases} -c_{(I+1)p+\mathrm{rem}((m+m-r-\frac{\varphi(m)}{2})+r,m)} & m-r < \frac{\varphi(m)}{2} \\ -c_{(I+1)p+(m-r-\frac{\varphi(m)}{2})+r} & m-r \geq \frac{\varphi(m)}{2} \end{cases} \quad \begin{matrix} \text{by Theorem 3.1} \\ \text{(Structure 4 )} \end{matrix}$$

$$= -c_{Ip+p+m-\frac{\varphi(m)}{2}}$$

$$= -c_{Ip+p-\frac{\varphi(m)}{2}} \qquad \text{by Theorem 3.1}$$

(Structure 1)

$$
\begin{aligned}
&= -c_{\frac{\varphi(mp)}{2}} \\
&= -M(\Phi_{mp})
\end{aligned}
$$

□

*Proof of Theorem 5.2.*

1. Let $I = \frac{\varphi(m)}{2} - 1$. Then from Lemma 5.1 and the proof of Theorem 5.1 we can easily see that

$$M(\Phi_{mp}) = c_{Ip+\mathrm{rem}(r-\frac{\varphi(m)}{2},m)}$$

Let $r = 1$. Then $\mathrm{rem}(r - \frac{\varphi(m)}{2}, m) = m + 1 - \frac{\varphi(m)}{2}$ , by Lemma 3.6

$$
\begin{aligned}
f_{m,p,I,0} &= \mathcal{N}\mathcal{R}_{\mathrm{rem}(I,m)}(\Psi_m \cdot \mathcal{E}_1\mathcal{T}_{I+1}\Phi_m) \\
&= \mathcal{N}\mathrm{rem}(x^{m+1-\frac{\varphi(m)}{2}}\Psi_m \sum_{s=0}^{I} a_s x^s, x^m - 1) \\
&= \mathcal{N}\mathrm{rem}\left(x^{m+1-\frac{\varphi(m)}{2}}\left(\sum_{t=0}^{m-\varphi(m)} a_0 b_t x^t + \cdots + \sum_{t=0}^{m-\varphi(m)} a_I b_t x^{t+I}\right), x^m - 1\right)
\end{aligned}
$$

Note that, for $0 \leq s \leq I$ and $0 \leq t \leq m - \varphi(m)$,

$$
\begin{aligned}
& m + 1 - \frac{\varphi(m)}{2} + s + t \equiv_m m + 1 - \frac{\varphi(m)}{2} \\
\Longleftrightarrow\ & s + t \equiv_m 0 \\
\Longleftrightarrow\ & s + t = 0
\end{aligned}
$$

from $0 \leq s+t \leq I+m-\varphi(m) = m-1-\frac{\varphi(m)}{2} < m$. Hence

$$M(\Phi_{mp}) = -a_0 b_0 = 1$$

2. Follows from the last part and Theorem 5.1.

$\square$

## 5.3 Application

In this subsection we provide an efficient algorithm to find $M(\Phi_{mp})$ for a very large prime number $p$.

**Algorithm 5.1** (Middle Term)**.**

**Input** *$m$, $p$ such that $p >> m$*

**Output** $M(\Phi_{mp})$

1. *Find a primes $p_0 > m$ such that $p \equiv_m p_0$*
2. *$mid \leftarrow M(\Phi_{mp_0})$ through direct computation*
3. *return mid*

**Example 5.2.** *Let $m = 105$. We compare the time needed to find the middle term by Algorithm 5.1 and direct computation. All calculations were made using Maple* 18 *and the time is in seconds.*

Table 5.1: Time needed computing $M(\Phi_{mp})$

| $p$ | $r$ | $p_0$ | $M(\Phi_{mp})$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|---|---|
| 15017 | 2 | 107 | $-1$ | 2.102 | 0.007 |
| 17117 | 2 | 107 | $-1$ | 2.187 | 0.016 |
| 18587 | 2 | 107 | $-1$ | 2.355 | 0.015 |
| 15439 | 4 | 109 | 1 | 1.782 | 0.007 |
| 16069 | 4 | 109 | 1 | 1.950 | 0.015 |
| 1.7959 | 4 | 109 | 1 | 2.237 | 0.015 |
| 15131 | 11 | 431 | 3 | 2.235 | 0.033 |
| 16811 | 11 | 431 | 3 | 2.440 | 0.040 |
| 19121 | 11 | 431 | 3 | 2.734 | 0.046 |
| 15973 | 13 | 223 | $-3$ | 2.597 | 0.023 |
| 18493 | 13 | 223 | $-3$ | 2.751 | 0.026 |
| 19753 | 13 | 223 | $-3$ | 2.986 | 0.033 |

*Table 5.1(continued)*

# Chapter 6

# Property: Number of terms

## Introduction

In this chapter, we investigate the number of terms with prescribed coefficient in $\Phi_n$.

**Notation 6.1.** *Let $f$ be a polynomial. Then $\mathrm{Nt}_c(f)$ denotes the number of terms with the coefficient $c$ in $f$.*

There have been some research on the number of term of cyclotomic polynomials.

1. Clearly, $\mathrm{Nt}_c(\Phi_p) = \begin{cases} p & c = 1 \\ 0 & c \neq 1 \end{cases}$

2. In [20], Carlitz founds an explicit formula for the number of terms of $\Phi_{p_1 p_2}(x)$.

We show the following newly found properties of number of terms (Theorem 6.1).

1. $\mathrm{Nt}_c(\Phi_{mp})$ is linear over $p$'s that are equivalent modulo $m$.

2. $\mathrm{Nt}_c(\Phi_{mp})$ and $\mathrm{Nt}_{-c}(\Phi_{m\tilde{p}})$ are parallel if $p + \tilde{p} \equiv_m 0$.

## 6.1 Main results

In this section we state the main result of this chapter.

**Definition 6.1.** *$P_{m,r} = \{p : p \text{ prime}, \ p > m \text{ and } p \equiv_m r\}$.*

**Theorem 6.1** (Number of terms with coefficient $c$)**.** *Let $p \in P_{m,r}$. Then there exist $A_{m,r,c}, B_{m,r,c} \in \mathbb{Q}$ such that*

1. *[Linear]* $\mathrm{Nt}_c(\Phi_{mp}) = A_{m,r,c}\, p + B_{m,r,c}$
2. *[Parallel]* $A_{m,m-r,-c} = A_{m,r,c} \qquad B_{m,m-r,-c} = -B_{m,r,c}$

**Example 6.1.** *Let $m = 15$.*

1. *Let $p_1 = 17$ and $p_2 = 47$. Then $r = 2$*

| $c$ | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $\mathrm{Nt}_c(\Phi_{15\cdot 17})$ | 0 | 37 | 56 | 34 | 2 |
| $\mathrm{Nt}_c(\Phi_{15\cdot 47})$ | 0 | 105 | 164 | 94 | 6 |
| $\mathrm{Nt}_c(\Phi_{15p})$ | 0 | $\frac{34}{15}p - \frac{23}{15}$ | $\frac{270}{15}p - \frac{465}{15}$ | $\frac{30}{15}p$ | $\frac{2}{15}p - \frac{4}{15}$ |

2. *Let $p_1 = 43$ and $p_2 = 73$. Then $r = 13$*

| $c$ | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $\mathrm{Nt}_c(\Phi_{15\cdot 43})$ | 6 | 86 | 146 | 99 | 0 |
| $\mathrm{Nt}_c(\Phi_{15\cdot 73})$ | 10 | 146 | 254 | 167 | 0 |
| $\mathrm{Nt}_c(\Phi_{15p})$ | $\frac{2}{15}p + \frac{4}{15}$ | $\frac{30}{15}p$ | $\frac{270}{15}p - \frac{735}{15}$ | $\frac{34}{15}p + \frac{23}{15}$ | 0 |

**Remark 6.1.** *We can easily see from the last example that $\mathrm{Nt}_c(\Phi_{mp})$ and $\mathrm{Nt}_c(\Phi_{m\tilde{p}})$, where $p + \tilde{p} \equiv_m 0$ are not parallel.*

**Example 6.2** (Hamming weight)**.** *In this example we focus on the number of non-zero terms in* $\Phi_{mp}$*. Clearly*

$$\mathrm{hw}(\Phi_{mp}) = \varphi(mp) + 1 - \mathrm{Nt}_0(\Phi_{mp})$$

*Hence for all* $p \in P_{m,r}$ *we have*

1. *[Linear]* $\quad \mathrm{hw}(\Phi_{mp}) = A_{m,r}\, p + B_{m,r}$
2. *[Parallel]* $A_{m,m-r} = A_{m,r} \qquad B_{m,m-r} = -B_{m,r}$

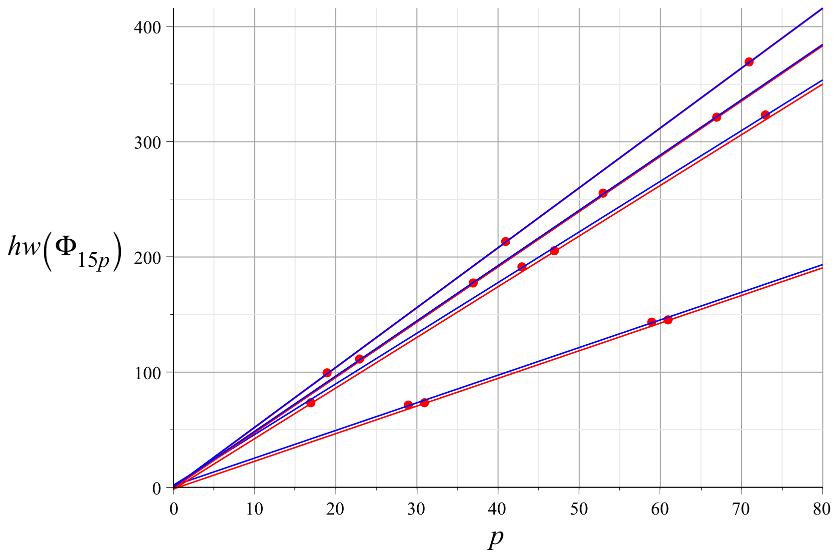
*where*

$$A_{m,r} = \varphi(m) + 1 - A_{m,r,0}$$

$$B_{m,r} = -1 - B_{m,r,0} - \varphi(m)$$

**Example 6.3.** *Let* $m = 15$*. Then we have*

$$\mathrm{hw}(\Phi_{15p}) = \begin{cases} \frac{36}{15}p - \frac{21}{15} & \textit{if} \quad p \equiv_{15} 1 \\ \frac{66}{15}p - \frac{27}{15} & \textit{if} \quad p \equiv_{15} 2 \\ \frac{78}{15}p + \frac{3}{15} & \textit{if} \quad p \equiv_{15} 4 \\ \frac{72}{15}p - \frac{9}{15} & \textit{if} \quad p \equiv_{15} 7 \\ \frac{72}{15}p + \frac{9}{15} & \textit{if} \quad p \equiv_{15} 8 \\ \frac{78}{15}p - \frac{3}{15} & \textit{if} \quad p \equiv_{15} 11 \\ \frac{66}{15}p + \frac{27}{15} & \textit{if} \quad p \equiv_{15} 13 \\ \frac{36}{15}p + \frac{21}{15} & \textit{if} \quad p \equiv_{15} 14 \end{cases}$$




