ABSTRACT

AMBROSINO, MARY ELIZABETH. Maximum Gap of (Inverse) Cyclotomic Polynomials. (Under the direction of Hoon Hong.)

The cyclotomic polynomial Φ_n is the monic polynomial whose zeroes are the n-th primitive roots of unity and the inverse cyclotomic polynomial Ψ_n is the monic polynomial whose zeroes are the n-th non-primitive roots of unity. They have numerous applications in number theory, abstract algebra, and cryptography. Thus it is beneficial to further our understanding of their properties. In this dissertation, we present results on the size of their maximum gap, that is, the largest difference between consecutive exponents in the polynomials, denoted $g(\Phi_n)$ and $g(\Psi_n)$. In this paper, we assume that n is odd, square-free. A summary of results is as follows: We present lower bounds for $g(\Phi_n)$ and $g(\Psi_n)$:

1. We prove five lower bounds: $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$, δ^{-} and $\varepsilon^{\pm}$
2. We observe that they are very often equal to $g(\Phi_n)$ and $g(\Psi_n)$
3. We analyze their time complexity compared to direct computation of $g(\Phi_n)$ and $g(\Psi_n)$

We discuss an exact expression for $g(\Phi_n)$:

1. We conjecture that, for $n = mp$ where m is a product of odd primes and p is an odd prime, $g(\Phi_{mp}) = \varphi(m)$ if and only if $p > m$
2. We present an algorithm which we use to check the conjecture for infinitely many values of mp
3. We prove the conjecture when $m = p_1p_2$ and $p = p_3$, where $p_3 \equiv_{p_1p_2} +1$, $p_2 \equiv_{p_1} \pm 1$

We discuss an exact expression for $g(\Psi_n)$:

1. We prove that $g(\Psi_n) = \delta^{-}$ under a certain condition
2. We show the condition "almost always" holds in a certain sense

Maximum Gap of (Inverse) Cyclotomic Polynomials

by

Mary Elizabeth Ambrosino

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

2017

APPROVED BY:

Erich Kaltofen	Ricky Liu
Ernest Stitzinger	Hoon Hong Chair of Advisory Committee

BIOGRAPHY

Mary Ambrosino was born and raised in New Jersey. She is the daughter of two supportive parents and sister of four loving older siblings. In 2008, she began her undergraduate education at The College of New Jersey, where she explored many interests including mathematics, chemistry and computer science. After attending two summer research programs and due to the encouragement of faculty members at TCNJ, she decided to pursue a graduate degree in mathematics. In 2012, she joined the graduate program in the mathematics department at NC State University. She has worked under the direction of Dr. Hoon Hong since the summer of 2013.

ACKNOWLEDGEMENTS

I would like to thank the following people:

My advisor, Dr. Hoon Hong, for your patience, encouragement, support and motivation. You have taught me many valuable lessons for which I am so grateful, including how to fight myself and my natural tendencies so that I can become a superwoman. I will always remember your advice, and I will continue to strive to be courageous, patient and humble.

My committee members, Dr. Ricky Liu, Dr. Erich Kaltofen, Dr. Ernie Stitzinger and Dr. Charles Smith, for your feedback and encouragement.

Dr. Eunjeong Lee, for your valuable collaboration and contributions, as well as your enthusiastic feedback and support.

The mathematics department at The College of New Jersey, in particular Dr. Carlos Alves. Thank you for believing in me and inspiring me to pursue this passion. Your continued guidance and support has meant so much to me.

My friends inside and outside the math department. Thank you for the laughs, good beers, and great food we've shared these past few years.

Christopher Leonetti, for your love and support, for believing in me and inspiring me to be the best I can be. For being there through highs and lows both on my emotional journey of graduate school and on our many physical journeys on the trail.

My parents, siblings and family for the unwavering support and unconditional love you've given me. I am so lucky to have all of you in my life. Thank you for always being there for me and believing in me. Your encouragement has been so important and I owe this great accomplishment to you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

In this dissertation we study the cyclotomic and inverse cyclotomic polynomial. The cyclotomic polynomial Φ_n is the monic polynomial whose zeroes are the n-th primitive roots of unity and the inverse cyclotomic polynomial Ψ_n is the monic polynomial whose zeroes are the n-th *non*-primitive roots of unity. Some examples of each are given below

$$\begin{aligned}
\Phi_1(x) &= -1+x & \Psi_1(x) &= 1\\
\Phi_2(x) &= 1+x & \Psi_2(x) &= -1+x\\
\Phi_3(x) &= 1+x+x^2 & \Psi_3(x) &= -1+x\\
\Phi_4(x) &= 1+x^2 & \Psi_4(x) &= -1+x^2\\
\Phi_5(x) &= 1+x+x^2+x^3+x^4 & \Psi_5(x) &= -1+x\\
\Phi_6(x) &= 1-x+x^2 & \Psi_6(x) &= -1-x+x^3+x^4\\
\Phi_7(x) &= 1+x+x^2+x^3+x^4+x^5+x^6 & \Psi_7(x) &= -1+x\\
\Phi_8(x) &= 1+x^4 & \Psi_8(x) &= -1+x^4\\
\Phi_9(x) &= 1+x^3+x^6 & \Psi_9(x) &= -1+x^3
\end{aligned}$$

The cyclotomic polynomials are a fundamental family of objects in number theory and

their properties and applications have long been studied. The inverse cyclotomic polynomials are relatively newer objects, but there have also been several recent studies on them. They have numerous applications in number theory, abstract algebra, and cryptography. The cyclotomic polynomial is used to prove many important theorems: a special case of Dirichlet's theorem on primes in arithmetic progressions [21], Wedderburn's Theorem that every finite division ring is a field [30] and the constructibility of regular n-gons [26], among others. The polynomials also have numerous applications in cryptography; in particular, they are used to construct certain cryptosystems [29, 35] and to study the efficiency of a certain class of cryptosystems [22].

Thus the cyclotomic and inverse cyclotomic polynomials are important objects and it is beneficial to further our understanding of them. Many of their properties have been studied previously, such as the maximum value of their coefficients and the number of nonzero terms [3, 4, 7, 8, 9, 10, 13, 14, 16, 17, 18, 19, 20, 25, 28, 33, 36]. In [23], a study was initiated on the size of their maximum gap, that is, the largest difference between consecutive exponents in the polynomials, denoted $g(\Phi_n)$ and $g(\Psi_n)$. In this dissertation, we continue that investigation and contribute some new results.

In Chapter 2, we review the basic properties and structures of the cyclotomic and inverse cyclotomic polynomials. We discuss some fundamental results, as well as more recent and relevant theorems on their structure and size of their maximum gap.

In Chapter 3, we present several lower bounds for the size of the maximum gap of the two polynomials. These expressions were discovered by carefully inspecting and finding patterns among the size of the maximum gap of many cyclotomic and inverse cyclotomic polynomials. Suppose that one of the maximum gaps in Φ_n or Ψ_n occurs between x^l and x^u (disregarding coefficients). We observed that very often u is a divisor of n and l is the signed sum of divisors of n. The first four bounds presented in this chapter, $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$ and δ^{-}, were constructed by generalizing u and l based off the indices of the divisors of n that appeared in them. Here the "+" refers to lower bounds for the cyclotomic polynomial and the "$-$" refers to those for

the inverse cyclotomic polynomial. We observe that they are simple to compute and very often equal to the size of the maximum gap. We generalize these four formulas into another lower bound, $\varepsilon^{\pm}$, which captures these and many more gap sizes, many of which are equal to the size of the maximum gap. The complexity of $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$, δ^{-} and $\varepsilon^{\pm}$ is analyzed; we compare their complexity to that of the fastest known algorithm for computing the cyclotomic and inverse cyclotomic polynomial. We also analyze the complexity of $\tilde{\varepsilon}^{\pm}$, another lower bound which we conjecture to capture the same gap sizes as $\varepsilon^{\pm}$, but is simpler to compute.

In Chapter 4, we conjecture an exact expression for $g(\Phi_n)$ under a certain condition. Let $n = mp$, where m is a product of odd primes and p is an odd prime. We conjecture that $g(\Phi_{mp}) = \varphi(m)$ if and only if $p > m$. We present an algorithm which we use to check the conjecture for infinitely many values of mp. This algorithm is based off a structure result found in [1]. It allows us to show that $g(\Phi_{mp})$ only depends on m and $\text{rem}(p, m)$. Thus given m, we only need to check finitely many values of p in order to check the conjecture for infinitely many p. We use this algorithm to verify the conjecture for $m < 1000$. We then prove the conjecture when $m = p_1p_2$ and $p = p_3$ where $p_3 \equiv_{p_1p_2} +1$ and $p_2 \equiv_{p_1} \pm 1$. This result is proved using another structure result found in [1] which allows us to perform a detailed analysis of the gap structure of $\Phi_{p_1p_2p_3}$.

In Chapter 5, we provide a sufficient condition that $g(\Psi_n)$ is equal to δ^{-}, one of the lower bounds presented in Chapter 3. We show that given k, the number of prime factors of n, the condition "almost always" holds in a certain sense when the first (smallest) prime factor of n is fixed.

Chapter 2

Review

In this chapter, we will review the definition and various properties of the cyclotomic and inverse cyclotomic polynomial.

2.1 Cyclotomic Polynomial

Given n, a positive integer, the roots of the polynomial $x^n - 1$ are of the form $e^{2\pi i \frac{k}{n}}$, where $1 \leq k \leq n$. Thus we have the following equation

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

The roots $\left\{ e^{2\pi i \frac{1}{n}}, \ldots, e^{2\pi i \frac{n}{n}} \right\}$ are called the n-th roots of unity. A root of unity is called primitive if it is of the form $e^{2\pi i \frac{k}{n}}$ where k is coprime to n, that is, $\gcd(k, n) = 1$.