## 6.2 Proofs

**Definition 6.2.** $\mathrm{Nt}_c(C_{m,p,i,j}) = \mathrm{Nt}_c(f_{m,p,i,j})$

**Notation 6.2.** *Let*

$$a_{m,r,c} = \sum_{i=0}^{\varphi(m)-1} \mathrm{Nt}_\mathrm{c}(C_{m,p,i,0})$$

$$b_{m,r,c} = \sum_{i=0}^{\varphi(m)-1} \mathrm{Nt}_\mathrm{c}\left(C_{m,p,i,q}\right)$$

$$A_{m,r,c} = \frac{a_{m,r,c}}{m}$$

$$B_{m,r,c} = b_{m,r,c} - rA_{m,r,c}$$

*The above notation is justified because of Theorem 3.1 (Structure 3).*

**Lemma 6.1.** *Let $p > m$. Then $C_{m,\tilde{p},\tilde{\imath},\tilde{q}} = \mathcal{R}_r(\mathcal{N}C_{m,p,i,0} + C_{m,p,i,q})$*

*Proof.* From Theorem 3.1 (Structure 4) we have

$$C_{m,\tilde{p},\tilde{\imath},0} = \mathcal{R}_r \mathcal{N} C_{m,p,i,0}$$

Hence $c_{\tilde{\imath}\tilde{p}}, \ldots, c_{\tilde{\imath}\tilde{p}+m-1-r}$ in $C_{m,\tilde{p},\tilde{\imath},0}$ are the same as $c_{ip+r}, \ldots, c_{ip+m-1}$ in $\mathcal{N}C_{m,p,i,0}$ which implies

$$C_{m,\tilde{p},\tilde{\imath},\tilde{q}} = \mathcal{R}_r(\mathcal{N}C_{m,p,i,0} + C_{m,p,i,q})$$

$\square$

*Proof of Theorem 6.1.*

1. (Linear)

$$\begin{aligned}
\mathrm{Nt}_{mp}(c) &= \sum_{i=0}^{\varphi(m)-1} \sum_{j=0}^{q} \mathrm{Nt_c}\left(C_{m,p,i,j}\right) && \text{from Notation 3.1} \\
&= \sum_{i=0}^{\varphi(m)-1} q \ \mathrm{Nt_c}\left(C_{m,p,i,0}\right) + \sum_{i=0}^{\varphi(m)-1} \mathrm{Nt_c}\left(C_{m,p,i,q}\right) && \text{Theorem 3.1} \\
& && \text{(Structures 1 and 2 )} \\
&= q \ a_{m,r,c} + b_{m,r,c} && \text{from Notation 6.2} \\
&= a_{m,r,c}\frac{(p-r)}{m} + \ b_{m,r,c} && q = \frac{p-r}{m} \\
&= A_{m,r,c} \ p + B_{m,r,c} && \text{from Notation 6.2}
\end{aligned}$$

2. (Parallel) For $\tilde{p} \in P_{m,m-r}$, without loss of generality we may assume $\tilde{p} > m$. Then we have $\gcd(m, m-r) = \gcd(m, r) = 1$ because $\tilde{p}$ is prime and $\tilde{p} \nmid m$. Therefore,

we have

$$
\begin{aligned}
\mathrm{Nt}_{-c}(\Phi_{m\tilde{p}}) &= \sum_{i=0}^{\varphi(m)-1} \sum_{j=0}^{\tilde{q}} \mathrm{Nt}_{-\mathrm{c}}(C_{m,\tilde{p},\tilde{\imath},j}) && \text{from Notation 3.1} \\
&= \sum_{i=0}^{\varphi(m)-1} \tilde{q}\ \mathrm{Nt}_{-c}\left(C_{m,\tilde{p},\tilde{\imath},0}\right) + \sum_{i=0}^{\varphi(m)-1} \mathrm{Nt}_{-c}\left(C_{m,\tilde{p},\tilde{\imath},\tilde{q}}\right) && \text{from Theorem 3.1} \\
& && \text{(Structures 1, 2)} \\
&= \tilde{q} \sum_{i=0}^{\varphi(m)-1} \mathrm{Nt}_{c}\left(C_{m,p,i,0}\right) \\
&\quad + \sum_{i=0}^{\varphi(m)-1} \mathrm{Nt}_{c}\left(C_{m,p,i,0}\right) - \mathrm{Nt}_{c}\left(C_{m,p,i,q}\right) && \text{from Lemma 6.1} \\
&= \tilde{q}\ a_{m,r,c} + \ a_{m,r,c} - b_{m,r,c} && \text{from Notation 6.2} \\
&= a_{m,r,c}\left(\frac{\tilde{p}+\tilde{r}}{m}\right) - b_{m,r,c} && \tilde{q} = \frac{\tilde{p}-(m-r)}{m} \\
&= A_{m,r,c}\ \tilde{p} - B_{m,r,c} && \text{from Notation 6.2}
\end{aligned}
$$

□

## 6.3 Application

In this section we will apply the linearity property in Theorem 6.1 to compute $\mathrm{Nt}_c(\Phi_{mp})$ when $p \gg m$.

**Algorithm 6.1** ($\mathrm{Nt}_c(\Phi_{mp})$).

**Input** *$m$, $p$ and $c$ such that $p \gg m$ and $c \in \mathbb{Z}$*

**Output** $\mathrm{Nt}_c(\Phi_{mp})$

1. *Find small primes $p_1, p_2 > m$ such that $p \equiv_m p_1 \equiv_m p_2$*

2. $N_1 \leftarrow \mathrm{Nt}_c(\Phi_{mp_1})$

   $N_2 \leftarrow \mathrm{Nt}_c(\Phi_{mp_2})$ *through direct computation*

3. $A_{m,r,c} \leftarrow \frac{N_2 - N_1}{p_2 - p_1}$

   $B_{m,r,c} \leftarrow N_1 - A_{m,r,c}\, p_1$

4. *return* $A_{m,r,c}\, p + B_{m,r,c}$

We implement the last algorithm in the following two examples to show how fast and useful it is. In the next example we fix the values of $r$ and change the values of $c$.

**Example 6.4.** *Let $m = 105, r = 1$. In Step 1, we used $p_1 = 211, p_2 = 421$. We compare the time needed to find $\mathrm{Nt}_1(\Phi_{mp})$ and $\mathrm{Nt}_2(\Phi_{mp})$ by Algorithm 6.1 and direct computation. All calculations were made using Maple 18 and the time is in seconds.*

Table 6.1: $\mathrm{Nt}_1(\Phi_{105p})$

| $p$ | $\mathrm{Nt}_1(\Phi_{105p})$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|
| 10501 | 56401 | 1.300 | 0.055 |
| 10711 | 57529 | 1.314 | 0.056 |
| 12391 | 66553 | 1.632 | 0.051 |
| 15121 | 81217 | 1.836 | 0.055 |

*Table 6.1(continued)*

| | | | |
|---|---|---|---|
| 16381 | 87985 | 2.084 | 0.053 |
| 17011 | 91369 | 2.251 | 0.060 |
| 20161 | 108289 | 2.589 | 0.055 |
| 21001 | 112801 | 2.724 | 0.062 |

Table 6.2: $\mathrm{Nt}_2(\Phi_{105p})$

| $p$ | $\mathrm{Nt}_2(\Phi_{105p})$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|
| 10501 | 400 | 1.352 | 0.053 |
| 10711 | 408 | 1.342 | 0.051 |
| 12391 | 472 | 1.541 | 0.056 |
| 15121 | 576 | 1.890 | 0.053 |
| 16381 | 624 | 2.068 | 0.056 |
| 17011 | 684 | 2.104 | 0.055 |
| 20161 | 768 | 2.522 | 0.050 |
| 21001 | 800 | 2.675 | 0.065 |

In the next example we fix $c$ and change the values of $r$.

**Example 6.5.** *Let $m = 165$. We compare the time needed to find $\mathrm{Nt}_3(\Phi_{mp})$ by Algorithm 6.1 and direct computation. All calculations were made using Maple 18 and the time is in seconds.*

Table 6.3: $\mathrm{Nt}_3(\Phi_{165p})$

| $p$ | $r$ | $p_1$ | $p_2$ | $\mathrm{Nt}_3(\Phi_{165p})$ | *Direct (sec)* | *Improved (sec)* |
|---|---|---|---|---|---|---|
| 80527 | 7 | 377 | 997 | 111275 | 39.572 | 0.338 |
| 81517 | 7 | 377 | 997 | 112643 | 22.119 | 0.232 |
| 81847 | 7 | 377 | 997 | 113099 | 19.796 | 0.262 |
| 82507 | 7 | 377 | 997 | 114011 | 21.954 | 0.250 |
| 82837 | 7 | 377 | 997 | 114467 | 18.392 | 0.223 |
| 81203 | 23 | 353 | 683 | 197834 | 24.263 | 0.186 |
| 81533 | 23 | 353 | 683 | 198638 | 21.125 | 0.207 |
| 82193 | 23 | 353 | 683 | 204266 | 21.966 | 0.182 |
| 83843 | 23 | 353 | 683 | 200246 | 24.722 | 0.203 |
| 84503 | 23 | 353 | 683 | 205874 | 21.338 | 0.216 |
| 80621 | 101 | 431 | 761 | 415320 | 25.539 | 0.239 |
| 81281 | 101 | 431 | 761 | 418720 | 21.761 | 0.233 |
| 81611 | 101 | 431 | 761 | 420420 | 21.861 | 0.228 |
| 82601 | 101 | 431 | 761 | 425520 | 21.295 | 0.40 |
| 83591 | 101 | 431 | 761 | 430620 | 22.903 | 0.229 |
| 80177 | 152 | 317 | 647 | 409138 | 23.278 | 0.180 |
| 82487 | 152 | 317 | 647 | 420926 | 21.774 | 0.188 |
| 83477 | 152 | 317 | 647 | 425926 | 21.684 | 0.191 |
| 84137 | 152 | 317 | 647 | 409138 | 23.278 | 0.180 |
| 84467 | 152 | 317 | 647 | 431030 | 22.182 | 0.176 |

# Chapter 7

# Property: Number of terms in $\Phi_{p_1p_2p_3}$

In the chapter, we investigate explicit formulas for the number of terms in cyclotomic polynomials. The only previously known results are as follows:

1. Clearly, $\mathrm{hw}(\Phi_p(x)) = p$.

2. In [20], Carlitz founds an explicit formula for the number of terms in $\Phi_{p_1p_2}(x)$.

In this chapter, we show explicit formulas for the number of terms in the following cases:

1. $p_2 \equiv_{p_1} \pm 1$ and $p_3 \equiv_{p_1p_2} +1$.

2. $p_2 \equiv_{p_1} \pm 1$ and $p_3 \equiv_{p_1p_2} -1$.

## 7.1 Main Results

In this section we state the main results of this chapter.

**Theorem 7.1.** *Suppose that $p_2 \equiv_{p_1} +1$ or $-1$. Then*

*1.* $\mathrm{hw}(\Phi_{p_1p_2p_3}) = N \cdot (p_3 - 1) + 1 \qquad$ *if* $p_3 \equiv_{p_1p_2} +1$

*2.* $\mathrm{hw}(\Phi_{p_1p_2p_3}) = N \cdot (p_3 + 1) - 1 \qquad$ *if* $p_3 \equiv_{p_1p_2} -1$

*where*

$$\begin{aligned} N &= \frac{2}{3} \frac{(p_1 - 1)\left((p_1 + 4)(p_2 - 1) - (r_2 - 1)\right)}{p_1 p_2} \\ r_2 &= \mathrm{rem}(p_2, p_1) \end{aligned}$$

**Example 7.1.**

*1. Let*

$$\begin{aligned} p_1 =& 170141183460469231731687303715884105727 \\ p_2 =& 193960949144934924174123526236107880528\,79 \\ p_3 =& 277206261634134971844028938110798851397484 0 \\ & 91203319282999801642607689554229994773 \end{aligned}$$

*Then* $p_2 \equiv_{p_1} +1$ *and* $p_3 \equiv_{p_1 \cdot p_2} +1$*. From Theorem 7.1, we have*

$$\begin{aligned} \mathrm{hw}(\Phi_{p_1p_2p_3}) =& 3144280094472279441139867399991460381645363 1 \\ & 9378314264410227381365880859736471707987021 0 \\ & 302237053703913523370734810 4609 \end{aligned}$$

*2. Let*

$$\begin{aligned} p_1 =& 170141183460469231731687303715884105727 \\ p_2 =& 1361129467683753853853498429727072845815 9 \end{aligned}$$

$$\begin{aligned} p_3 =& 67622580114592658127365455245073738185509803 \\ & 313049731446826220708392153351876515 7 \end{aligned}$$

*Then* $p_2 \equiv_{p_1} -1$ *and* $p_3 \equiv_{p_1 \cdot p_2} +1$*. From Theorem 7.1, we have*

$$\begin{aligned} \mathrm{hw}(\Phi_{p_1 p_2 p_3}) =& 767025720623145861999031980616129015405383 20 \\ & 1348107546824075031297870699472828776106967 5 \\ & 8415342362606954703001208582545 \end{aligned}$$

*3. Let*

$$\begin{aligned} p_1 =& 170141183460469231731687303715884105727 \\ p_2 =& 193960949144934924174123526236107880528 79 \\ p_3 =& 75901714495060766100150780673194923596930 \\ & 167829480279868993306904486425562974758 9 \end{aligned}$$

*Then* $p_2 \equiv_{p_1} +1$ *and* $p_3 \equiv_{p_1 \cdot p_2} -1$*. From Theorem 7.1, we have*

$$\begin{aligned} \mathrm{hw}(\Phi_{p_1 p_2 p_3}) =& 860933835391219370788297026188137961640 99 \\ & 2303059670009694670210882769020707005867 1 \\ & 073194875172885141667980657964361975 9 \end{aligned}$$

*4. Let*

$$
\begin{aligned}
p_1 =& 170141183460469231731687303715884105727 \\
p_2 =& 136112946768375385385349842972707284581 59 \\
p_3 =& 463168356949264781694283940034751631407 6 \\
& 013925551351468960700048520010503553185 9
\end{aligned}
$$

*Then* $p_2 \equiv_{p_1} -1$ *and* $p_3 \equiv_{p_1 \cdot p_2} -1$*. From Theorem 7.1, we have*

$$
\begin{aligned}
\mathrm{hw}(\Phi_{p_1 p_2 p_3}) =& 52536008261859305616372053466858151740094739 81 \\
& 83635306043887007738267602378649846648607934 35 \\
& 16600178558541301452642639
\end{aligned}
$$

**Remark 7.1** (Sparsity of $\Phi_{p_1 p_2 p_3}$)**.** *For large* $p_1, p_2$ *and* $p_3$*, the families of cyclotomic polynomials considered in this chapter are very sparse. To see this, consider the ratio*

$$
\begin{aligned}
\frac{\mathrm{hw}\left(\Phi_{p_1 p_2 p_3}\right)}{\deg\left(\Phi_{p_1 p_2 p_3}\right)} &= \frac{\frac{2}{3} \frac{(p_1-1)((p_1+4)(p_2-1)-(r_2-1))}{p_1 p_2} (p_3 \mp 1) \pm 1}{(p_1-1)(p_2-1)(p_3-1)} \\
&\approx \frac{\frac{2}{3} \frac{p_1(p_1 p_2 - r_2)}{p_1 p_2} p_3}{p_1 p_2 p_3} \\
&\approx \frac{\frac{2}{3} \frac{p_1 p_1 p_2}{p_1 p_2} p_3}{p_1 p_2 p_3} \\
&\approx \frac{2}{3} \frac{1}{p_2}
\end{aligned}
$$

## 7.2 Proof

**Notation 7.1.** *Let*

$$m = p_1 p_2$$

$$q_2 = \mathrm{quo}(p_2, p_1)$$

$$r_2 = \mathrm{rem}(p_2, p_1)$$

$$q_3 = \mathrm{quo}(p_3, p_1 p_2)$$

$$r_3 = \mathrm{rem}(p_3, p_1 p_2)$$

**Remark 7.2.** *From lemma 3.6 from chapter 3, we have*

$$\begin{aligned} f_{m,p,i,0} &= \mathcal{N}\mathcal{R}_{\mathrm{rem}(ir,m)}(\Psi_m \cdot \mathcal{E}_r \mathcal{T}_{i+1} \Phi_m) \\ &= -\mathrm{rem}(x^{m-\mathrm{rem}(ir,m)} \Psi_m \sum_{s=0}^{i} a_s x^{sr}, x^m - 1) \end{aligned}$$

*where* $\Phi_m(x) = \sum_{s=0}^{\varphi(m)} a_s x^s$. *In this chapter we frequently use both versions of the previous equation.*

**Lemma 7.1.** *Let* $r_2 = 1$. *Then*

$$f_{p_1,p_2,i,0} = \begin{cases} 1 - x & i = 0 \\ -x + x^{p_1 - i} & i \neq 0 \end{cases}$$

$$f_{p_1,p_2,i,q_2} = \begin{cases} 1 & i = 0 \\ 0 & i \neq 0 \end{cases}$$

*Proof.* Note

$$
\begin{aligned}
f_{p_1,p_2,i,0} &= \mathcal{N}\mathcal{R}_{\mathrm{rem}(i\cdot 1,p_1)}(\Psi_{p_1}\cdot\mathcal{E}_1\mathcal{T}_{i+1}\Phi_{p_1}) && \text{Lemma 3.6}\\
&= -\mathrm{rem}(x^{p_1-i}\ (x-1)\sum_{s=0}^{i}x^s, x^{p_1}-1)\\
&= -\mathrm{rem}(x^{p_1-i}\left(x^{i+1}-1\right), x^{p_1}-1) && \text{cancelling}\\
&= -\mathrm{rem}(x^{p_1+1}-x^{p_1-i}, x^{p_1}-1)\\
&= -\begin{cases} x-1 & i=0\\ x-x^{p_1-i} & i\neq 0\end{cases}\\
&= \begin{cases} 1-x & i=0\\ -x+x^{p_1-i} & i\neq 0\end{cases}\\
&\qquad (\text{Note } p_1-i\geq p_1-q_2=p_1-\left\lfloor\frac{\varphi\left(p_1p_2\right)}{p_2}\right\rfloor=2)\\
f_{p_1,p_2,i,q_2} &= \mathcal{T}_1 f_{p_1,p_2,i,0}\\
&= \begin{cases} \mathrm{rem}(1-x,x^1) & i=0\\ \mathrm{rem}(-x+x^{p_1-i},x^1) & i\neq 0\end{cases}\\
&= \begin{cases} 1 & i=0\\ 0 & i\neq 0\end{cases}
\end{aligned}
$$

□

**Lemma 7.2.** *Let $r_2=1$. Then for $i\neq 0$ we have*

1. $\Phi_{p_1}\cdot(-x+x^{p_1-i}) \quad = \quad (-1+x^{p_1}) \quad \cdot \displaystyle\sum_{s=1}^{p_1-1-i} x^s$
2. $\Phi_{p_1}\cdot f_{p_1,p_2,i} \quad = \quad (-1+x^{p_1q_2})\cdot \displaystyle\sum_{s=1}^{p_1-1-i} x^s$

*Proof.*

1. Note

$$
\begin{aligned}
\Phi_{p_1} \cdot (-x + x^{p_1-i}) &= \left(\sum_{s=0}^{p_1-1} x^s\right) \ (-x + x^{p_1-i}) \\
&= \left(\sum_{s=0}^{p_1-1} x^s\right) \ (-1+x) \ \left(\sum_{s=1}^{p_1-i-1} x^s\right) && \text{factoring} \\
&= (-1 + x^{p_1}) \ \left(\sum_{s=1}^{p_1-1-i} x^s\right) && \text{cancelling}
\end{aligned}
$$

2. Note

$$
\begin{aligned}
\Phi_{p_1} \cdot f_{p_1,p_2,i} &= \Phi_{p_1} \cdot \sum_{j=0}^{q_2} f_{p_1,p_2,i,j} x^{jp_1} \\
&= \left(\sum_{s=0}^{p_1-1} x^s\right) \ \left(\sum_{j=0}^{q_2-1} (-x + x^{p_1-i}) \ x^{jp_1} + 0 \ x^{q_2 p_1}\right) && \text{Lemma 7.1} \\
&= \left(\sum_{s=0}^{p_1-1} x^s\right) (-x + x^{p_1-i}) \ \left(\sum_{j=0}^{q_2-1} x^{jp_1}\right) \\
&= \left(\sum_{s=0}^{p_1-1} x^s\right) (-1+x) \left(\sum_{s=1}^{p_1-i-1} x^s\right) \ \left(\sum_{j=0}^{q_2-1} x^{jp_1}\right) && \text{factoring} \\
&= (-1 + x^{p_1}) \left(\sum_{s=1}^{p_1-i-1} x^s\right) \ \left(\sum_{j=0}^{q_2-1} x^{jp_1}\right) && \text{cancelling} \\
&= \left(\sum_{s=1}^{p_1-i-1} x^s\right) (-1 + x^{p_1}) \left(\sum_{j=0}^{q_2-1} x^{jp_1}\right) \\
&= \left(\sum_{s=1}^{p_1-i-1} x^s\right) (-1 + x^{q_2 p_1}) && \text{cancelling}
\end{aligned}
$$

$\square$

**Lemma 7.3** (Multiples of $p_1$)**.** *Let* $r_2 = 1, r_3 = 1$ *and* $i = (uq_2 + v)\, p_1,$ *where*

$0 \leq u \leq \frac{(p_1-1)}{2} - 1$ *and* $0 \leq v \leq q_2 - 1$. *Then*

$$\mathrm{hw}\left(f_{m,p_3,i,0}\right) = 2(p_1 - u)$$

*Proof.* Let $i = (uq_2 + v)p_1$. Then we consider the following cases:

- Case $v = 0$. Then we claim that

$$f_{m,p_3,i,0} = x^{m-i} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u}^{p_1-1} x^{p_2+s}$$

  we will use induction on $u$ to prove the claim.