Example 2.1. *The first few n-th roots of unity and n-th primitive roots of unity are given below.*

n	$n-th$ *roots of unity*	$n-th$ *primitive roots of unity*
1	$\left\{e^{2\pi i\frac{1}{1}}\right\} = \{1\}$	$\{1\}$
2	$\left\{e^{2\pi i\frac{1}{2}}, e^{2\pi i\frac{2}{2}}\right\}$	$\left\{e^{2\pi i\frac{1}{2}}\right\} = \{-1\}$
3	$\left\{e^{2\pi i\frac{1}{3}}, e^{2\pi i\frac{2}{3}}, e^{2\pi i\frac{3}{3}}\right\}$	$\left\{e^{2\pi i\frac{1}{3}}, e^{2\pi i\frac{2}{3}}\right\}$
4	$\left\{e^{2\pi i\frac{1}{4}}, e^{2\pi i\frac{2}{4}}, e^{2\pi i\frac{3}{4}}, e^{2\pi i\frac{4}{4}}\right\}$	$\left\{e^{2\pi i\frac{1}{4}}, e^{2\pi i\frac{3}{4}}\right\} = \{i, -i\}$
5	$\left\{e^{2\pi i\frac{1}{5}}, e^{2\pi i\frac{2}{5}}, e^{2\pi i\frac{3}{5}}, e^{2\pi i\frac{4}{5}}, e^{2\pi i\frac{5}{5}}\right\}$	$\left\{e^{2\pi i\frac{1}{5}}, e^{2\pi i\frac{2}{5}}, e^{2\pi i\frac{3}{5}}, e^{2\pi i\frac{4}{5}}\right\}$

Definition 2.1 (Cyclotomic Polynomial)**.** *The n-th cyclotomic polynomial* Φ_n *is the polynomial whose zeroes are the n-th primitive roots of unity.*

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

Example 2.2. *The first few cyclotomic polynomials are given below*

$$\begin{aligned}
\Phi_1 &= x - e^{2\pi i} && = -1 + x \\
\Phi_2 &= x - e^{2\pi i\frac{1}{2}} = x - (-1) && = 1 + x \\
\Phi_3 &= \left(x - e^{2\pi i\frac{1}{3}}\right)\left(x - e^{2\pi i\frac{2}{3}}\right) = \left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right) && = 1 + x + x^2 \\
\Phi_4 &= \left(x - e^{2\pi i\frac{1}{4}}\right)\left(x - e^{2\pi i\frac{3}{4}}\right) = (x - i)(x + i) && = 1 + x^2 \\
\Phi_5 &= \left(x - e^{2\pi i\frac{1}{5}}\right)\left(x - e^{2\pi i\frac{2}{5}}\right)\left(x - e^{2\pi i\frac{3}{5}}\right)\left(x - e^{2\pi i\frac{4}{5}}\right) && = 1 + x + x^2 + x^3 + x^4
\end{aligned}$$

We observe that the above examples of the cyclotomic polynomial are all monic and have integer coefficients. In general, this is true. It may also seem that all cyclotomic polynomials have coefficients that are either $-1, 0$, or 1. However, in general this is not true. The smallest n whose cyclotomic polynomial has a coefficient not in $\{-1, 0, 1\}$ is 105, and was discovered in 1883 by Migotti [31]. It is interesting to note that 105 is also the smallest number that is the

product of three odd primes.

Example 2.3.

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

Observe that the coefficient of x^7 and x^{41} in Φ_{105} is -2.

We recall some basic functions from number theory, Euler's totient function and the Möbius function. These functions and some results using them are useful for proving many properties of the cyclotomic polynomial.

Definition 2.2 (Euler's totient function)**.** *Let $\varphi(n)$ be the number of positive integers less than or equal to n that are relatively prime to n.*

Remark 2.1. *From the definition of Φ_n and $\varphi(n)$ we see that* $\deg(\Phi_n) = \varphi(n)$.

Example 2.4. *A few examples of Euler's totient function are given below.*

$$\begin{aligned}\varphi(1) &= 1, \quad \varphi(2) &= 2 \\ \varphi(6) &= 2, \quad \varphi(10) &= 4\end{aligned}$$

Lemma 2.1. *Let m, n be integers. We have*

1. $n = \sum_{d|n} \varphi(d)$
2. *If* $\gcd(m, n) = 1$, *then* $\varphi(mn) = \varphi(m)\varphi(n)$
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

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

Proof. Proofs of this theorem can be found in many textbooks, including [6, 15, 34]. □

Definition 2.3 (Möbius function)**.** *We define $\mu(n)$ as follows*

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

where p_i are distinct prime numbers.

Remark 2.2. *If $\gcd(m, n) = 1$, then $\mu(mn) = \mu(m)\mu(n)$.*

Example 2.5. *The following are some examples of the Möbius function.*

$$\begin{aligned} \mu(1) &= 1, \quad \mu(2) = -1 \\ \mu(4) &= 0, \quad \mu(15) = 1 = (-1) \cdot (-1) = \mu(3) \cdot \mu(5) \end{aligned}$$

Definition 2.4. *We define the radical of a positive integer n to be the product of the distinct prime factors of n. That is,*

$$rad(n) = \prod_{\substack{p \mid n \\ p \text{ prime}}} p$$

Example 2.6. *The following are some examples of the radical.*

$$\begin{aligned} rad(3) &= 3, \quad rad(15) = 15 \\ rad(27) &= 3, \quad rad(1125) = 15 \end{aligned}$$

Corollary 2.1. *We have the following*

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

Proof. The proof for $n = 1$ is obvious. Suppose that $n > 1$. Let $P = \text{rad}(n)$. Any divisor d of n that does not divide P is not square free, so $\mu(d) = 0$. Thus

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

Let p be any prime that divides P. Then

$$\sum_{d|P} \mu(d) = \sum_{d|\frac{P}{p}} \mu(d) + \mu(pd) = \sum_{d|\frac{P}{p}} \mu(d) - \mu(d) = 0$$

□

Example 2.7. *The following is an example of Corollary 2.1. When $n = 12$, we see that*

$$\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) = 1 - 1 - 1 + 0 + 1 + 0 = 0$$

Theorem 2.1 (Möbius inversion formula)**.** *Let f and g be functions such that $f(n) = \prod_{d|n} g(d)$. Then $g(n) = \prod_{d|n} \left(f\left(\frac{n}{d}\right)\right)^{\mu(d)}$.*

Proof. We have

$$\prod_{d|n} \left(f\left(\frac{n}{d}\right)\right)^{\mu(d)} = \prod_{d|n} \left(\prod_{e|\frac{n}{d}} g(e)\right)^{\mu(d)}$$

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

where the last line holds by Corollary 2.1. □

We will now use the previous definitions and results to prove some basic results regarding the cyclotomic polynomial.

Theorem 2.2. *We have*

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

Proof. Consider

$$x^n - 1 = \prod_{1 \le k \le n} \left(x - e^{2\pi i \frac{k}{n}} \right) = \prod_{d|n} \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=d}} \left(x - e^{2\pi i \frac{k}{n}} \right) = \prod_{d|n} \Phi_{n/d}(x) = \prod_{d|n} \Phi_d(x)$$

□

Theorem 2.3. *We have*

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

Proof. Recall from Theorem 2.2

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

By letting $f(n) = x^n - 1$ and $g(n) = \Phi_n(x)$ in Theorem 2.1, we have

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

□

Remark 2.3. *Note that from the above theorem we easily see that*

$$\Phi_p = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p-1}$$

Example 2.8. *The following is an example of Theorem 2.3.*

$$\Phi_{12}(x) = x^4 - x^2 + 1$$

$$\begin{aligned}\prod_{d|12} \left(x^d - 1\right)^{\mu(12/d)} &= (x^1 - 1)^{\mu(12)}(x^2 - 1)^{\mu(6)}(x^3 - 1)^{\mu(4)}(x^4 - 1)^{\mu(3)}(x^6 - 1)^{\mu(2)}(x^{12} - 1)^{\mu(1)} \\ &= (x^2 - 1)^1(x^4 - 1)^{-1}(x^6 - 1)^{-1}(x^{12} - 1)^1 \\ &= x^4 - x^2 + 1\end{aligned}$$

Theorem 2.4. $\Phi_n \in \mathbb{Z}[x]$ *and is monic.*

Proof. We will prove this by induction on n. When $n = 1$, clearly $\Phi_n = x - 1$. Assume $\Phi_d \in \mathbb{Z}[x]$ and is monic for all $d < n$. Recall that

$$x^n - 1 = \Phi_n \cdot \prod_{\substack{d|n \\ d<n}} \Phi_d$$

From the induction hypothesis, $\prod_{\substack{d|n \\ d<n}} \Phi_d \in \mathbb{Z}[x]$ and is monic. From the definition of Φ_n, we see that it is monic. Thus $\Phi_n \in \mathbb{Q}[x]$ and is monic. Since $x^n - 1 \in \mathbb{Z}[x]$, we have that $\Phi_n \in \mathbb{Z}[x]$. □

Theorem 2.5. $\Phi_n(x)$ *is irreducible over* $\mathbb{Q}[x]$.

Proof. Proofs of this theorem can be found in many textbooks, including [6, 15, 34]. □

Theorem 2.6. *If $n \geq 3$ is odd, then*

$$\Phi_{2n}(x) = \Phi_n(-x)$$

Proof. We have

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

□

Theorem 2.7. *We have*

$$\Phi_n(x) = \Phi_{rad(n)}\left(x^{\frac{n}{rad(n)}}\right)$$

Proof. Consider

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

□

Example 2.9. *The following examples demonstrate Theorems 2.6 and 2.7*

1. $\Phi_3(x) = 1 + x + x^2$
2. $\Phi_6(x) = \Phi_3(-x) = 1 - x + x^2$
3. $\Phi_9(x) = \Phi_3\left(x^3\right) = 1 + x^3 + x^6$

Theorem 2.8. *Let $n \geq 2$ and $\Phi_n = \sum_{s=0}^{\varphi(n)} a_s x^s$. Then we have*

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

Proof. 1. Let α be a root of $\Phi_n(x)$. Since $\Phi_n(x) \in \mathbb{Z}[x]$ and complex roots come in conjugate pairs, $\overline{\alpha} = 1/\alpha$ is a root of $\Phi_n(x)$. Note that $x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right)$ is a polynomial in $\mathbb{Z}[x]$ with degree $\varphi(n)$ and root α. Since $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$, we have that $\Phi_n(x) = c \cdot x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right)$ for some nonzero rational number c. Note that $\Phi_n(1) = c \cdot \Phi_n(1)$ so $c = 1$ and we have that $\Phi_n(x) = x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right)$.

2. Note

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

□

Example 2.10. *Let $n = 15$. Then $\varphi(15) = 8$ and*

$$\begin{aligned}
\Phi_{15}(x) &= 1 - x + x^3 - x^4 + x^5 - x^7 + x^8 \\
x^8 \Phi_{15}\left(\frac{1}{x}\right) &= x^8 \left(x^{-8} - x^{-7} + x^{-5} - x^{-4} + x^{-3} - x^{-1} + x^0\right) \\
&= 1 - x + x^3 - x^4 + x^5 - x^7 + x^8
\end{aligned}$$

Clearly,

$$\begin{aligned}
a_0 &= a_8 = 1 & a_1 &= a_7 = -1 \\
a_2 &= a_6 = 0 & a_3 &= a_5 = 1 \\
a_4 &= -1
\end{aligned}$$

2.2 Inverse Cyclotomic Polynomial

The inverse cyclotomic polynomial has been studied more frequently in recent years. While the n-th cyclotomic polynomial has the n-th primitive roots of unity as its zeroes, the inverse cyclotomic polynomial has the n-th non-primitive roots of unity as its zeroes.

Definition 2.5 (Inverse cyclotomic polynomial)**.** *The n-th inverse cyclotomic polynomial Ψ_n is the polynomial whose zeroes are the n-th non-primitive roots of unity.*

$$\Psi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n) \neq 1}} \left(x - e^{2\pi i \frac{k}{n}}\right)$$

Remark 2.4. *The inverse cyclotomic polynomial is not the actually inverse of the cyclotomic*

polynomial; rather, it would be more precise to call it the multiplicative inverse, since we have the following relation

$$x^n - 1 = \Phi_n(x) \cdot \Psi_n(x)$$

Example 2.11. *The first few inverse cyclotomic polynomials are given below*

$$\begin{aligned}
\Psi_1(x) &= \frac{x-1}{x-1} &&= 1 \\
\Psi_2(x) = \left(x - e^{2\pi i \frac{2}{2}}\right) &= \frac{x^2-1}{x+1} &&= -1 + x \\
\Psi_3(x) = \left(x - e^{2\pi i \frac{3}{3}}\right) &= \frac{x^3-1}{x^2+x+1} &&= -1 + x \\
\Psi_4(x) = \left(x - e^{2\pi i \frac{2}{4}}\right)\left(x - e^{2\pi i \frac{4}{4}}\right) &= \frac{x^4-1}{x^2+1} &&= -1 + x^2 \\
\Psi_5(x) = \left(x - e^{2\pi i \frac{5}{5}}\right) &= \frac{x^5-1}{x^4+x^3+x^2+x+1} &&= -1 + x
\end{aligned}$$

We observe that the above examples of the inverse cyclotomic polynomial are all monic and have integer coefficients. In general, this is true. It shares these and several other properties with the cyclotomic polynomial.

Definition 2.6. *For consistency, we define the degree of the inverse cyclotomic polynomial to be $\psi(n)$. Note that $\varphi(n) + \psi(n) = n$. (Also note that this is different than the Dedekind psi function.)*

Theorem 2.9. *We have the following*

1. $\Psi_n(x) \in \mathbb{Z}[x]$ *and is monic*
2. $\Psi_n(x) = \prod_{\substack{d|n \\ d \neq n}} \left(x^d - 1\right)^{-\mu(n/d)}$
3. $\Psi_{2n}(x) = (1 - x^n) \cdot \Psi_n(-x)$, *if* $n \geq 3$ *is odd*
4. $\Psi_n(x) = \Psi_{rad(n)}\left(x^{\frac{n}{rad(n)}}\right)$

5. $\Psi_n(x) = -x^{\psi(n)}\Psi_n\left(\frac{1}{x}\right)$

Proof. .

1. Since $\Phi_n(x) \in \mathbb{Z}[x]$ and $x^n - 1 \in \mathbb{Z}[x]$, we have that $\Psi_n(x) \in \mathbb{Z}[x]$. By the definition of $\Psi_n(x)$ we see that it is monic.

2. $\Psi_n(x) = \dfrac{x^n-1}{\Phi_n(x)} = \dfrac{x^n-1}{\prod\limits_{d|n}\left(x^d-1\right)^{\mu(n/d)}} = \prod\limits_{\substack{d|n \\ d\neq n}}\left(x^d-1\right)^{-\mu(n/d)}$

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

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

5. $\Psi_n(x) = \dfrac{x^n-1}{\Phi_n(x)} = \dfrac{x^n-1}{x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right)} = -x^n\dfrac{\left(\frac{1}{x}\right)^n-1}{x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right)} = -x^{\psi(n)}\dfrac{\left(\frac{1}{x}\right)^n-1}{\Phi_n\left(\frac{1}{x}\right)} = -x^{\psi(n)}\Psi_n\left(\frac{1}{x}\right)$

□

Note that unlike the cyclotomic polynomial, the inverse cyclotomic polynomial is not irreducible in $\mathbb{Q}[x]$. In fact, if n is not prime then $\Psi_n(x)$ is reducible, as we see in the next theorem.

Theorem 2.10. *We have*

$$\Psi_n(x) = \prod_{\substack{d|n \\ d\neq n}}\Phi_d(x)$$

Proof. By Theorem 2.2 we have

$$\Psi_n(x) = \frac{x^n-1}{\Phi_n(x)} = \frac{\prod_{d|n}\Phi_d(x)}{\Phi_n(x)} = \prod_{\substack{d|n \\ d\neq n}}\Phi_d(x)$$

□

2.3 Structure of (Inverse) Cyclotomic Polynomial

Currently, there are no explicit non-recursive formulas to compute Φ_n or Ψ_n. In this section, we review some well known results and formulas about the the structure of the cyclotomic and inverse cyclotomic polynomials.

Proposition 2.1. *Let p be prime. We have*

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$$

Proof. See Remark 2.3 in Section 2.1. □

Proposition 2.2. *Let p be prime. We have*

$$\Psi_p(x) = -1 + x$$

Proof. We have

$$\Psi_p(x) = \frac{x^p - 1}{\Phi_p(x)} = \frac{x^p - 1}{1 + x + x^2 + \cdots + x^{p-1}} = -1 + x$$

□

The first nontrivial case of the cyclotomic polynomial is when n is the product of two distinct odd primes. The following theorem can be found in [12].

Theorem 2.11. *We have*

$$\Phi_{p_1p_2}(x) = \left(\sum_{i=0}^{r} x^{ip}\right)\left(\sum_{j=0}^{s} x^{jq}\right) - \left(\sum_{i=r+1}^{q-1} x^{ip}\right)\left(\sum_{j=s+1}^{p-1} x^{jq}\right) x^{-pq}$$

where p and q are distinct primes, and $(p-1)(q-1) = rp + sq$, where r and s are non-negative integers. Moreover, if $\Phi_{pq}(x) = \sum_{k=0}^{\varphi(pq)} a_k x^k$, then for any $0 \le k \le (p-1)(q-1)$ we have

1. $a_k = 1$ *if and only if* $k = ip + jq$ *for some* $0 \leq i \leq r$ *and* $0 \leq j \leq s$

2. $a_k = -1$ *if and only if* $k + pq = ip + jq$ *for some* $r + 1 \leq i \leq q - 1$ *and* $s + 1 \leq j \leq p - 1$

3. $a_k = 0$ *otherwise.*

Proof. Let

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

We will show that $f(x) = \Phi_{pq}(x)$ by showing

1. $f(x)$ is monic

2. $f(x)$ has degree $\varphi(pq)$

3. $f(\zeta) = 0$ where ζ is a primitive $pq-$th root of unity

First note that the first and second products in $f(x)$ are both monic, so $f(x)$ is monic, proving (1). The degree of the first product is

$$rp + sq = (p - 1)(q - 1) = \varphi(pq)$$

The degree of the second product is

$$(q - 1)p + (p - 1)q - pq = (p - 1)(q - 1) - 1 = \varphi(pq) - 1$$

Thus the degree of $f(x)$ is $\varphi(pq)$, proving (2). Let ζ be a primitive $pq-$th root of unity. Then

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

This implies

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

Hence

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

Since $\zeta^{pq}=1$, we have that ζ is a zero of $f(x)$, proving (3).

To prove the second statement of the theorem, we will show that the monomial terms in each of the two products in $f(x)$ are respectively different. Suppose not, so there exist $i_1, i_2 \in [0, q-1]$ and $j_1, j_2 \in [0, p-1]$ such that

$$i_1p + j_1q = i_2p + j_2q \quad \text{or} \quad i_1p + j_1q = i_2p + j_2q - pq$$

Then $q|(i_1 - i_2)$, so $i_1 = i_2$. Similarly, $j_1 = j_2$. □

Proposition 2.3. *We have*

$$\Psi_{pq}(x) = -\left(1 + x + \cdots + x^{p-1}\right) + \left(x^q + x^{q+1} + \cdots + x^{q+p-1}\right)$$

Proof. Note that by Theorem 2.10

$$\begin{aligned}\Psi_{pq}(x) &= \Phi_1(x)\cdot\Phi_p(x)\cdot\Phi_q(x)\\ &= (x-1)\left(1 + x + \cdots + x^{p-1}\right)\left(1 + x + \cdots + x^{q-1}\right)\\ &= \left(1 + x + \cdots + x^{p-1}\right)(-1 + x^q)\\ &= -\left(1 + x + \cdots + x^{p-1}\right) + \left(x^q + x^{q+1} + \cdots + x^{q+p-1}\right)\end{aligned}$$

□

The first nontrivial case of the inverse cyclotomic polynomial is when n is the product of three distinct odd primes. Currently, there are no explicit non-recursive formulas.

In [1], the structure of Φ_n was studied extensively. Many results were presented, including

the following two theorems. Their proofs can be found in [1].

Theorem 2.12. *Let m be odd square-free, and p prime. Let $q = \mathrm{quo}\,(p, m)$ and $r = \mathrm{rem}\,(p, m)$. Let*

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

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

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

(C1) $f_{m,p,i,0} = \cdots = f_{m,p,i,q-1}$

(C2) $f_{m,p,i,q} = \mathrm{rem}\,(f_{m,p,i,0}, x^r)$

(C3) $f_{m,p,i,0} = f_{m,p',i,0}$ *if* $p \equiv_m p'$

Theorem 2.13 (Structure Theorem)**.** *Let $p_3 \equiv_{p_1 p_2} +1$ and $p_2 \equiv_{p_1} \pm 1$. We have*

$$\Phi_n(x) = \sum_{a=0}^{\varphi(p_1 p_2)-1} f_a(x)\, x^{a p_3} \qquad \deg f_a < p_3$$

$$f_a(x) = \sum_{b=0}^{q_3} f_{a,b}(x)\, x^{b p_1 p_2} \qquad \deg f_{a,b} < p_1 p_2$$

$$f_{a,0}\,(x) = \cdots = f_{a,q_3-1}\,(x)$$

$$= \begin{cases} +A(x) & & -x^{p_2} A(x) & & \text{if } a = 0 \\ +B(x) & -x^{(u+1)p_2 - a} & -x^{p_2} B(x) & +x^{p_1 p_2 - a} & \text{if } a > 0,\ w \leq u \text{ and } \neg\mathcal{D}(a) \\ +C(x) & & -x^{p_2} B(x) & +x^{p_1 p_2 - a} & \text{if } a > 0,\ w \leq u \text{ and } \mathcal{D}(a) \\ -D(x) & -x^{(u+1)p_2 - a} & +x^{p_2} D(x) & +x^{p_1 p_2 - a} & \text{if } a > 0,\ w > u \text{ and } \neg\mathcal{D}(a) \\ -x^{(u+1)p_2 - a} & -D(x) & +x^{p_2} D(x) & +x^{p_1 p_2 - a} & \text{if } a > 0,\ w > u \text{ and } \mathcal{D}(a) \end{cases}$$

$$f_{a,q_3}\,(x) = \begin{cases} 1 & \text{if } a = 0 \\ 0 & \text{if } a > 0 \end{cases}$$

where

$$A(x) = \sum_{k=0}^{p_1-1} x^k, \qquad B(x) = \sum_{k=u+1-w}^{p_1-1-w} x^k, \qquad C(x) = \sum_{k=u+1-w}^{p_1-2-w} x^k, \qquad D(x) = \sum_{k=p_1-w}^{p_1+u-w} x^k$$

$$\begin{aligned}
u &:= \operatorname{quo}(a, \overline{p_2}) \\
v &:= \operatorname{quo}(\operatorname{rem}(a, \overline{p_2}), p_1) \\
w &:= \operatorname{rem}(\operatorname{rem}(a, \overline{p_2}), p_1) \\
q_3 &:= \operatorname{quo}(p_3, p_1 p_2) \\
\overline{p_2} &:= \begin{cases} p_2 - 1 & \text{if } p_2 \equiv_{p_1} +1 \\ p_2 & \text{if } p_2 \equiv_{p_1} -1 \end{cases} \\
\mathcal{D}(a) &:\Leftrightarrow p_2 \equiv_{p_1} -1 \ \wedge \ v = q_2
\end{aligned}$$