  1. If $u = 0$, then

$$\begin{aligned} f_{m,p_3,0,0} &= -\operatorname{rem}(\Psi_m \cdot (a_0x^0), x^m - 1)) && \text{by Lemma 3.6} \\ &= -\left(\operatorname{rem}(\Psi_m \cdot (1), x^m - 1)\right) && a_0 = 1 \\ &= -\Psi_m \\ &= 1 + \sum_{s=1}^{p_1-1} x^s - \sum_{s=0}^{p_1-1} x^{p_2+s} \end{aligned}$$

  2. Assume

$$f_{m,p_3,uq_2p_1,0} = x^{m-u-q_2p_1} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u}^{p_1-1} x^{p_2+s}$$

  3. Consider $f_{m,p_3,i,0}$, where $i = (u+1)q_2p_1$

$$\begin{aligned} f_{m,p_3,i,0} &= -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) && i < m \\ &= -\operatorname{rem}(x^{m-i}\Psi_m \cdot \sum_{s=0}^{u} x^{sp_2} f_{p_1,p_2,s}, x^m - 1) && \text{by Lemma 7.2} \end{aligned}$$

$$
\begin{aligned}
&= \operatorname{rem}(x^{m-p_1q_2} f_{m,p_3,uq_2p_1,0} \\
&\quad - x^{m+u-p_1q_2}\Psi_m f_{p_1,p_2,u}, x^m - 1) && \text{by induction} \\
&= \operatorname{rem}(x^{m-i} + \sum_{s=u+1}^{p_1-1} x^{s+m-p_1q_2} - \sum_{s=u}^{p_1-1} x^{s+1} \\
&\quad (x^{u+1} - x^{p_2+u} - x^{u-p_1q_2} + x^u) \sum_{s=1}^{p_1-1-u} x^s, x^m - 1) && \text{by Lemma 7.1} \\
&= x^{m-i} + \sum_{s=u+1}^{p_1-1} x^{s+m-p_1q_2} - \sum_{s=u}^{p_1-1} x^{s+1} + \sum_{s=1}^{p_1-1-u} x^{s+u+1} && \text{since all} \\
&\quad - x^{p_2} \sum_{s=1}^{p_1-1-u} x^{s+u} - \sum_{s=1}^{p_1-1-u} x^{s+u-p_1q_2} + \sum_{s=1}^{p_1-1-u} x^{s+u} && \text{exponents} \\
& && \text{are} \le m-1 \\
&= x^{m-i} - x^{p_1} + \sum_{s=1}^{p_1-1-u} x^{s+u+1} - x^{p_2} \sum_{s=1}^{p_1-1-u} x^{s+u} && \text{by cancelation} \\
&= x^{m-(u+1)q_2p_1} + \sum_{s=u+2}^{p_1-1} x^s - x^{p_2} \sum_{s=u+1}^{p_1-1} x^{s+u}
\end{aligned}
$$

Hence we proved the claim.

- Case $v = 1$. Consider $f_{m,p_3,i,0}$ where $i = (uq_2 + 1)p_1$

$$
\begin{aligned}
f_{m,p_3,i,0} &= -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
&= \operatorname{rem}(-x^{m-i}\Psi_m \cdot (f_{m,p_3,0} + \cdots \\
&\quad + x^{up_2}(x^{p_1-u} - x), x^m - 1) && \text{by Lemma 7.1} \\
&= \operatorname{rem}\left(\left(x^{m-p_1} f_{m,p_3,uq_2p_1} + x^{u+1-p_1}\Psi_m - \Psi_m\right), x^m - 1\right) && \text{by the case } v = 0 \\
&= \operatorname{rem}((x^{m-p_1}(x^{m-uq_2p_1} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u}^{p_1-1} x^{p_2+s})
\end{aligned}
$$

$$
\begin{aligned}
&\quad + x^{u+1-p_1}\Psi_m - \Psi_m), x^m - 1) \\
&= x^{m-i} + \sum_{s=u+1}^{p_1-1} x^{s+m-p_1} - \sum_{s=u}^{p_1-1} x^{p_2-p_1+s} && \text{since exponents} \\
&\quad - \sum_{s=0}^{p_1-1} x^{s+u+1+m-p_1} + \sum_{s=0}^{p_1-1} x^{p_2-p_1+u+1+s} + \Psi_m && \text{are} \le m-1 \\
&= x^{m-i} - \sum_{s=0}^{u} x^s + x^{p_2}\sum_{s=0}^{u} x^s + x^{p_2-p_1+u} + \Psi_m && \text{by cancelation} \\
&= x^{m-i} - x^{p_2-p_1+u} + \sum_{s=u+1}^{p_1-1} x^s - x^{p_2}\sum_{s=u+1}^{p_1-1} x^s
\end{aligned}
$$

- Case $v > 1$. Consider $f_{m,p_3,i,0}$ where $i = (uq_2 + v)p_1$

$$
\begin{aligned}
f_{m,p_3,i,0} &= -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
&= -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{(uq_2 j+1)p_1} a_s x^s, x^m - 1) \qquad a_s = 0 \text{ for} \\
&\qquad\qquad\qquad\qquad\qquad\qquad (uq_2+1)p_1 < s < (uq_2+v)p_1 \\
&= -\operatorname{rem}(x^{m-p_1(v-1)} f_{m,p_3,(uq_2+1)p_1,0}, x^m - 1)
\end{aligned}
$$

Hence $\operatorname{hw}(f_{m,p_3,i,0}) = 2(p_1 - u)$ as desired. $\square$

**Lemma 7.4** (Non Multiples of $p_1$). *Let $r_2 = 1, r_3 = 1$ and $i = (uq_2 + v)\,p_1 + t$, where $0 \le u \le \frac{(p_1-1)}{2} - 1, 0 \le v \le q_2 - 1$ and $1 \le t \le p_1 - 1$. Then*

$$
\operatorname{hw}(f_{p_1,p_2,i,0}) = \begin{cases} 2(p_1 - u) & t = 1, \cdots, u \\ 2(2+u) & t = u+1, \cdots, p_1 - 1 \end{cases}
$$

*Proof.* We consider the following cases:

- Case $1 \leq t \leq u$. We have $a_{(uq_2+v)p_1+t} = 0$ by Lemma 7.2. Therefore $f_{m,p_3,i,0} = \text{rem}(x^{m-t} f_{m,p_3,i,0}, x^m - 1)$. Thus for $1 \leq t \leq u$

$$\text{hw}(f_{m,p_3,i,0}) = 2(p_1 - u)$$

  since the rotation does not change the number of terms

- Case $t = u + 1$. Here we have two cases:

  1. $v = 0$

$$\begin{aligned}
f_{m,p_3,,0} =& \; - \text{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
=& \; - \text{rem}(x^{m-(i}\Psi_m \cdot (f_{p_1,p_2,0} + \cdots \\
& + x^{p_2(u-1)} f_{p_1,p_2,u-1} - x^{i-t+(u+1)}), x^m - 1) && \text{by Lemma7.1} \\
=& \; \text{rem}(x^{m-(u+1)} f_{m,p_3,i-t,0} + \Psi_m, x^m - 1) \\
=& \; \text{rem}(x^{m-(u+1)}(x^{m-i+t} + \sum_{s=u+1}^{p_1-1} x^s \\
& - \sum_{s=u}^{p_1-1} x^{p_2+s}) + \Psi_m, x^m - 1) && \text{by Lemma 7.3} \\
=& \; x^{m-(p_2u+1))} + \sum_{s=u+1}^{p_1-1} x^{s-u-1} && \text{by distribution} \\
& + \sum_{s=u}^{p_1-1} x^{p_2+s-u-1} + \Psi_m && \text{and exponents} \leq m \\
=& \; x^{m-(p_2u+1)} - x^{p_2-1} + \sum_{s=0}^{p_1-u-2} x^s
\end{aligned}$$

$$- \sum_{s=0}^{p_1-u-2} x^{p_2+s} + \Psi_m \qquad \text{by changing index}$$

$$= x^{m-(p_2u+1)} - x^{p_2-1} - \sum_{s=p_1-u-1}^{p_1-1} x^s$$

$$+ \sum_{s=p_1-u-1}^{p_1-1} x^{p_2+s} \qquad \text{by cancelation}$$

$$= x^{m-(p_2u+1)} - x^{p_2-1} - \sum_{s=1}^{u+1} x^{p_1-s} + \sum_{s=1}^{u+1} x^{p_1+p_2-s} \qquad \text{by changing index}$$

2. Case $v \neq 0$. Then $i = (uq_2 + v)p_1 + u + 1$

$$f_{m,p_3,i,0} = \text{rem}(-x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1)$$

$$= \text{rem}(-x^{m-i}\Psi_m \cdot (f_{p_1,p_2,0} + \cdots + x^{p_2(u-1)} f_{p_1,p_2,u-1}$$

$$+ x^{p_2u} \sum_{w=0}^{v-1} (x^{p_1-u} - x) x^{p_1 w} \quad - x^{p_2 j + p_1 v + 1}), x^m - 1)$$

$$= \text{rem}(x^{m-(p_1v+1)}(x^u f_{m,p_3,p_1q_2u} - \Psi_m \sum_{w=0}^{v-1} (x^{p_1-u} - x) x^{p_1 w}$$

$$+ \Psi_m, x^m - 1)$$

$$= \text{rem}(x^{m-(p_1v+u+1)}(x^{m-p_1q_2u} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u}^{p_1-1} x^{p_2+s})$$

$$- x^{m-(p_1v+1)}\Psi_m \sum_{w=0}^{v-1} (x^{p_1-u} - x) x^{p_1 w} + \Psi_m, x^m - 1)$$

$$= x^{m-i} - x^{p_2-p_1v-1} + x^{m-p_1v} \sum_{s=u+1}^{p_1-1} x^{s-u-1}$$

$$- x^{m-p_1v} \sum_{s=u}^{p_1-1} x^{p_2+s-u-1} - x^{m-(p_1v+1)}\Psi_m \sum_{w=0}^{v-1} (x^{p_1-u} - x) x^{p_1 w} + \Psi_m$$

$$= x^{m-i} - x^{p_2-p_1v-1} + x^{m-p_1v} \sum_{s=0}^{p_1-u-2} x^s - x^{m-p_1v} \sum_{s=0}^{p_1-u-2} x^{p_2+s}$$

$$
\begin{aligned}
&- x^{m-(p_1v+1)}\Psi_m \sum_{w=0}^{v-1}(x^{p_1-u} - x)x^{p_1 w} + \Psi_m \\
&= x^{m-i} - x^{p_2-p_1v-1} + \sum_{s=0}^{p_1-u-2} x^s - \sum_{s=0}^{p_1-u-2} x^{p_2+s} + \Psi_m \\
&= x^{m-i} - x^{p_2-p_1v-1} + \sum_{s=p_1-u-1}^{p_1-1} x^s - \sum_{s=p_1-u-1}^{p_1-1} x^{p_2+s} \\
&= x^{m-i} - x^{p_2-p_1v-1} + \sum_{s=1}^{u+1} x^{p_1-s} - \sum_{s=1}^{u+1} x^{p_2+p_1-s}
\end{aligned}
$$

- Case $u + 1 < t < p_1 - 1$. Then $i = (q_2u + v)p_1 + t$.

  From Lemma 7.1 we have $a_s = 0 \quad$ for $(uq_2 + v)p_1 + u + 2 \leq s \leq (uq_2 + v)p_1 + p_1 - 1$.