2.4 Size of Maximum Gap

In this section we introduce the notion of the size of the maximum gap of a polynomial, and in particular of the cyclotomic and inverse cyclotomic polynomial. We review the trivial cases and previous results.

Definition 2.7 (Size of maximum gap)**.** *Let $f(x) = \sum_{i=1}^{t} c_t x^{e_t}$ where $c_i \neq 0$ and $e_1 < \cdots < e_t$. The size of the maximum gap, written as $g(f)$, is given by*

$$g(f) = \max_{1 \leq i < t} (e_{i+1} - e_i), \qquad g(f) = 0 \text{ when } t = 1$$

Example 2.12. *We give some examples of the size of the maximum gap.*

1. *Let $f_1(x) = 1 + x + x^3 - x^5 + 2x^6$. Then $g(f_1) = 2$ since 2 is the maximum amongst*

$1-0$, $3-1$, $5-3$, $6-5$.

2. *Let* $f_2(x) = -x + x^3 + 5x^{15} - 3x^{20} + x^{21}$. *Then* $g(f_2) = 12$ *since* 12 *is the maximum amongst* $3-1$, $15-3$, $20-5$, $21-20$.

Remark 2.5. *Note that we use the phrase "size of maximum gap" to refer to the maximum difference between exponents that appear in a polynomial. We may also use the phrase "gap" to refer to any gap between exponents that appear, and "maximum gap" to refer to the largest of all such gaps. For example, there is a gap between* $-x^5$ *and* $2x^6$ *in* $f_1(x)$ *above, and the maximum gap occurs between* x *and* x^3, *and* x^3 *and* $-x^5$. *Note that where the maximum gap occurs may not be unique in a polynomial, but the size of the maximum gap is unique.*

We now consider the size of the maximum gap in terms of the cyclotomic and inverse cyclotomic polynomial.

Proposition 2.4. *We have*

1. $g(\Phi_n) = \dfrac{n}{rad(n)} g\left(\Phi_{rad(n)}\right)$
2. $g(\Psi_n) = \dfrac{n}{rad(n)} g\left(\Psi_{rad(n)}\right)$
3. $g(\Phi_{2n}) = g(\Phi_n)$, *where* $n \geq 3$ *is odd*
4. $g(\Psi_{2n}) = \max\{\varphi(n),\, g(\Psi_n)\}$, *where* $n \geq 3$ *is odd*

Proof. Note

1. By Theorem 2.7, we have that $\Phi_n(x) = \Phi_{\mathrm{rad}(n)}\left(x^{\frac{n}{\mathrm{rad}(n)}}\right)$. Thus $g(\Phi_n) = \frac{n}{\mathrm{rad}(n)} g\left(\Phi_{\mathrm{rad}(n)}\right)$.
2. By Theorem 2.9, we have that $\Psi_n(x) = \Psi_{\mathrm{rad}(n)}\left(x^{\frac{n}{\mathrm{rad}(n)}}\right)$. Thus $g(\Psi_n) = \frac{n}{\mathrm{rad}(n)} g\left(\Psi_{\mathrm{rad}(n)}\right)$.
3. By Theorem 2.6, we have that $\Phi_{2n}(x) = \Phi_n(-x)$. Thus $g(\Phi_{2n}) = g(\Phi_n)$.
4. By Theorem 2.9, we have that $\Psi_{2n}(x) = (1-x^n)\cdot\Psi_n$. Thus $g(\Psi_{2n}) = \max\{\varphi(n),\, g(\Psi_n)\}$.

□

Therefore, without losing generality, from now on we will only study the size of the maximum gap of the cyclotomic and inverse cyclotomic polynomial where n is odd and square-free.

Proposition 2.5. *Let p, q, and r be distinct odd primes. Then we have that*

1. $g(\Phi_1) = 1$
2. $g(\Psi_1) = 0$
3. $g(\Phi_p) = 1$
4. $g(\Psi_p) = 1$
5. $g(\Phi_{pq}) = p - 1$
6. $g(\Psi_{pq}) = q - p + 1$
7. $g(\Psi_{pqr}) = 2qr - \psi(pqr)$ *"almost always", where $p < q < r$.*

Proof. Note that (1), (2), (3), (4), (6) are trivial. (5) was first proved in [23]. Additional proofs can be found in [11, 32, 37]. (7) was proved in [23], and a more precise notion of "almost always" is given there. □

The original motivation for studying the size of the maximum gap of the cyclotomic and inverse cyclotomic polynomial came from elliptic curve cryptography; the computing time of the Ate_i pairing over elliptic curves depends on the maximum gap of the inverse cyclotomic polynomials whose degree are decided from the parameter of the elliptic curves [24, 27, 36, 38]. However the problem of finding the maximum gap is interesting on its own and its study can be viewed as a first step toward the detailed understanding of the sparsity structure of Φ_n and Ψ_n.

2.5 Time Complexities

In this section, we review the bit time complexities for some relevant computations. We use the big O notation which we define as follows

Definition 2.8 (Big O Notation)**.** *Let $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ be functions defined on real numbers. Then we have $f(x_1, \ldots, x_n) = O\left(g(x_1, \ldots, x_n)\right)$ if and only if*

$$\exists M > 0,\, N > 0 \;\; \forall (x_1, \ldots, x_n) \quad \left(\exists i \; x_i \geq N \;\Rightarrow\; |f(x_1, \ldots, x_n)| \;\leq\; M\, |g(x_1, \ldots, x_n)| \;\right)$$

We present the bit time complexities of some common operations using big O notation:

1. Multiplying two numbers of length L_1, L_2: $O(L_1 L_2)$
2. Adding two numbers of length L_1, L_2: $O(\max\{L_1,\, L_2\})$
3. Adding s numbers with length L: $O(sL + s^2)$. See Lemma 2.2 which follows for the proof.
4. Taking the maximum of two numbers of length L_1, L_2: $O(\max\{L_1,\, L_2\})$
5. Factoring a number with length L (using the General Number Field Sieve [5]):
   $O\left(\exp \sqrt[3]{\left(\frac{64}{9} + o(1)\right) L(\log L)^2}\right)$

We prove the claim in (3) above. Let $L(a)$ be the length of a. As a worst case scenario, let us assume

$$L(a_1) = \cdots = L(a_s) = \max\{L(a_1),\, \ldots,\, L(a_s)\} = L$$

for integers $\{a_1,\, \ldots,\, a_s\}$.

Lemma 2.2. *We have*

1. $L(a_1 + \cdots + a_s) \leq L + s - 1$

2. $T_+(s, L) = O\left(sL + s^2\right)$

for integers $\{a_1, \ldots, a_s\}$ *and where* $T_+(s, L)$ *is the time required to add* s *numbers, the largest of which is length* L*.*

Proof. We prove the first claim by induction on $s \geq 2$. First note

$$L(a_1 + a_2) \leq \max\{L(a_1),\, L(a_2)\} + 1 = L + 1$$

Now assume the claim is true for s, that is,

$$L(a_1 + \cdots + a_s) \leq L + s - 1$$

We want to show this is true for $s + 1$.

$$\begin{aligned} L(a_1 + \cdots + a_{s+1}) &= L\left((a_1 + \cdots + a_s) + a_{s+1}\right) \\ &\leq \max\{L(a_1 + \cdots + a_s),\, L(a_{s+1})\} + 1 \end{aligned}$$

By the induction hypothesis, we have

$$L(a_1 + \cdots + a_s) \leq L + s - 1$$

Therefore,

$$\begin{aligned} L(a_1 + \cdots + a_{s+1}) &\leq \max\{L(a_1 + \cdots + a_s),\, L(a_{s+1})\} + 1 \\ &\leq \max\{L + s - 1,\, L\} + 1 \\ &= L + s \end{aligned}$$

which proves the claim.

We prove the second claim by first showing the following

$$T_+(s,L) = O\left((s-1)L + \binom{s-1}{2}\right)$$

for all $s \geq 2$. We will prove this by induction on s. First note

$$T_+(2,L) = O(L)$$
$$(2-1)L + \binom{2-1}{2} = L$$

Assume true for s, so that

$$T_+(s,L) = O\left((s-1)L + \binom{s-1}{2}\right) \tag{2.1}$$

We want to show this is true for $s+1$. Note that since $a_1 + \cdots + a_{s+1} = (a_1 + \cdots + a_s) + a_{s+1}$, we have

$$T_+(s+1,L) = T_+(s,L) + T_+(2, L+s-1) \tag{2.2}$$

Note that

$$T_+(2, L+s-1) = O(L+s-1) \tag{2.3}$$

Combining (2.1), (2.2) and (2.3), we get that

$$T_+(s+1,L) = O\left(sL + \binom{s-1}{2} + \binom{s-1}{1}\right)$$
$$T_+(s+1,L) = O\left(sL + \binom{s}{2}\right)$$

which proves the claim. Therefore,

$$T_+(s+1,L) = O\left(sL + \binom{s}{2}\right)$$

$$T_+(s+1, L) = O\left(sL + s^2\right)$$

□

We consider the time complexity of computing Φ_n and Ψ_n. In [2] the fastest known algorithms for computing the polynomials were given. In Section 5 of that paper, the authors state that the number of computations in $\mathbb{Z}$ required to compute Φ_n and Ψ_n is $O\left(2^{\omega(n)}\varphi(n)\right)$ and $O\left(2^{\omega(n)}\psi(n)\right)$, respectively. Note that this does not take into consideration the bit lengths of the intermediate integers. Thus, if they are taken into consideration, the time complexity could be larger. Let k be the number of prime factors of n and L be the length of the largest prime factor of n. Note that $\varphi(n) < 2^{kL}$. Assume, though unrealistic, that the bit length of all intermediate integers remains L. Then we have that the time complexity of computing Φ_n, $T_\Phi(k, L)$, is

$$\begin{aligned}
T_\Phi(k, L) &= O\left(2^k 2^{kL} L^2\right) \\
T_\Phi(k, L) &= O\left(2^{k(L+1)} L^2\right) \\
T_\Phi(k, L) &= O\left(2^{k(L+1)+\nu L}\right) \\
T_\Phi(k, L) &= O\left(2^{k(L+1)+\nu(L+1)}\right) \\
T_\Phi(k, L) &= O\left(2^{(k+\nu)(L+1)}\right)
\end{aligned}$$

where $\nu > 0$ is an arbitrarily small number. Similarly, the time complexity of computing Ψ_n is $O\left(2^{(k+\nu)(L+1)}\right)$. Of course, this is an optimistic estimate, as the length of the intermediate integers will be larger than L.

Chapter 3

Lower Bounds

In this chapter, we present various lower bounds for the cyclotomic and inverse cyclotomic polynomial.

Introduction

Our challenge is to find general expressions for $g(\Phi_n)$ and $g(\Psi_n)$ where n is the product of an *arbitrary* number of odd primes. To understand the complexity of this problem, we consider the following graphs, where the x-axis is n odd, square-free and the y-axis is $g(\Phi_n)$ and $g(\Psi_n)$.

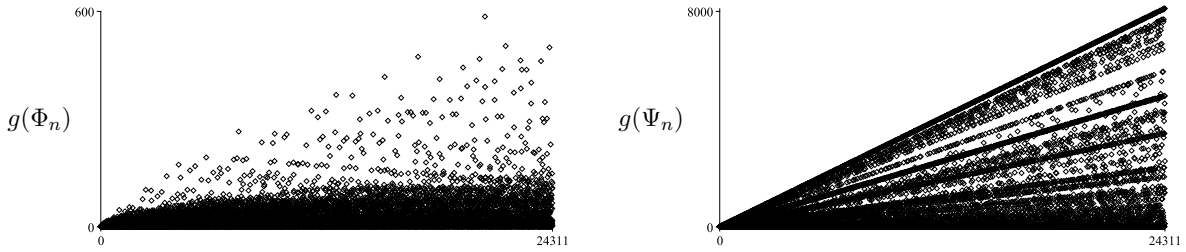


Figure 3.1 Plots of $g(\Phi_n)$ and $g(\Psi_n)$

We observe that although at first there may seem to be some patterns in the plots, in general, the size of the maximum gap does not follow any obvious universal patterns. After several years of attempts we have not yet found any general expressions, due to combinatorial blowup in the number of cases to consider. Thus, we propose to consider instead a weaker challenge: find expressions for *lower bounds* of $g(\Phi_n)$ and $g(\Psi_n)$. The weaker challenge is still useful for the original motivation from elliptic curve cryptography.

Thus, in this chapter, we tackle the weaker challenge of finding expressions for lower bounds. The main contributions (precisely stated in Section 3.1) are as follows.

1. We provide four expressions ($\alpha^{\pm}, \beta^{\pm}$, $\gamma^{\pm}$ and δ^{-}) for lower bounds (Theorems 3.1, 3.2, 3.3 and 3.4). These expressions were discovered by carefully inspecting and finding patterns among the maximum gaps of many cyclotomic and inverse cyclotomic polynomials. The four expressions are easy to compute. Furthermore, numerous computer experiments indicate that the combination (maximum) of the four expressions is *very often* exact (Section 3.3.1).

2. We abstract the four expressions into a single general expression $\varepsilon^{\pm}$ (Theorem 3.5). The general expression was discovered by observing that each of the four expressions can be rewritten as the difference of two numbers, say u and l, where u is a certain divisor of n and l is a signed sum of several other divisors of n. We also observed that there is indeed a gap between x^l and x^u in the polynomials, which led to an idea for proving the general expression. The general expression takes more time to compute, since it captures many other gaps that are not captured by the four expressions. As a result, $\varepsilon^{\pm}$ is always greater than or equal to $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$ and δ^{-}. Indeed, numerous computer experiments indicate that it is *almost always* exact (Section 3.3.2).

3. We analyze the complexity of $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$ and δ^{-}. We also analyze the complexity of $\varepsilon^{\pm}$ and $\tilde{\varepsilon}^{\pm}$, another general lower bound which we observe captures all the same gaps as $\varepsilon^{\pm}$

but is simpler to compute.

The chapter is structured as follows: In Section 3.1, we precisely state the lower bounds and the conjecture informally described above. In Section 3.2, we illustrate each bound using small examples. In Section 3.3, we report experimental findings on the quality of the bounds (how often they are exact). In Section 3.4, we prove the lower bounds. In Section 3.5, we analyze the complexity of the lower bounds.

3.1 Main Results

In this section, we precisely state the main results of this chapter. From now on, let $n = p_1 \cdots p_k$ where $p_1 < \cdots < p_k$ are odd primes. We are ready to state the four lower bounds for (inverse) cyclotomic polynomials.

Theorem 3.1 (Special bound $\alpha^{\pm}$)**.** *We have* $g(\Phi_n) \geq \alpha^+(n)$ *and* $g(\Psi_n) \geq \alpha^-(n)$ *where*

$$\alpha^{\pm}(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (p_r - \varphi(p_1 \cdots p_{r-1}))$$

Theorem 3.2 (Special bound $\beta^{\pm}$)**.** *We have* $g(\Phi_n) \geq \beta^+(n)$ *and* $g(\Psi_n) \geq \beta^-(n)$ *where*

$$\beta^{\pm}(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (\min\{p_{r+1}, p_1 \cdots p_r\} - \psi(p_1 \cdots p_r))$$

Theorem 3.3 (Special bound $\gamma^{\pm}$)**.** *We have* $g(\Phi_n) \geq \gamma^+(n)$ *and* $g(\Psi_n) \geq \gamma^-(n)$ *where*

$$\gamma^{\pm}(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(p_1 \cdots p_r - \sum_{\substack{d \mid n \\ \omega(d) < r}} \pm \mu(n/d) \; d \right)$$

Theorem 3.4 (Special bound δ^-)**.** *We have* $g(\Psi_n) \geq \delta^-(n)$ *where*

$$\delta^-(n) = 2\frac{n}{p_1} - \psi(n)$$

Now we describe a more general lower bound, which is abstracted from the above four special bounds. For this, we need a few notations.

Notation 3.1. *For a positive integer* d *and a set* B *of positive integers, let*

$$\begin{array}{rclcrcl} \overline{d} & = & \{h \,:\, d \mid h\} & & \underline{B} & = & \bigcup_{d\in B} \underline{d} \\ \underline{d} & = & \{h \,:\, h \mid d\} & & B^{\pm} & = & \{d \in B \,:\, \mu(n/d) = \pm 1\} \end{array}$$

Now are ready to state the general bound, unifying the four special bounds.

Theorem 3.5 (General bound $\varepsilon^{\pm}$)**.** *We have* $g(\Phi_n) \geq \varepsilon^+(n)$ *and* $g(\Psi_n) \geq \varepsilon^-(n)$ *where*

$$\varepsilon^{\pm}(n) = \max_{\substack{B\subseteq \underline{n}\setminus\{n\} \\ \mathcal{C}^{\pm}(B)}} \left(\min(\underline{n} \setminus \{n\} \setminus B) \;-\; \sum_{d\in B} \pm\mu(n/d)\;\; d \right)$$

where

$$\mathcal{C}^{\pm}(B) \quad \Leftrightarrow \quad \forall d \in \underline{B} \qquad \#(B^{\pm} \cap \overline{d}) \;\geq\; \#(B^{\mp} \cap \overline{d})$$

Remark 3.1. *The above four special bounds* $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$ *and* δ^- *can be obtained from the general bound* $\varepsilon^{\pm}$ *by considering only certain* B*'s:*

$\alpha^{\pm}$*:* $B = \{d : d | p_1 \cdots p_{r-1}$ *and* $\omega(d) < r\}$ *for* $1 \leq r < k$ *and* $\rho(k-r) = \mp 1$

$\beta^{\pm}$*:* $B = \{d : d | p_1 \cdots p_r$ *and* $\omega(d) < r\}$ *for* $1 \leq r < k$ *and* $\rho(k-r) = \mp 1$

$\gamma^{\pm}$*:* $B = \{d : d | p_1 \cdots p_k$ *and* $\omega(d) < r\}$ *for* $1 \leq r < k$ *and* $\rho(k-r) = \mp 1$

δ^-*:* $B = \{d : d | p_1 \cdots p_k$ *and* $\omega(d) < k$ *and* $d \neq p_2 \cdots p_k\}$

It turns out that these B's satisfy $\mathcal{C}^{\pm}(B)$.

3.2 Examples

In Table 3.1 below, we give the values of $g(\Phi_n)$, $g(\Psi_n)$ and the lower bounds on several values of n.

Table 3.1 Values of the size of the maximum gap and lower bounds on several values of n

n	$3\cdot5\cdot11\cdot13$	$3\cdot5\cdot7\cdot71$	$7\cdot11\cdot13\cdot17$	$3\cdot7\cdot11\cdot13$	$3\cdot5\cdot7\cdot11$
$g(\Phi_n)$	**3**	**14**	**210**	**17**	**10**
$\alpha^+(n)$	**3**	2	6	2	2
$\beta^+(n)$	2	**14**	6	2	2
$\gamma^+(n)$	2	2	**210**	2	2
$\varepsilon^+(n)$	**3**	**14**	**210**	**17**	2

n	$5\cdot7\cdot11\cdot13$	$7\cdot11\cdot13\cdot17$	$3\cdot5\cdot7\cdot11$	$7\cdot11\cdot13\cdot41$	$7\cdot11\cdot13$
$g(\Psi_n)$	**3**	**30**	**95**	**11**	**7**
$\alpha^-(n)$	**3**	5	3	5	6
$\beta^-(n)$	0	-4	0	4	6
$\gamma^-(n)$	0	**30**	-10	6	6
$\delta^-(n)$	-123	-635	**95**	-515	5
$\varepsilon^-(n)$	**3**	**30**	**95**	**11**	6

In the above tables, we marked the exact ones in boldface, that is, the ones that match $g(\Phi_n)$ or $g(\Psi_n)$. For the last column, we chose the smallest n such that $g(\Phi_n)$ and $g(\Psi_n)$ is not

equal to any of the lower bounds. After checking all the values of $n < 15013$, we have not found any such example for the cyclotomic case where $k = 3$.