  Hence

$$
\begin{aligned}
f_{m,p_3,i,0} &= \operatorname{rem}(-x^{m-i}\Psi_m \sum_{s=0}^{i-t+u+1} a_s x^s, x^m - 1) \\
&= \operatorname{rem}(-x^{t-u-1} f_{m,p_3,(uq_2+v)p_1+(j+1),0}, x^m - 1)
\end{aligned}
$$

  Thus $\operatorname{hw}(f_{m,p_3,i,0}) = \operatorname{hw}(f_{m,p_3,(uq_2+v)p_1+(j+1),0})$

From all the previous cases we have

$$
\operatorname{hw}(f_{m,p_p,(uq_2+v)p_1+t,0}) = \begin{cases} 2(p_1 - u) & t = 1, \cdots, u \\ 2(2 + u) & t = u + 1, \cdots, p_1 - 1 \end{cases}
$$

$\square$

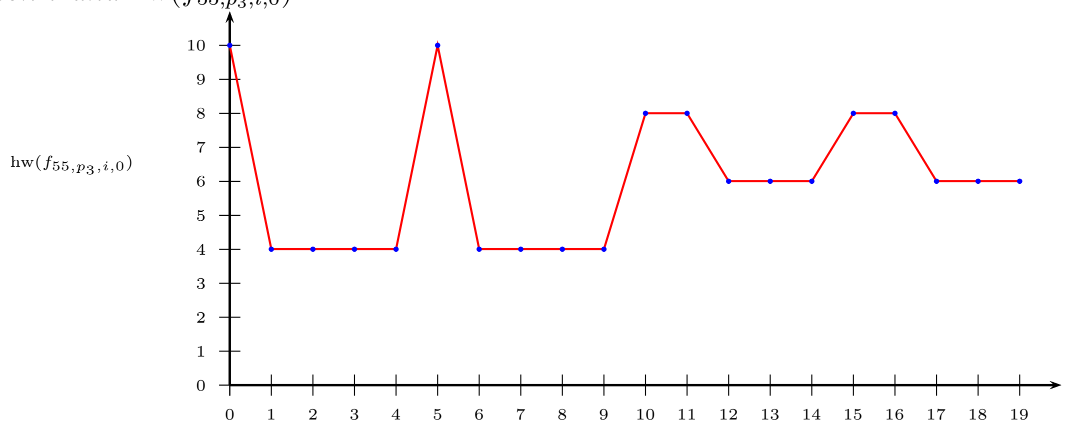
**Lemma 7.5.** *Let* $r_2 = 1, r_3 = 1$ *and* $i = (uq_2 + v)\, p_1 + t,$ *where* $0 \leq u \leq \frac{(p_1-1)}{2} - 1,$

$0 \leq v \leq q_2 - 1$ *and* $1 \leq t \leq p_1 - 1$. *Then*

$$\mathrm{hw}(f_{m,p_3,i,0}) = \begin{cases} 2(p_1 - u) & t = 0, \cdots, u \\ 2(2+u) & t = u+1, \cdots, p_1 - 1 \end{cases}$$

*Proof.* Immediate from the previous two lemmas. $\square$

**Example 7.2.** *We will illustrate Lemma 7.5 by an example. Let* $p_1 = 5, p_2 = 11$ *and* $p_3 = 331$. *Note that* $r_2 = 1$ *and* $r_3 = 1$. *The following figure presents the relationship between* $i$ *and* $\mathrm{hw}(f_{55,p_3,i,0})$.




**Lemma 7.6.** *Let* $r_2 = p_1 - 1$. *Then* $f_{p_1,p_2,i,j} = (1 - x^{i+1})$.

*Proof.* Note

$$\begin{aligned} f_{p_1,p_2,i,0} &= \mathcal{NR}_{(p_1-1)} f_{p_1,\tilde{p_2},\tilde{i},0} && \text{by Structure 4} \\ &= \begin{cases} \mathcal{NR}_{(p_1-1)}(1-x) & i = p_1 - 2 \\ \mathcal{NR}_{(p_1-1)}(-x + x^{i+2}) & i \neq p_1 - 2 \end{cases} && \text{by Lemma 7.2} \\ &= \begin{cases} \mathrm{rem}(-x^{p_1-1}(1-x), x^{p_1} - 1) & i = p_1 - 2 \\ \mathrm{rem}(-x^{p_1-1}(-x + x^{i+2}), x^{p_1-1}) & i \neq p_1 - 2 \end{cases} \end{aligned}$$

$$
\begin{aligned}
&= 1 - x^{i+1} \\
f_{p_1,p_2,i,q_2} &= \mathcal{T}_{p_1-1} f_{p_1,p_2,i,0} \\
&= 1 - x^{i+1}
\end{aligned}
$$

□

**Lemma 7.7.** *Let $r_2 = p_1 - 1$. For $i \neq 0$, we have*

1. $\Phi_{p_1} \cdot (1 - x^{i+1}) = (1 - x^{p_1}) \cdot \sum_{s=0}^{i} x^s$
2. $\Phi_{p_1} \cdot f_{p_1,p_2,i} = (1 - x^{(q_2+1)p_1}) \cdot \sum_{s=0}^{i} x^s$

*Proof.*

1. Note

$$
\begin{aligned}
\Phi_{p_1} \cdot (1 - x^{i+1}) = &\left(\sum_{s=0}^{p_1-1} x^s\right)(1 - x^{i+1}) \\
&= (1 + x + \cdots + x^{p_1-1}) - (x^{i+1} + x^{i+2} + \cdots + x^{i+p_1}) && \text{expanding} \\
&= (1 + \cdots + x^i) - (x^{p_1} + \cdots + x^{p_1+i}) && \text{cancelling} \\
&= (1 - x^{p_1}) \cdot \sum_{s=0}^{i} x^s && \text{factoring}
\end{aligned}
$$

2. Note

$$
\begin{aligned}
\Phi_{p_1} \cdot f_{p_1,p_2,i} &= \Phi_{p_1} \cdot (1 - x^{i+1}) \sum_{s=0}^{q_2} x^{sp_1} && \text{by Lemma 7.6} \\
&= (1 - x^{p_1}) \sum_{s=0}^{i} x^s \cdot \sum_{s=0}^{q_2} x^{sp_1}
\end{aligned}
$$

$$= \left(\sum_{s=0}^{q_2} x^{sp_1} - x^{p_1}\sum_{s=0}^{q_2} x^{sp_1}\right)\sum_{s=0}^{i} x^s$$

$$= (1 - x^{p_1(q_2+1)})\sum_{s=0}^{i} x^s \qquad \text{cancelling}$$

□

**Lemma 7.8** ($p_2u+t$)**.** *Let $i = p_2u + t$ where $0 \le u \le \frac{(p_1-1)}{2}$ and $0 \le t \le u$. Then*

$$\mathrm{hw}(f_{m,p_3,i,0}) = 2(p_1 - u)$$

*Proof.* We consider the following cases:

1. Case $t = 0$. We claim that

$$f_{m,p_3,i,0} = x^{m-i} - x^{p_2} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u+1}^{p_1-1} x^{p_2+s}$$

   We will use induction on $u$ to prove the claim

   (a) $f_{m,p_3,0,0} = x^m + x^{p_2} + \sum_{s=1}^{p_1-1} x^s - \sum_{s=j+1}^{p_1-1} x^{p_2+s} = -\Psi_m$

   (b) Assume that $f_{m,p_3,i,0} = x^{m-i} - x^{p_2} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u+1}^{p_1-1} x^{p_2+s}$

   (c) Consider $f_{m,p_2,p_2(u+1),0}$

$$\begin{aligned} f_{m,p_3,p_2(u+1),0} = &- \mathrm{rem}(x^{m-p_2(u+1)}\Psi_m \sum_{s=0}^{p_2(u+1)} a_s x^s, x^m - 1) \\ = &- \mathrm{rem}(x^{m-p_2(u+1)}\Psi_m \cdot \sum_{s=0}^{u} x^{p_2 s} f_{m,p_3,s} \\ &+ x^{m-p_2(u+1)}\Psi_m x^{p_2(u+1)}, x^m - 1) \end{aligned}$$

$$
\begin{aligned}
&= -\operatorname{rem}(x^{m-p_2}(f_{m,p_3,p_2u,0} - \Psi_m f_{m,p_3,u} \\
&\quad - \Psi_m(1-x^{p_2})), x^m - 1) && \text{by induction} \\
&= -\operatorname{rem}(x^{m-p_2(u+1)} - 1 + \sum_{s=u+1}^{p_1-1} x^{s+m-p_2} \\
&\quad - \sum_{s=u+1}^{p_1-1} x^s + x^{m-p_2}\Psi_m f_{m,p_3,u} \\
&\quad - \Psi_m \cdot (-x^{m-p_2} + 1), x^m - 1) \\
&= -x^{m-p_2(u+1)} - 1 + \sum_{s=u+1}^{p_1-1} x^{s+m-p_2} - \sum_{s=u+1}^{p_1-1} x^s \\
&\quad + x^{m-p_2}\Psi_m f_{m,p_3,u} - \Psi_m \cdot (-x^{m-p_2} + 1) && \text{by expanding} \\
&= -x^{m-p_2(u+1)} - x^{p_2} - \sum_{s=0}^{u+1} x^s + \sum_{s=0}^{u} x^{s+p_2} && \text{by carrying} \\
&\quad - \sum_{s=0}^{p_1-1} x^{s+p_2} + \sum_{s=0}^{p_1-1} x^s && \text{calculations} \\
&= x^{m-p_2(u+1)} - x^{p_2} + \sum_{s=u+2}^{p_1-1} x^s - \sum_{s=u+2}^{p_1-1} x^{p_2+s}
\end{aligned}
$$

2. Case $t \neq 0$. Since $a_s = 0$ for $s = p_2u+1, \cdots, p_2u+t$. Hence we have

$$
\begin{aligned}
f_{m,p_3,i,0} &= -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
&= -\operatorname{rem}(x^{m-t} f_{m,p_3,p_2u,0}, x^m - 1)
\end{aligned}
$$

From all cases above we have $\operatorname{hw}(f_{m,p_3,i,0}) = 2(p_1 - u)$ as desired. □

**Lemma 7.9** ($p_2u + p_1v$)**.** *Let* $i = p_2u + p_1v$ *where* $0 \leq u \leq \frac{(p_1-1)}{2}$ *and* $1 \leq v \leq q_2 - 1$. *Then*

$$\mathrm{hw}(f_{m,p_3,i,0}) = 2(p_1 - u)$$

*Proof.*

$$\begin{aligned}
f_{m,p_3,i,0} &= -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} x^s, x^m - 1) \\
&= -\operatorname{rem}(x^{m-i}\Psi_m \cdot (\sum_{k=0}^{u-1} x^{kp_2} f_{p_1,p_2,s} + x^{up_2} \sum_{w=0}^{v-1} (1 - x^{u+1}) x^{wp_1} \\
&\quad + x^{p_2 u + v p_1}), x^m - 1) && \text{by Lemma 7.6} \\
&= -\operatorname{rem}(x^{m-p_1 v} f_{m,p_3,p_2 u,0} + x^{m-p_1 k}(1 - x^{p_2})(1 - x^{p_1 k}) \cdot \sum_{s=0}^{u} x^s \\
&\quad - \Psi_m \cdot (-x^{m-p_1 k} + 1), x^m - 1) \\
&= -\operatorname{rem}(x^{m-vp_1} f_{m,p_3,p_2 u,0} - x^{m-vp_1}\Psi_m \cdot (1 - x^{u+1}) \sum_{w=0}^{v-1} x^{wp_1} \\
&\quad - \Psi_m \cdot (1 - x^{m-vp_1}), x^m - 1) \\
&= -x^{m-i} - x^{p_2 - vp_1} + \sum_{s=u+1}^{p_1-1} x^{s-vp_1} - \sum_{s=u+1}^{p_1-1} x^{p_2+s-vp_1} && \text{since all} \\
&\quad + (1 - x^{p_2})(x^{m-vp_1} - 1) \cdot \sum_{s=0}^{u} x^s - \Psi_m \cdot (-x^{m-vp_1} + 1) && \text{exponents } > m \\
&= -x^{m-i} - x^{p_2 - vp_1} - x^{m-vp_1}\Psi_m + (-1 + x^{p_2}) \cdot \sum_{s=0}^{u} x^s \\
&\quad - \Psi_m \cdot (-x^{m-vp_1} + 1) && \text{by accumulation} \\
&= x^{m-i} - x^{p_2 - vp_1} + (-1 + x^{p_2}) \cdot \sum_{s=0}^{u} x^s - \Psi_m && \text{by cancelation} \\
&= x^{m-i} - x^{p_2 - vp_1} + \sum_{s=u+1}^{p_1-1} x^s - \sum_{s=u+1}^{p_1-1} x^{p_2+s}
\end{aligned}$$

$\square$

**Lemma 7.10** $(up_2 + q_2p_1)$**.** *Let* $i = up_2 + q_2p_1$*, where* $0 \le u \le \frac{(p_1-1)}{2}$*. Then we have*

$$\mathrm{hw}(f_{m,p_3,i,0}) = 2(p_1 - u - 1)$$

*Proof.*

$$\begin{aligned}
f_{m,p_3,i,0} = & -\mathrm{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
= & -\mathrm{rem}(x^{m-i}\Psi_m \cdot (\sum_{s=0}^{up_2+(q_2-1)p_1} a_s x^s - x^{i-p_1+u+1} + x^i), x^m - 1) \quad \text{by Lemma 7.6} \\
= & \,\mathrm{rem}(x^{m-p_1} f_{m,p_3,i-p_1,0} - \Psi_m \cdot (1 - x^{m+u+1-p_1}), x^m - 1) \\
= & \, x^{m-i} - x^{p_2-(q_2-2)p_1} + \sum_{s=u+1}^{p_1-1} x^{m-p_1+s} \quad \text{since all} \\
& - \sum_{s=u+1}^{p_1-1} x^{p_2-p_1+s} - \Psi_m + x^{m+u+1-p_1}\Psi_m \quad \text{exponents} > m \\
= & \, x^{m-i} + \sum_{s=u+1}^{p_1-2} x^s - \sum_{s=u+1}^{p_1-1} x^{p_2+s}
\end{aligned}$$

Hence $\mathrm{hw}(f_{m,p_3,u,0}) = 2(p_1 - u - 1)$ as desired. □

**Lemma 7.11** $(up_2 + vp_1 + t)$**.** *Let* $i = up_2 + vp_1 + t$*, where* $0 \le u \le \frac{(p_1-1)}{2}$ *and* $u + 1 \le t \le p_1 - 1$ *and* $0 \le v \le q_2$*. Then*

$$\mathrm{hw}(f_{m,p_3,i,0}) = 2(2 + u)$$

*Proof.* We consider the following cases:

1. Case $v = 0$ and $t = u + 1$

$$
\begin{aligned}
f_{m,p_3,i,0} = & -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
= & -\operatorname{rem}(x^{m-i}\Psi_m \cdot (f_0 + \cdots + x^{(u-1)p_2} f_{u-1} + x^{up_2}(1 - x^{u+1})), x^m - 1) \\
= & \, x^{m-(u+1)} f_{m,p_3,up_2,0} + \Psi_m \\
= & \, x^{m-i} - x^{p_2-u-1} + \sum_{s=u+1}^{p_1-1} x^{s-u-1} \\
& - \sum_{s=u+1}^{p_1-1} x^{p_2+s-u-1} - \sum_{s=0}^{p_1-1} x^s + \sum_{s=0}^{p_1-1} x^{p_2+s} \\
= & \, x^{m-i} - x^{p_2-u-1} + \sum_{s=0}^{p_1-2-u} x^s \\
& - \sum_{s=0}^{p_1-u-2} x^{p_2+s} - \sum_{s=0}^{p_1-1} x^s + \sum_{s=0}^{p_1-1} x^{p_2+s} \\
= & \, x^{m-i} - x^{p_2-u-1} - \sum_{s=p_1-u-1}^{p_1-1} x^s + \sum_{s=p_1-u-1}^{p_1-1} x^{p_2+s} \\
= & \, x^{m-i} - x^{p_2-u-1} - \sum_{s=1}^{u+1} x^{p_1-s} + \sum_{s=1}^{u+1} x^{p_2+p_1-s}
\end{aligned}
$$

2. Case $v = 0$ and $t > u + 1$

$$
\begin{aligned}
f_{m,p_3,i,0} = & -\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} a_s x^s, x^m - 1) \\
= & -\operatorname{rem}(x^{m-(up_2+t)}\Psi_m \sum_{s=0}^{up_2+u+1} a_s x^s, x^m - 1) \\
& \quad \text{because } a_s = 0 \text{ for } up_2 + u + 2 \le s \le up_2 + k \\
= & \operatorname{rem}(x^{m-t-j-1} f_{m,p_3,up_2+u+1,0}, x^m - 1)
\end{aligned}
$$

3. Case $v \neq 0$

$$
\begin{aligned}
f_{m,p_3,i,0} = &-\operatorname{rem}(x^{m-i}\Psi_m \sum_{s=0}^{i} x^s, x^m - 1) \\
= &-\operatorname{rem}(x^{m-i}\Psi_m(f_{p_1,p_2,0} + \cdots + x^{p_2(u-1)} f_{p_1,p_2,u-1} \\
&+ x^{up_2}(1 - x^{u+1})\Psi_m \sum_{s=0}^{v} x^{sp_1}), x^m - 1) \\
= &\operatorname{rem}(x^{m-t-vp_1-u-1}(f_{m,p_3,up_2+(u+1),0}) \\
&- x^{m-t-vp_1}(1 - x^{u+1})\Psi_m \sum_{s=1}^{v} x^{sp_1}, x^m - 1) \qquad \text{by direct calculations} \\
= &\; x^{m-t}(x^{-(up_2+vp_1)} - x^{p_2-u-vp_1}) \\
&- x^{m-t}\left(\sum_{s=1}^{u+1} x^{p_1-s+1} + \sum_{s=1}^{u+1} x^{p_2+p_1-s+1}\right)
\end{aligned}
$$

From all the cases above we can see that

$$
\operatorname{hw}(f_{m,p_3,i,0}) = 2(2 + u)
$$

$\square$

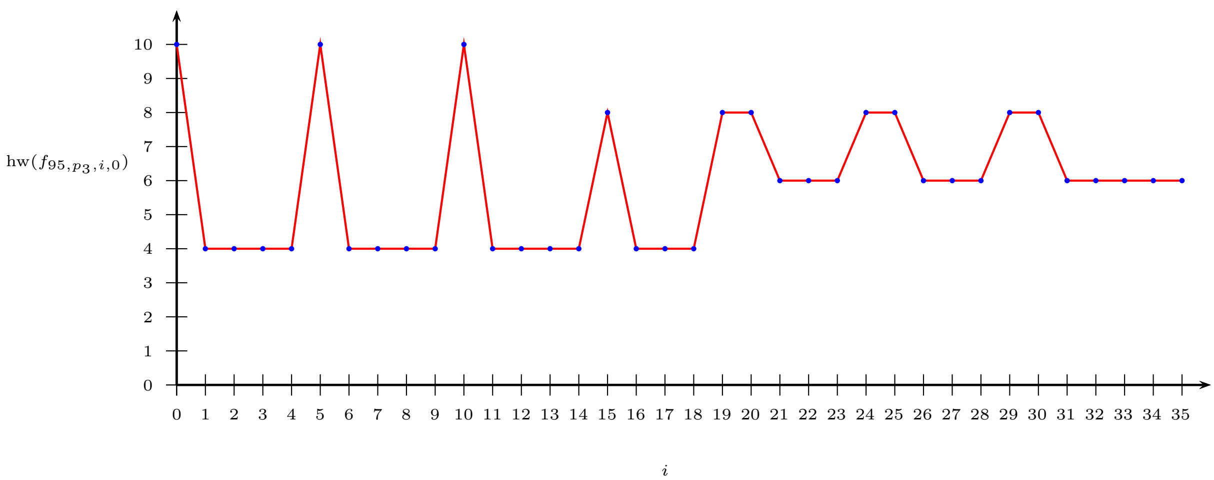
**Lemma 7.12.** *Let* $i = up_2 + vp_1 + t$, *where* $0 \leq u \leq \frac{(p_1-3)}{2}$, $0 \leq v \leq q_2$ *and* $0 \leq t \leq p_1 - 1$.

*Then*

$$\mathrm{hw}(f_{m,p_3,i,0}) = \begin{cases} 2(p_1-u) & t=0,\ldots,u \textit{ and } v=0 \\ 2(p_1-u) & v=1,\ldots,q_2-1 \textit{ and } t=0 \\ 2(p_1-u-1) & t=0 \textit{ and } v=q_2 \\ 2(2+u) & t=u+1,\ldots,p_1-1 \\ & \textit{and} \quad v=0,\ldots q_2 \end{cases}$$

*Proof.* Immediate from the previous four lemmas □

**Example 7.3.** *We will illustrate Lemma 7.12 by an example. Let* $p_1 = 5, p_2 = 19$ *and* $p_3 = 191$. *Note that* $r_2 = 4$ *and* $r_3 = 1$. *The following figure presents the relationship between* $i$ *and* $\mathrm{hw}(f_{95,p_3,i,0})$.




Next we will prove the main theorem of this chapter

*Proof of Theorem 7.1* ($p_2 \equiv_{p_1} +1$ *and* $p_3 \equiv_{p_1p_2} +1$). We have $r_2 = 1$ and $r_3 = 1$. Note

$$\mathrm{hw}(\Phi_{mp_3}) = \sum_{i=0}^{\varphi(m)-1} \mathrm{hw}(f_{m,p_3,i})$$

$$= q_3\left(\sum_{i=0}^{\varphi(m)-1} \mathrm{hw}\left(f_{m,p_3,i,0}\right)\right) + \mathrm{hw}(f_{m,p_3,i,q_3}) \qquad \text{Structure 1}$$

$$= 2q_3\left(\sum_{i=0}^{\frac{\varphi(m)}{2}-1} \mathrm{hw}\left(f_{m,p_3,i,0}\right)\right) + 1 \qquad \text{Structures 2 and 5}$$

Note that

$$\frac{\varphi(m)}{2} - 1 = \left(\left(\frac{p_1-1}{2} - 1\right) q_2 + (q_2 - 1)\right) p_1 + (p_1 - 1)$$

Thus

$$\left\{i : 0 \le i \le \frac{\varphi(m)}{2} - 1\right\} = \{(uq_2 + v)\,p_1 + t : 0 \le u \le \frac{p_1-1}{2} - 1,$$
$$0 \le v \le q_2 - 1, 0 \le t \le p_1 - 1\}$$

Hence

$$\begin{aligned}
\mathrm{hw}(\Phi_{mp_3}) &= 2q_3\left(\sum_{u=0}^{\frac{p_1-1}{2}-1}\sum_{v=0}^{q_2-1}\sum_{t=0}^{p_1-1} \mathrm{hw}\left(f_{m,p_3,(uq_2+v)p_1+t,0}\right)\right) + 1 \\
&= 2q_3\left(\sum_{u=0}^{\frac{p_1-1}{2}-1}\sum_{v=0}^{q_2-1}\left(\sum_{t=0}^{u} 2(p_1-u) + \sum_{t=u+1}^{p_1-1} 2(2+u)\right)\right) + 1 && \text{Lemma 7.5} \\
&= \frac{2}{3} q_3 q_2 p_1 \left(p_1 - 1\right)\left(p_1 + 4\right) + 1 && \text{summing and simplifying} \\
&= \frac{2}{3}\frac{p_3-1}{p_1p_2}\left(p_2-1\right)\left(p_1-1\right)(p_1+4) + 1 && q_2 = \frac{p_2-1}{p_1},\ q_3 = \frac{p_3-1}{p_1p_2} \\
&= \frac{2}{3}\frac{\left(p_1-1\right)\left(\left(p_1+4\right)\left(p_2-1\right) - \left(r_2-1\right)\right)}{p_1p_2}\left(p_3-1\right) + 1 && \text{rearranging} \\
&= N\left(p_3-1\right) + 1
\end{aligned}$$