3.2.1 Examples for special bounds

In the following, we will illustrate how the bounds $\alpha^{\pm}$, $\beta^{\pm}$, $\gamma^{\pm}$ and δ^{-} in Table 3.1 are computed for some of the examples. First we compute examples for the cyclotomic polynomial, and then examples for the inverse cyclotomic polynomial.

Example 3.1 (α^{+})**.** *Let $n = 3 \cdot 5 \cdot 11 \cdot 13$. We will compute $\alpha^{+}(n)$. Let*

$$u = p_r$$
$$l = \varphi(p_1 \cdots p_{r-1})$$

The following shows the values of $u-l$ for all choices of r such that $1 \leq r < k$ and $\rho(k-r) = -1$.

r	u	l	$u-l$
1	3	1	2
3	11	8	3

Thus $\alpha^{+}(n) = 3$.

Example 3.2 (β^{+})**.** *Let $n = 3 \cdot 5 \cdot 7 \cdot 71$. We will compute $\beta^{+}(n)$. Let*

$$u = \min\{p_{r+1}, p_1 \cdots p_r\}$$
$$l = \psi(p_1 \cdots p_r)$$

The following shows the values of $u - l$ for all choices of r such that $1 \leq r < k$ and $\rho(k-r) =$

-1.

r	u	l	$u-l$
1	3	1	2
3	71	57	14

Thus $\beta^+(n) = 14$.

Example 3.3 (γ^+)**.** *Let* $n = 7 \cdot 11 \cdot 13 \cdot 17$. *We will compute* $\gamma^+(n)$. *Let*

$$u = p_1 \cdots p_r$$

$$B = \{d \ : \ d \mid n \ \textit{and} \ \omega(d) < r\}$$

$$l = \sum_{d \in B} \mu(n/d) \ \ d$$

The following shows the values of $u - l$ *for all choices of* r *such that* $1 \leq r < k$ *and* $\rho(k-r) = -1$.

r	u	B	l	$u-l$
1	7	{1}	1	6
3	$7 \cdot 11 \cdot 13$	{1, 7, 11, 13, 17, 77, 91, 119, 143, 187, 221}	791	210

Thus $\gamma^+(n) = 210$.

Example 3.4 (α^-)**.** *Let* $n = 5 \cdot 7 \cdot 11 \cdot 13$. *We will compute* $\alpha^-(n)$. *Let*

$$u = p_r$$

$$l = \varphi(p_1 \cdots p_{r-1})$$

The following shows the values of $u - l$ *for all choices of* r *such that* $1 \leq r < k$ *and* $\rho(k-r) = +1$.

r	u	l	$u-l$
2	7	4	3

Thus $\alpha^{-}(n) = 3$.

Example 3.5 (γ^{-})**.** *Let* $n = 7 \cdot 11 \cdot 13 \cdot 17$. *We will compute* $\gamma^{-}(n)$. *Let*

$$\begin{aligned} u &= p_1 \cdots p_r \\ B &= \{d \ : \ d \mid n \ \textit{and} \ \omega(d) < r\} \\ l &= \sum_{d \in B} -\mu(n/d) \ \ d \end{aligned}$$

The following shows the values of $u - l$ *for all choices of* r *such that* $1 \leq r < k$ *and* $\rho(k - r) = +1$.

r	u	B	l	$u - l$
2	$7 \cdot 11$	{1, 7, 11, 13, 17}	47	30

Thus $\gamma^{-}(n) = 30$.

Example 3.6 (δ^{-})**.** *Let* $n = 3 \cdot 5 \cdot 7$. *We will compute* $\delta^{-}(n)$. *Note*

$$\begin{aligned} \delta^{-}(n) &= 2\frac{n}{p_1} - \psi(n) \\ &= 2\frac{3 \cdot 5 \cdot 7}{3} - (3 \cdot 5 \cdot 7 - (3-1)(5-1)(7-1)) \\ &= 13 \end{aligned}$$

Thus $\delta^{-}(n) = 13$.

3.2.2 Examples for general bound

In the following, we will illustrate how the bounds $\varepsilon^{\pm}$ in Table 3.1 are computed for some of the examples. First we compute examples for the cyclotomic polynomial, and then examples for the inverse cyclotomic polynomial.

Example 3.7 (ε^+)**.** *Let $n = 3 \cdot 7 \cdot 11 \cdot 13$. We will compute $\varepsilon^+(n)$. Let*

$$u = \min A$$
$$l = \sum_{d \in B} \mu\left(n/d\right)\ d$$

The following shows the values of $u - l$ for some A and B such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $\mathcal{C}^+(B)$. There are 1566 such pairs of A and B, so we only list a few below.

A	B	u	l	$u - l$
$\{3, 7, 11, 13, 3 \cdot 7, \ldots\}$	$\{1\}$	3	1	2
$\{11, 13, 3 \cdot 11, 3 \cdot 13, 7 \cdot 11, \ldots\}$	$\{1, 3, 7, 3 \cdot 7\}$	11	12	-1
$\{13, 3 \cdot 13, 7 \cdot 11, 7 \cdot 13, \ldots\}$	$\{1, 3, 7, 11, 3 \cdot 7, 3 \cdot 11\}$	13	34	-21
$\{7 \cdot 11, 7 \cdot 13, 11 \cdot 13, \ldots\}$	$\{1, 3, 7, 11, 13, 3 \cdot 7, 3 \cdot 11, 3 \cdot 13\}$	$7 \cdot 11$	60	17
$\ldots$	$\ldots$			

Thus $\varepsilon^+(n) = 17$.

Example 3.8 (ε^-)**.** *Let $n = 7 \cdot 11 \cdot 13 \cdot 41$. We will compute $\varepsilon^-(n)$. Let*

$$u = \min A$$
$$l = \sum_{d \in B} -\mu\left(n/d\right)\ d$$

The following shows the values of $u - l$ for some A and B such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$,

and $\mathcal{C}^-(B)$. There are 13301 such pairs of A and B, so we only list a few below.

A	B	u	l	$u-l$
$\{11, 13, 41, 7\cdot 11, 7\cdot 13, \ldots\}$	$\{1, 7\}$	11	6	5
$\{1, 41, 7\cdot 11, 7\cdot 13, 11\cdot 13, \ldots\}$	$\{7, 11, 13\}$	1	31	-30
$\{41, 7\cdot 11, 7\cdot 13, 11\cdot 13, \ldots\}$	$\{1, 7, 11, 13\}$	41	30	11
$\ldots$	$\ldots$			

Thus $\varepsilon^-(n) = 11$.

In the following, we explain the condition $\mathcal{C}^{\pm}(B)$. Recall that

$$\mathcal{C}^{\pm}(B) \quad \Leftrightarrow \quad \forall d \in \underline{B} \quad \#(B^{\pm} \cap \overline{d}) \;\geq\; \#(B^{\mp} \cap \overline{d})$$

In words, this condition is true if for every number d that divides some number in B, the number of multiples of d in $B^{\pm}$ is greater than or equal to the number of multiples of d in $B^{\mp}$. We also explain the condition though examples. We will consider the "+" case; the "$-$" case is analogous. Let $n = 3\cdot 5\cdot 7\cdot 11$ and $B = \{1, 3, 3\cdot 5\}$. Note that $B^+ = \{1, 3\cdot 5\}$ and $B^- = \{3\}$. We consider every element of the set $\underline{B} = \{1, 3, 5, 3\cdot 5\}$.

b	$\#\left(B^+ \cap \overline{b}\right)$	$\#\left(B^- \cap \overline{b}\right)$
1	2	1
3	1	1
5	1	0
$3\cdot 5$	1	0

Since for every choice of b, the middle column is greater than or equal to the right column, the condition $\mathcal{C}^+(B)$ is true for this choice of B.

Again let $n = 3 \cdot 5 \cdot 7 \cdot 11$ and now choose $B = \{1,\, 3,\, 7,\, 3 \cdot 5\}$. Note that $B^+ = \{1,\, 3 \cdot 5\}$ and $B^- = \{3,\, 7\}$. We consider every element of the set $\underline{B} = \{1,\, 3,\, 5,\, 7,\, 3 \cdot 5\}$

b	$\#\left(B^+ \cap \overline{b}\right)$	$\#\left(B^- \cap \overline{b}\right)$
1	2	2
3	1	1
5	1	0
7	0	1
$3 \cdot 5$	1	0

When $b = 7$, we have that the middle column is less than the right column, thus the condition $\mathcal{C}^+(B)$ is false for this choice of B.

We make the interesting observation that this condition is combinatorial, not arithmetic. That is, given the number k of prime factors of n, we can compute all sets B such that $\mathcal{C}^{\pm}(B)$ is true. For example, if we write the first set B in terms of the indices of the prime factors of n, such that $B = \{\{0\}, \{1\}, \{1, 2\}\}$ we can determine whether $\mathcal{C}^+(B)$ is true without knowing the values of the prime factors.

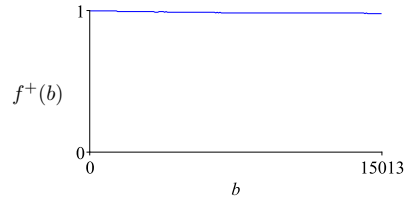
b	$\#\{c \in B^+ \mid b \subset c\}$	$\#\{c \in B^- \mid b \subset c\}$
$\{0\}$	2	1
$\{1\}$	1	1
$\{2\}$	1	0
$\{1, 2\}$	1	0

This is all to say that the condition $\mathcal{C}^{\pm}(B)$ in $\varepsilon^{\pm}(n)$ does not need to be checked for every choice of B; rather, the sets B such that $B \subsetneq \underline{n} \setminus \{n\}$ and $\mathcal{C}^{\pm}(B)$ can be predetermined given k.

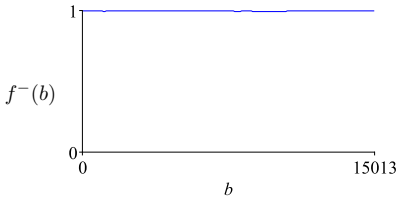
3.3 Quality

3.3.1 Quality of special bounds

The following graphs in Figure 3.2 show how often the lower bound is equal to the size of the maximum gap.



$$f^+(b) = \frac{\#\{n < b \ : \ g(\Phi_n) = \max\{\alpha^+(n),\, \beta^+(n),\, \gamma^+(n)\}\}}{\#\{n < b\}}$$



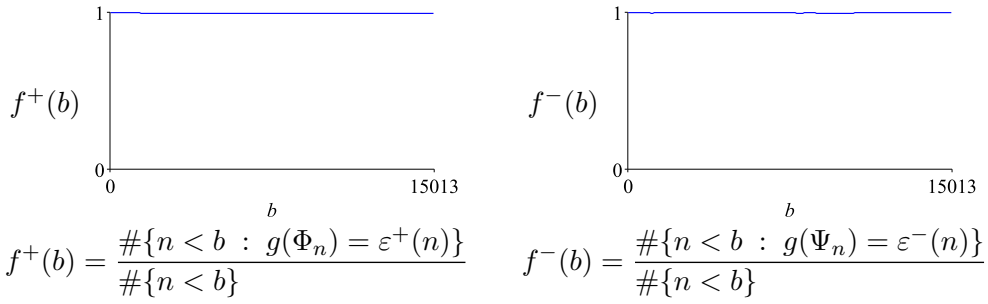
$$f^-(b) = \frac{\#\{n < b \ : \ g(\Psi_n) = \max\{\alpha^-(n),\, \beta^-(n),\, \gamma^-(n),\, \delta^-(n)\}\}}{\#\{n < b\}}$$

Figure 3.2 Plots of how often the size of the maximum gap is equal to one of the special lower bounds

In the above graphs, $f^+(15013) = 0.9829$ and $f^-(15013) = 0.9984$.

3.3.2 Quality of general bound

The following graphs in Figure 3.3 show how often the lower bound is equal to the size of the maximum gap.



$$f^+(b) = \frac{\#\{n < b \ : \ g(\Phi_n) = \varepsilon^+(n)\}}{\#\{n < b\}} \qquad f^-(b) = \frac{\#\{n < b \ : \ g(\Psi_n) = \varepsilon^-(n)\}}{\#\{n < b\}}$$

Figure 3.3 Plots of how often the size of the maximum gap is equal to the general bound

In the above graphs, $f^+(15013) = 0.9957$ and $f^-(15013) = 0.9984$.

3.4 Proof

In this section, we prove the main results (Theorems 3.1, 3.2, 3.3, 3.4 and 3.5). We will first prove the general lower bound $\varepsilon^{\pm}$ (Theorem 3.5). Then we will prove the three special lower bounds $\alpha^{\pm}$, $\beta^{\pm}$ and $\gamma^{\pm}$ (Theorems 3.1, 3.2, and 3.3) as certain restrictions of Theorem 3.5. Although δ^- (Theorem 3.4) can be proven in the same manner, we prove it in a different (simpler) manner. In order to simplify the presentation of the proof, we introduce some notations.

Notation 3.2.

$$n_r = p_1 \cdots p_r \qquad l^{\pm}(B) = \sum_{d \in B} \pm\mu\left(n/d\right) \ d$$

3.4.1 Proof of general bound

Recall

$$\varepsilon^{\pm}(n) = \max_{\substack{B \subsetneq \underline{n} \setminus \{n\} \\ \mathcal{C}^{\pm}(B)}} \left(\min(\underline{n} \setminus \{n\} \setminus B) \ - \ \sum_{d \in B} \pm\mu\left(n/d\right) \ d \right)$$

where

$$\mathcal{C}^{\pm}(B) \quad \Leftrightarrow \quad \forall d \in \underline{B} \qquad \#(B^{\pm} \cap \overline{d}) \;\geq\; \#(B^{\mp} \cap \overline{d})$$

The idea of the proof is as follows (we will explain the process for the cyclotomic polynomial; the proof for the inverse cyclotomic polynomial is analogous):

1. Recall that
$$\Phi_n = \prod_{d \in \underline{n}} \left(x^d - 1\right)^{\mu(n/d)}$$

2. We choose $B \subset \underline{n}$ and split Φ_n accordingly
$$\Phi_n = \prod_{d \in B} \left(x^d - 1\right)^{\mu(n/d)} \prod_{d \in \underline{n} \setminus B} \left(x^d - 1\right)^{\mu(n/d)}$$
The condition $\mathcal{C}^{+}(B)$ ensures that the first product is a polynomial.

3. We write Φ_n as follows (ignoring the signs of each term)
$$\Phi_n = G^{+} + x^u + x^{u+1} H$$
where $G^{+} = \prod_{d \in B} \left(x^d - 1\right)^{\mu(n/d)}$, $u = \min\left(\underline{n} \setminus \{n\} \setminus B\right)$, and H is some polynomial.

4. If $u > \deg(G^{+})$, then there is a gap in Φ_n between $x^{\deg(G^{+})}$ and x^u.

5. Note that $\deg(G^{+}) = \sum_{b \in B} \mu(n/d)\, d$. Thus $g(\Phi_n) \geq \min\left(\underline{n} \setminus \{n\} \setminus B\right) - \sum_{b \in B} \mu(n/d) d$

6. Taking the maximum over all sets B satisfying $\mathcal{C}^{+}(B)$ gives us $\varepsilon^{+}(n)$, our first lower bound for Φ_n.

We break the proof into several lemmas.

Notation 3.3. *Let*

$$F_C := \prod_{c \in C} (x^c - 1)$$

and $F(C) = 1$ *if* $C = \emptyset$.

Lemma 3.1. *We have that* $\dfrac{F_{B^\pm}}{F_{B^\mp}}$ *is a polynomial if*

$$\mathcal{C}^\pm(B) = \mathit{true}$$

$$B \subset \underline{n}$$

Proof. Let $C \subset \underline{n}$. Consider the following equalities.

$$F_C = \prod_{c\in C}(x^c - 1) = \prod_{c\in C}\prod_{d|c}\Phi_d = \prod_{d\in\underline{n}}\prod_{\substack{c\in C\\ d|c}}\Phi_d = \prod_{d\in\underline{n}}\Phi_d^{\#\{c\in C\,:\,d|c\}} = \prod_{d\in\underline{n}}\Phi_d^{\#(C\cap\overline{d})}$$

Thus

$$\frac{F_{B^\pm}}{F_{B^\mp}} = \frac{\prod\limits_{d\in\underline{n}}\Phi_d^{\#(B^\pm\cap\overline{d})}}{\prod\limits_{d\in\underline{n}}\Phi_d^{\#(B^\mp\cap\overline{d})}} = \prod_{d\in\underline{n}}\Phi_d^{\#(B^\pm\cap\overline{d})-\#(B^\mp\cap\overline{d})}$$

Note that for $d \in \underline{n} \setminus \underline{B}$, we have $\#(B^+ \cap \overline{d}) = 0$ and $\#(B^- \cap \overline{d}) = 0$. Thus,

$$\frac{F_{B^\pm}}{F_{B^\mp}} = \prod_{d\in\underline{B}}\Phi_d^{\#(B^\pm\cap\overline{d})-\#(B^\mp\cap\overline{d})}$$

Recall $\mathcal{C}^\pm(B) \iff \forall d \in \underline{B}\ \ \#(B^\pm \cap \overline{d}) \geq \#(B^\mp \cap \overline{d})$. Therefore, $\frac{F_{B^\pm}}{F_{B^\mp}}$ is a polynomial. □

Lemma 3.2. *We have*

$$P^\pm \equiv_{x^{\min(A)+1}} \pm\begin{cases} -(-1)^{|A|}G^\pm - x^{\min(A)} & \text{if } \min(A) \in A^\pm \\ -(-1)^{|A|}G^\pm + x^{\min(A)} & \text{if } \min(A) \in A^\mp \end{cases}$$

where

$$P^{\pm} = \frac{F_{\underline{n}^{\pm}}\ F_{\{n\}^{\mp}}}{F_{\underline{n}^{\mp}}}$$

$$G^{\pm} = \frac{F_{B^{\pm}}}{F_{B^{\mp}}}$$

$$A \uplus B = \underline{n} \setminus \{n\}$$

$$A \neq \emptyset$$

$$\mathcal{C}^{\pm}(B) = \mathit{true}$$

$$|B| = \#\{b \in B\}$$

and the notation $\square \equiv_{x^{\min(A)+1}} \triangle$ *stands for* $x^{\min(A)+1}|\square - \triangle$.

Proof. For simplicity, in the rest of this proof we will use u instead of $\min(A)$. Since $A \neq \emptyset$, $\min(A)$ is defined. Note

$$F_{\underline{n}^{\mp}}\ P^{\pm} = F_{\underline{n}^{\pm}}\ F_{\{n\}^{\mp}}$$

$$F_{\{n\}^{\mp}}\ F_{A^{\mp}}\ F_{B^{\mp}}\ P^{\pm} = F_{A^{\pm}}\ F_{B^{\pm}}\ F_{\{n\}^{\pm}}\ F_{\{n\}^{\mp}}$$

Case: $u \in A^{\pm}$. Since $u = \min A$ we have

$$F_{A^{\pm}\setminus\{u\}} \equiv_{x^{u+1}} (-1)^{|A^{\pm}|-1}$$

$$F_{A^{\mp}} \equiv_{x^{u+1}} (-1)^{|A^{\mp}|}$$

$$F_{\{n\}^{\pm}} \equiv_{x^{u+1}} (-1)^{|\{n\}^{\pm}|}$$

$$F_{\{n\}^{\mp}} \equiv_{x^{u+1}} (-1)^{|\{n\}^{\mp}|}$$

Thus

$$F_{B^{\mp}}\ P^{\pm} \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^{\pm}|}(x^u - 1)\ F_{B^{\pm}}$$

Since $\mathcal{C}^{\pm}(B)$, by Lemma 3.1 we have

$$F_{B^{\mp}}\ P^{\pm} \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^{\pm}|}(x^u - 1)\ F_{B^{\mp}}\ G^{\pm}$$

Note that 0 is the only root of x^{u+1} and $F_{B^{\mp}}(0) = (-1)^{|B^{\mp}|}$. Hence $\gcd(F_{B^{\mp}}, x^{u+1}) = 1$. Thus we can cancel $F_{B^{\mp}}$ from both sides, obtaining

$$\begin{aligned} P^{\pm} &\equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^{\pm}|}(x^u - 1)G^{\pm} \\ &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^{\pm}|}G^{\pm} + (-1)^{|A|-1+|\{n\}^{\pm}|}x^u G^{\pm} \end{aligned}$$

Note that $G^{\pm}(0) = (-1)^{|B|}$. Thus we have

$$\begin{aligned} P^{\pm} &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^{\pm}|}G^{\pm} + (-1)^{|A|-1+|\{n\}^{\pm}|+|B|}x^u \\ &\equiv_{x^{u+1}} (-1)^{-1+|\{n\}^{\pm}|}\left(-(-1)^{|A|}G^{\pm} + (-1)^{|A|+|B|}x^u\right) \\ &\equiv_{x^{u+1}} \pm\left(-(-1)^{|A|}G^{\pm} + (-1)^{2^k-1}x^u\right) \\ &\equiv_{x^{u+1}} \pm\left(-(-1)^{|A|}G^{\pm} - x^u\right) \end{aligned}$$

which proves the lemma.