$\square$

*Proof of Theorem 7.1* ($p_2 \equiv_{p_1} -1$ *and* $p_3 \equiv_{p_1 p_2} +1$). We have $r_2 = 1$ and $r_3 = 1$. Note

$$\begin{aligned}
\mathrm{hw}(\Phi_{mp_3}) = & \sum_{i=0}^{\varphi(m)-1} \mathrm{hw}(f_{m,p_3,i}) \\
&= q_3 \left( \sum_{i=0}^{\varphi(m)-1} \mathrm{hw}\left(f_{m,p_3,i,0}\right) \right) + \mathrm{hw}(f_{m,p_3,i,q_3}) && \text{Structure 1} \\
&= 2q_3 \left( \sum_{i=0}^{\frac{\varphi(m)}{2}-1} \mathrm{hw}\left(f_{m,p_3,i,0}\right) \right) + 1 && \text{Structures 2 and 5}
\end{aligned}$$

Note that

$$\frac{\varphi(m)}{2} - 1 = \left( \frac{p_1 - 3}{2} \right) p_2 + q_2 p_1 + \frac{(p_1 - 1)}{2}$$

Thus

$\left\{ i : 0 \le i \le \frac{(p_1-1)}{2} p_2 \right\} = \left\{ up_2 + vp_1 + t : \ 0 \le u \le \frac{p_1-3}{2},\ 0 \le v \le q_2, 0 \le t \le p_1 - 1 \right\}$

Notice that $\frac{\varphi(m)}{2} - 1 = \frac{(p_1-1)(p_2-1)}{2} - 1 < \frac{(p_1-1)}{2} p_2$, thus in computing $\mathrm{hw}(\Phi_{mp_3})$ we need only $f_{m,p_3,i,0}$ where $0 \le i \le \frac{\varphi(m)}{2} - 1$. Hence

$$\begin{aligned}
\mathrm{hw}(\Phi_{mp_3}) = 2q_3 & \left( \sum_{u=0}^{\frac{p_1-3}{2}-1} \sum_{v=0}^{q_2} \sum_{t=0}^{p_1-1} \mathrm{hw}\left(f_{m,p_3,i,0}\right) \right) \\
&+ 2q_3 \left( \sum_{v=0}^{q_2} \sum_{t=0}^{\frac{p_1-1}{2}} \mathrm{hw}\left(f_{m,p_3,i,0}\right) \right) + 1 \\
&= 2q_3 \left( \sum_{u=0}^{\frac{p_1-3}{2}-1} \left( \sum_{v=0}^{q_2} 2 \left( \sum_{t=0}^{u} (p_1 - u) + \sum_{t=u+1}^{p_1-1} (2 + u) \right) \right) \right) \\
&+ 2q_3 \left( \sum_{v=0}^{q_2} \left( \sum_{t=0}^{\frac{p_1-3}{2}} \frac{p_1+3}{2} + \sum_{t=\frac{p_1-1}{2}}^{p_1-1} \frac{p_1+1}{2} \right) + \frac{p_1+1}{2} \right)
\end{aligned}$$

$$
\begin{aligned}
&+ 2q_3(p_1 - 1 - u) + 1 && \text{Lemma 7.12} \\
&= \frac{2}{3} q_3 \left(p_1 - 1\right) \left(p_1 + 4p_1 q_2 + p_1^2 + p_1^2 q_2 - 6\right) + 1 && \text{summing and simplifying} \\
&= \frac{2}{3} \frac{p_3 - 1}{p_1 p_2} \left(p_1 - 1\right) \left(4p_2 - 2p_1 + p_1 p_2 - 2\right) + 1 && q_2 = \frac{p_2 - p_1 + 1}{p_1} \\
& && q_3 = \frac{p_3 - 1}{p_1 p_2} \\
&= \frac{2}{3} \frac{\left(p_1 - 1\right) \left(\left(p_1 + 4\right) \left(p_2 - 1\right) - \left(r_2 - 1\right)\right)}{p_1 p_2} \left(p_3 - 1\right) + 1 && \text{rearranging} \\
&= N(p_3 - 1) + 1
\end{aligned}
$$

$\square$

*Proof of Theorem 7.1 ($p_2 \equiv_{p_1} +1$ and $p_3 \equiv_{p_1 p_2} -1$).* This follows from the case

$$p_2 \equiv_{p_1} +1 \quad \text{and} \quad p_3 \equiv_{p_1 p_2} +1$$

$$
\begin{aligned}
\mathrm{hw}(\Phi_{mp_3}) &= A_{m,1}\ p_3 - B_{m,1} && \text{Theorem 6.1} \\
&= Np_3 + (N - 1) && \text{from the case } p_2 \equiv_{p_1} +1 \text{ and } p_3 \equiv_{p_1 p_2} +1 \\
&= N(p_3 + 1) - 1
\end{aligned}
$$

$\square$

*Proof of Theorem 7.1 ($p_2 \equiv_{p_1} -1$ and $p_3 \equiv_{p_1 p_2} -1$).* This follows from the case

$$p_2 \equiv_{p_1} -1 \quad \text{and} \quad p_3 \equiv_{p_1 p_2} +1$$

$$\begin{aligned}
\mathrm{hw}(\Phi_{mp_3}) &= A_{m,-1}\ p_3 - B_{m,-1} && \text{Theorem 6.1} \\
&= Np_3 + (N-1) && \text{from the case} \\
& && p_2 \equiv_{p_1} -1 \text{ and } p_3 \equiv_{p_1 p_2} +1 \\
&= N(p_3+1) - 1
\end{aligned}$$

$\square$

# REFERENCES


[1] http://www.cecm.sfu.ca/~ada26/cyclotomic/.

[2] A. Arnold. Algorithms for computing cyclotomic polynomials. Master's thesis, Simon Fraser university, 2011.

[3] A. Arnold and M. Monagan. A high-performance algorithm for calculating cyclotomic polynomials. *Proceedings of PASCO, ACM Press*, pages 112–120, 2010.

[4] A. Arnold and M. Monagan. Calculating cyclotomic polynomials of very large height. *Math. Comp.*, 80:2359–2379, 2011.

[5] S. Asgarli. Wedderburn's little theorem. http://www.math.ubc.ca/~reichst/423-project-wedderburn.pdf.

[6] G. Bachman. On the coefficients of ternary cyclotomic polynomials. *J. Number Theory*, 100:104–116, 2003.

[7] G. Bachman. Flat cyclotomic polynomials of order three. *Bull.London Math. Soc.*, 38:53–60, 2006.

[8] A. S. Bang. "om ligningen $\phi_n(x) = 0$". *Nyt Tidsskrift for Mathematio*, 6:6–12, 1895.

[9] P.T Bateman. Note on the coefficients of the cyclotomic polynomials. *Bull. Amer . Math*, 55:1180–1181, 1949.

[10] M. Beiter. The midterm coefficient of the cyclotomic polynomial $f_{pq}(x)$. *American mathematical monthly*, 71:769–770, 1964.

[11] M. Beiter. Magnitude of the coefficients of the cyclotomic polynomial $f_{pqr}$. *The American Mathematical Monthly*, 75(4):370–372, 1968.

[12] M. Beiter. Coefficients of the cyclotomic polynomial $f_{3qr}(x)$. *Fibonacci Quart*, 16:302–306, 1978.

[13] B. Bezdega. Sparse binary cyclotomic polynomials. *Journal of number theory*, 132:410–413, 2012.

[14] D. Bloom. On the coefficients of the cyclotomic polynomials. *Amer. Math. Monthly*, 75:372–377, 1968.

[15] D. Burton. *Elementary number theory.* McGraw-Hill Education, 7 edition, 2010.

[16] B. Bzdega. Bounds on ternary cyclotomic coefficients. *Acta Arithmtica 144(1), 5-16*, 2010.

[17] B. Bzdega. On the height of cyclotomic polynomials. *Acta Arithmtica 152(4), 349-359*, 2012.

[18] B. Bzdega. Jumps of ternary cyclotomic polynomials. *Acta Arithmtica 163(3), 203-213*, 2014.

[19] B. Bzdega. On a certain family of inverse ternary cyclotomic polynomials. *J. Number Theory*, 141:1–12, 2014.

[20] L. Carlitz. The number of terms in the cyclotomic polynomial $f_{pq}(x)$. *The American Mathematical Monthly*, 73(9):979–981, 1966.

[21] L. Carlitz. The sum of squares of the coefficients of cyclotomic polynomials. *Acta Mathematica Academiae Scientiarums*, 18:297–304, 1967.

[22] J. ChunGang. A specific family of cyclotomic polynomials of order three. *Sci China Math*, 53:2269–2274, 2010.

[23] P. Clark. Dirichlet's theorem on primes in arithmetic progressions. `http://math.uga.edu/~pete/4400DT.pdf`.

[24] G. Dredsen. On the middle coefficient of a cyclotomic polynomial. *Amer. Math. Monthly*, 18(6):979–981, 2004.

[25] U. Dudley. *Elementary number theory*. Dover Publications, second edition, 1978.

[26] E. Fouvry. On binary cyclotomic polynomials. *Algebra and number theory*, 7(5):12071223, 2013.

[27] H-S. Lee H. Hong, E. Lee. Explicit formula for optimal ate pairing over cyclotomic family of elliptic curves. *Finite Fields Appl*, 34:45–74, 2015.

[28] H-S. Lee H. Hong, E. Lee and C-N. Park. Maximum gap in (inverse) cyclotomic polynomial. *Journal of Number Theory*, 132:2297–2317, 2012.

[29] N. Kaplan. Flat cyclotomic polynomials of order three. *Journal of Number Theory*, 127:118–126, 2007.

[30] N. Kaplan. Bounds for the maximal height of divisors of $x^n - 1$. *Journal of Number Theory*, 129:2673–2688, 2009.

[31] N. Kaplan. Flat cyclotomic polynomials of order four and higher. *Integers*, 10:357–363, 2010.

[32] T. Y. Lam and K. H. Leung. On the cyclotomic polynomial $\phi_{pq}(x)$. *Ame. Math. Monthly*, 103(7):562–564, 1996.

[33] E. Lehmer. On the magnitude of the coefficients of the cyclotomic polynomials. *Bull. Amer. Math. Soc*, 42:389–392, 1936.

[34] A. Lenstra. Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields. In *ACISP '97 Proceedings of the Second Australasian Conference on Information Security and Privacy*, pages 127–138, 1997.

[35] A. Migotti. Aur theorie der kreisteilungsgleichung. *Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften*, 87:7–14, 1883.

[36] P. Moree. Inverse cyclotomic polynomials. *Journal of Number Theory*, 129(3):667–680, 2009.

[37] K. Rosen. *Elementary number theory and its applications*. Pearson, 2010.

[38] J. Suzuki. On coefficients of cyclotomic polynomials. *Proc. Japan Acad.*, 63:279–280, 1987.

[39] S. Tanaka and K. Nakamula. *Pairing-Based Cryptography*, chapter Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials, pages 136– 145. Springer Berlin Heidelberg, 2008.

[40] R.C. Vaughan. Bounds for the coefficients of cyclotomic polynomials. *The Michigan Mathematical Journal*, 21(4):289–295, 1975.

[41] S. Weintraub. Several proofs of the irreducibility of the cyclotomic polynomials. *Amer. Math. Monthly*, 120:537–545, 2013.

[42] B. Zhang. A note on ternary cyclotomic polynomials. *Bull. Korean Math. Soc*, 51(4):949–955, 2014.

[43] J. Zhao and X. Zhang. A proof of the corrected Beiter conjecture. *arXiv:0910.2770*, 2009.

# APPENDIX

# Appendix A

# Maple Codes

## A.1 Utilities

```
restart:
with(numtheory):
with(ListTools):
with(plots):
with(plottools):
with(FileTools):
unprotect(negate):
unprotect(rotate):

hwp := proc(f)
  local fe;
  fe := expand(f);
  return nops([coeffs(f)]);
end:

hw := proc(n)
  return hwp(cyclotomic(n,x));
end:

plist := proc(n,r,t,N)
  local S,i,p;
  S := [];
  p := t;
  for i from 1 to N do
    p := nextprime(p);
```

```
    while p mod n <> r or n mod p = 0 do
      p := nextprime(p);
    od:
    S := [op(S),p];
  od;
  return S;
end:

findprime := proc(p0,n,r)
  local q,p,P;
  for q from ceil((p0+1-r)/n) to 1000 do
    p := n*q + r;
    if isprime(p) then return p fi;
  od:
  print("findprime: FAIL"):
end:

list_plot := proc(C,w,h)
  local i,P,X;
  P := [];
  for i from 0 to nops(C)-1 do
    P := [op(P),[i-0.5,C[i+1]],[i+0.5,C[i+1]]];
  od;
  P := display(CURVES(P),color=red,thickness=1);
  X := display(CURVES([[-0.5,0],[w-0.5,0]]),linestyle=dot, thickness=1);
  return display(P,X, axes=none,view=-h..h,size=[w*5,(h+1)*20]);
end:
```

## A.2 Partition

```
block := proc(m,p,i,j)
  local f,r,q,c,Cij,e,l;
  q := iquo(p,m);
  r := irem(p,m);
  f := cyclotomic(m*p,x);
  c := k->coeff(f,x,k);
  if j < q then
    l := m-1;
  else
    l := r-1;
```

```
  fi;
  Cij := [seq(c(i*p+j*m+e),e=0..l)];
  return Cij;
end:

partition := proc(m,p)
  local q,r,k,h,P,j,i,Cij;
  k := phi(m)-1;
  q := iquo(p,m):
  r := irem(p,m):
  h := norm(cyclotomic(m*p,x),infinity):
  P := Array(0..q,0..k):
  for j from 0 to q do
    for i from 0 to k do
     Cij := block(m,p,i,j);
     P[j,i] := list_plot(Cij,m,h);
    od;
  od:
  return display(Array(P));
end:
```

## A.3 Operation

```
truncate  := (A,s) -> A[1..s]:
negate    := A     -> map(a->-a,A):
flip      := A     -> Reverse(A):
rotate    := (A,s) -> Rotate(A,s):
expan     := (A,s) -> [seq(op([A[i],0$(s-1)]),i=1..nops(A)-1),A[-1]]:

operations := proc(A,t,r,re)
  local w,h,P;
  w := nops(A);
  h := max(map(a->abs(a),A));
  P := Array(1..2,1..5);
  P[1,1] :=  list_plot(A, w,h);
  P[2,1] :=  list_plot(truncate(A,t), w,h);

  P[1,2] :=  list_plot(A, w,h);
  P[2,2] :=  list_plot(negate(A), w,h);
```

```
  P[1,3] :=  list_plot(A, w,h);
  P[2,3] :=  list_plot(flip(A), w,h);

  P[1,4] :=  list_plot(A, w,h);
  P[2,4] :=  list_plot(rotate(A,r), w,h);

  P[1,5] :=  list_plot(A, w,h);
  P[2,5] :=  list_plot(expan(A,re), w*re,h);
  display(P);
end:
```

## A.4 Structure 1

```
structure1 := proc(m,p)
  local k,h,q,r,PP,P,j,i,Cij;
  k := phi(m)-1;
  h := norm(cyclotomic(m*p,x),infinity);
  q := iquo(p,m);
  r := irem(p,m);

  PP := []:
  for j from 0 to q-1 do
  P := [];
  for i from 0 to k do
     Cij := block(m,p,i,j);
     P := [op(P),list_plot(Cij,m,h)];
  od;
  PP := [op(PP),P];
  od:
  display(Array(PP));
end:
```

## A.5 Structure 2

```
structure2 := proc(m,p)
  local h,k,q,r,C0,TC0,Cq,P,i;
  k := phi(m)-1;
  h := norm(cyclotomic(m*p,x),infinity);
  q := iquo(p,m);
```

```
  r := irem(p,m);

  P := Array(1..3,0..k);
  for i from 0 to k do
    C0[i]  := block(m,p,i,0);
    P[1,i] := list_plot(C0[i],m,h);
  od;

  for i from 0 to k do
    TC0[i] := truncate(C0[i],r);
    P[2,i] := list_plot(TC0[i],m,h);
  od;

  for i from 0 to k do
    Cq[i]  := block(m,p,i,q);
    P[3,i] := list_plot(Cq[i],m,h);
  od;

  display(Array(P));
end:
```

## A.6 Structure 3

```
structure3 := proc(m,p)
  local h,k,r,pt,q1,q2,P,Cp,Cpt,i;
  k := phi(m)-1;
  h := norm(cyclotomic(m*p,x),infinity);
  q1 := iquo(p,m);
  r  := irem(p,m);
  pt := findprime(p,m,r);
  q2 := iquo(pt,m);
  print(evaln(pt)=pt);

  P := Array(1..2,0..k);
  for i from 0 to k do
    Cp[i] := block(m,p,i,0);
    P[1,i] := list_plot(Cp[i],m,h);
  od;
```

```
  for i from 0 to k do
    Cpt[i] := block(m,pt,i,0);
    P[2,i] := list_plot(Cpt[i],m,h);
  od;

  display(Array(P));
end:
```

## A.7 Structure 4

```
structure4 := proc(m,p)
  local h,k,r,i,pt,rt,it,P,C,RC,NRC,Ct;
  h := norm(cyclotomic(m*p,x),infinity);
  k  := phi(m)-1;
  r  := irem(p,m);
  rt := -r mod m;
  pt := findprime(m,m,rt);
  print(evaln(pt)=pt);

  P := Array(1..4,0..k);
  for i from 0 to k do
    C[i]   := block(m,p,i,0);
    P[1,i] := list_plot(C[i],m,h);
  od;

  for i from 0 to k do
    RC[i]  := rotate(C[i],r);
    P[2,i] := list_plot(RC[i],m,h);
  od;

  for i from 0 to k do
    NRC[i] := negate(RC[i]);
    P[3,i] := list_plot(NRC[i],m,h);
  od;

  for i from 0 to k do
    it     := k - i;
    Ct[it]  := block(m,pt,it,0);
    P[4,i] := list_plot(Ct[it],m,h);
  od;
```

```
  display(Array(P));
end:
```

## A.8 Structure 5

```
structure5 := proc(m,p)
  local h,k,r,i,rt,it,P,C,FC,RFC,Ct;
  k  := phi(m)-1;
  h := norm(cyclotomic(m*p,x),infinity);
  r  := irem(p,m);
  rt := k-r mod m;

  P := Array(1..4,0..k);
  for i from 0 to k do
    C[i]   := block(m,p,i,0);
    P[1,i] := list_plot(C[i],m,h);
  od;

  for i from 0 to k do
    FC[i]  := flip(C[i]);
    P[2,i] := list_plot(FC[i],m,h);
  od;

  for i from 0 to k do
    RFC[i] := rotate(FC[i],rt);
    P[3,i] := list_plot(RFC[i],m,h);
  od;

  for i from 0 to k do
    it     := k - i;
    Ct[it]  := block(m,p,it,0);
    P[4,i] := list_plot(Ct[it],m,h);
  od;

  display(Array(P));
end:
```

## A.9 Norm

```
algorithm_norm := proc (m,p,k)
  local r,p1,p2,N1,N2,f1,f2, A, B;
  r := irem(p,m);
  p1 := findprime(m,m,r);
  p2 := findprime(p1,m,r);
  f1 := cyclotomic(m*p1,x);
  f2 := cyclotomic(m*p2,x);
  N1 := (norm(f1,k))^k;
  N2 := (norm(f2,k))^k;
  A  := (N2-N1)/(p2-p1) ;
  B  := N1-A*p1;
  return (A*p+B)^(1/k);
end:

compare_norm := proc(m,ps,k)
  local p,r,tp,tn,wp,wn;
  printf("%4s %10s %4s %18s %15s %15s\n","m","p",
   "r","Norm(mp)","prev(sec)","new(sec)");
  for p in ps do
    r  := irem(p,m);
    tn := time():  wn := algorithm_norm (m,p,k);         tn := time() - tn;
    tp := time():  wp := norm(cyclotomic(m*p,x),k);  tp := time() - tp;
    printf("%4d %10d %4d %18f %15.3f %15.3f\n",m,p,r,wp,tp,tn);
  od:
end:
```

## A.10 Mid terms

```
M := proc(m,p)
  local f;
  f := cyclotomic(m*p,x);
  return coeff(f,x,phi(m*p)/2);
end:

algorithm_M := proc(m,p)
  local r,p0,mid;
  r := irem(p,m);
  p0 := findprime(m,m,r);
```

```
  mid :=  M(m,p0);
  return mid;
end:

compare_M := proc(m,ps)
  local p,r,tp,tn,wp,wn;
  printf("%4s %10s %4s %12s %10s %10s\n","m","p","r","M(mp)"
         ,"prev(sec)","new(sec)");
  for p in ps do
    r  := irem(p,m);
    tn := time():  wn := algorithm_M (m,p);         tn := time() - tn;
    tp := time():  wp := M(m,p);  tp := time() - tp;
    if wp <> wn then print("ERROR:",m,p,r,wn,wp); return fi;
    printf("%4d %10d %4d %12d %10.3f %10.3f\n",m,p,r,wp,tp,tn);
  od:
end:
```

## A.11 Number of Terms

```
Nt := proc (m,p,c)
  local nt,i,f,ph;
  f  := cyclotomic (m*p,x);
  nt := 0;
  ph := phi(m*p);
  for i from 0 to ph do
     if c =coeff(f,x,i) then
       nt:= nt+1;
     fi;
  od:
  return nt;
end:

algorithm_Nt := proc (m,p,c)
  local r,p1,p2,N1,N2, A, B;
  r := irem(p,m);
  p1 := findprime(m,m,r);
  p2 := findprime(p1,m,r);
  N1 := Nt(m,p1,c);
  N2 := Nt(m,p2,c);
  A  := (Nt2-Nt1)/(p2-p1) ;
```

```
  B  := N1-A*p1;
  return A*p+B;
end:

compare_Nt := proc(m,ps,c)
  local p,r,tp,tn,wp,wn;
  printf("%4s %10s %4s %18s %15s %15s\n",
  "m","p","r","Nt(mp,c)","prev(sec)","new(sec)");
  for p in ps do
    r  := irem(p,m);
    tn := time():  wn := algorithm_Nt (m,p,c);         tn := time() - tn;
    tp := time():  wp := Nt(m,p,c);  tp := time() - tp;
    printf("%4d %10d %4d %18f %15.3f %15.3f\n",m,p,r,wp,tp,tn);
  od:
end:

ntc := proc(L,c)
  local h,n;
  h := 0;
  for n in L do
    h := h + `if`(n=c, 1, 0);
  od;
  return h;
end:

ABmpc := proc(m,p,c)
  local k,h,q,r,A,B,i,Ci0;
  k := phi(m)-1;
  q := iquo(p,m);
  r := irem(p,m);

  A := 0:
  B := 0;
  for i from 0 to k do
     Ci0 := block(m,p,i,0);
     A   := A + ntc(Ci0,c);
     B   := B + ntc(Ci0[1..r],c);
  od;
  return A/m, B-r*A/m;
end:
```

```
Amp := proc(m,p,c)
  local k,h,q,r,A,B,i,Ci0;
  k := phi(m)-1;
  q := iquo(p,m);
  r := irem(p,m);

  A := []:
  for i from 0 to k do
     Ci0 := block(m,p,i,0);
     A   := [op(A), ntc(Ci0,c)];
  od;
  return add(A[i],i=1..nops(A)),A;
end:
```