Case: $u \in A^{\mp}$. Since $u = \min A$ we have

$$\begin{aligned} F_{A^{\pm}} &\equiv_{x^{u+1}} (-1)^{|A^{\pm}|} \\ F_{A^{\mp}\setminus\{u\}} &\equiv_{x^{u+1}} (-1)^{|A^{\mp}|-1} \\ F_{\{n\}^{\pm}} &\equiv_{x^{u+1}} (-1)^{|\{n\}^{\pm}|} \\ F_{\{n\}^{\mp}} &\equiv_{x^{u+1}} (-1)^{|\{n\}^{\mp}|} \end{aligned}$$

Thus

$$(x^u - 1)F_{B^\mp} \cdot P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} F_{B^\pm}$$

Since $\mathcal{C}^\pm(B)$, by Lemma 3.1 we have

$$(x^u - 1)F_{B^\mp} \cdot P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} F_{B^\mp} \cdot G^\pm$$

Note that 0 is the only root of x^{u+1} and $F_{B^\mp}(0) = (-1)^{|B^\mp|}$. Hence $\gcd(F_{B^\mp}, x^{u+1}) = 1$. Thus we can cancel $F_{B^\mp}$ from both sides, obtaining

$$(x^u - 1)\ P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} G^\pm$$

Multiplying both sides by $(x^u + 1)$, we have

$$\begin{aligned}
(x^u + 1)(x^u - 1)P^\pm &\equiv_{x^{u+1}} (x^u + 1)(-1)^{|A|-1+|\{n\}^\pm|} G^\pm \\
(x^{2u} - 1)P^\pm &\equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} G^\pm + (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm \\
-P^\pm &\equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} G^\pm + (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm \\
P^\pm &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^\pm|} G^\pm - (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm
\end{aligned}$$

Note that $G^\pm(0) = (-1)^{|B|}$. Thus we have

$$\begin{aligned}
P^\pm &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^\pm|} G^\pm - (-1)^{|A|-1+|\{n\}^\pm|+|B|} x^u \\
&\equiv_{x^{u+1}} (-1)^{-1+|\{n\}^\pm|} \left(-(-1)^{|A|} G^\pm - (-1)^{|A|+|B|} x^u \right) \\
&\equiv_{x^{u+1}} \pm \left(-(-1)^{|A|} G^\pm - (-1)^{2^{k-1}} x^u \right) \\
&\equiv_{x^{u+1}} \pm \left(-(-1)^{|A|} G^\pm + x^u \right)
\end{aligned}$$

which proves the lemma.

□

Proof of Theorem 3.5-(1). Using the same notation as in Lemma 3.2, note

$$P^+ = \Phi_n$$

Let A and B be such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $\mathcal{C}^+(B)$. By Lemma 3.2, we have

$$\Phi_n = + \begin{cases} -(-1)^{|A|} G^+ - x^{\min(A)} + x^{\min(A)+1} H & \text{if } \min(A) \in A^+ \\ -(-1)^{|A|} G^+ + x^{\min(A)} + x^{\min(A)+1} H & \text{if } \min(A) \in A^- \end{cases}$$

for some polynomial H. Note

$$\deg G^+ = \deg \left(\frac{F_{B^+}}{F_{B^-}} \right) = \sum_{d \in B^+} d - \sum_{d \in B^-} d = \sum_{d \in B} \mu(n/d)\, d = l^+(B)$$

If $\min(A) \leq l^+(B)$, then clearly

$$g(\Phi_n) \geq \min(A) - l^+(B)$$

If $\min(A) > l^+(B)$, then $x^{l^+(B)}$ and $x^{\min(A)}$ appear in Φ_n, so we have

$$g(\Phi_n) \geq \min(A) - l^+(B)$$

Thus

$$g(\Phi_n) \geq \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^+(B)}} \min(A) - l^+(B) = \max_{\substack{B \subsetneq \underline{n} \setminus \{n\} \\ \mathcal{C}^+(B)}} \left(\min(\underline{n} \setminus \{n\} \setminus B) \ - \ \sum_{d \in B} \mu(n/d) \ d \right) = \varepsilon^+(n)$$

The theorem has been proved. □

Proof of Theorem 3.5-(2). Using the same notation as in Lemma 3.2, note

$$P^- = \Psi_n$$

Let A and B be such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $\mathcal{C}^-(B)$. By Lemma 3.2, we have

$$\Psi_n = -\begin{cases} -(-1)^{|A|}G^- - x^{\min(A)} + x^{\min(A)+1}H & \text{if } \min(A) \in A^- \\ -(-1)^{|A|}G^- + x^{\min(A)} + x^{\min(A)+1}H & \text{if } \min(A) \in A^+ \end{cases}$$

for some polynomial H. Note

$$\deg G^- = \deg\left(\frac{F_{B^-}}{F_{B^+}}\right) = \sum_{d \in B^-} d - \sum_{d \in B^+} d = \sum_{d \in B} -\mu(n/d)\, d = l^-(B)$$

If $\min(A) \leq l^-(B)$, then clearly

$$g(\Psi_n) \geq \min(A) - l^-(B)$$

If $\min(A) > l^-(B)$, then $x^{l^-(B)}$ and $x^{\min(A)}$ appear in Ψ_n, so we have

$$g(\Psi_n) \geq \min(A) - l^-(B)$$

Thus

$$g(\Psi_n) \geq \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^-(B)}} \min(A) - l^-(B) = \max_{\substack{B \subsetneq \underline{n} \setminus \{n\} \\ \mathcal{C}^-(B)}} \left(\min(\underline{n} \setminus \{n\} \setminus B) \; - \; \sum_{d \in B} -\mu(n/d) \; d \right) = \varepsilon^-(n)$$

The theorem has been proved. □

3.4.2 Proof of special bounds

We will first prove the lower bounds $\alpha^{\pm}$, $\beta^{\pm}$ and $\gamma^{\pm}$, which are all proved in a similar manner. We will then prove δ^{-} in a different manner.

We prove the lower bounds $\alpha^{\pm}$, $\beta^{\pm}$ and $\gamma^{\pm}$ by restricting the choice of B as mentioned in Section 5.1. Recall that the restrictions of B for are very similar. To handle them all at the same time, we will use the following uniform notation

$$\Omega_{jr} = \left\{ c \in \underline{n_j} : \omega(c) < r \right\}$$

Note that B for $\alpha^{\pm}$, $\beta^{\pm}$ and $\gamma^{\pm}$ can be compactly written as $B = \Omega_{r-1,r}$, $B = \Omega_{rr}$ and $B = \Omega_{kr}$ respectively. In the following three lemmas, we will show that $\mathcal{C}^{\pm}(\Omega_{jr})$ holds. Recall that

$$\mathcal{C}^{\pm}(\Omega_{jr}) \quad \Leftrightarrow \quad \forall d \in \underline{\Omega_{jr}} \quad \#(\Omega^{\pm}_{jr} \cap \overline{d}) \;\geq\; \#(\Omega^{\mp}_{jr} \cap \overline{d})$$

The outline of the proof is as follows:

1. Given $d \in \underline{\Omega_{jr}}$ and $s \in \{+,-\}$ we show that $\#(\Omega^{s}_{jr} \cap \overline{d})$ can be written as a sum of binomial coefficients.

2. Using a telescoping sum property of binomial coefficients, we show $\#(\Omega^{\pm}_{jr} \cap \overline{d}) - \#(\Omega^{\mp}_{jr} \cap \overline{d})$ is non-negative

Lemma 3.3. *We have, for $s \in \{+,-\}$, that*

$$\#\left(\Omega^{s}_{jr} \cap \overline{d}\right) = \sum_{\substack{0 \leq i < r - \omega(d) \\ \rho(i) = s\rho(k - \omega(d))}} \binom{j - \omega(d)}{i}$$

for $1 \leq r < k$, $r - 1 \leq j \leq k$ and $d \in \underline{\Omega_{jr}}$.

Proof. Note

$$\begin{aligned}
\#\left(\Omega_{jr}^{s}\cap\overline{d}\right) &= \#\big\{c\in\underline{n_j} \quad : \omega(c)<r, \qquad \mu(n/c)=s,\, d\mid c\,\big\}\\
&= \#\big\{ld\in\underline{n_j} \quad : \omega(ld)<r, \qquad \mu(n/(ld))=s\big\}\\
&= \#\big\{l\in\underline{n_j/d} \quad : \omega(l)<r-\omega(d), \quad \mu(l)=s\mu(n/d)\,\big\}
\end{aligned}$$

Note

$$s\mu(n/d)=s\rho(k-\omega(d))$$

Thus

$$\begin{aligned}
\#\left(\Omega_{jr}^{s}\cap\overline{d}\right) &= \#\biguplus_{\substack{0\le i<r-\omega(d)\\ \rho(i)=s\rho(k-\omega(d))}}\Big\{l\in\underline{n_j/d}:\omega(l)=i\Big\}\\
&= \sum_{\substack{0\le i<r-\omega(d)\\ \rho(i)=s\rho(k-\omega(d))}}\#\Big\{l\in\underline{n_j/d}:\omega(l)=i\Big\}\\
&= \sum_{\substack{0\le i<r-\omega(d)\\ \rho(i)=s\rho(k-\omega(d))}}\binom{\omega(n_j/d)}{i}\\
&= \sum_{\substack{0\le i<r-\omega(d)\\ \rho(i)=s\rho(k-\omega(d))}}\binom{j-\omega(d)}{i}
\end{aligned}$$

which proves the lemma. □

Lemma 3.4 (Telescoping sum)**.** *We have*

$$\sum_{0\le i\le u}\rho(i)\binom{t}{i}=\begin{cases}\rho(u)\binom{t-1}{u} & \text{if } t\ge 1\\ 1 & \text{if } t=0\end{cases}$$

Proof. When $t \geq 1$, we have

$$\begin{aligned}
\sum_{0\leq i\leq u} \rho(i)\binom{t}{i} &= \sum_{0\leq i\leq u} \rho(i)\binom{t-1}{i-1} + \sum_{0\leq i\leq u} \rho(i)\binom{t-1}{i} \\
&= -\sum_{-1\leq i\leq u-1} \rho(i)\binom{t-1}{i} + \sum_{0\leq i\leq u} \rho(i)\binom{t-1}{i} \\
&= -\rho(-1)\binom{t-1}{-1} + \rho(u)\binom{t-1}{u} \\
&= \rho(u)\binom{t-1}{u}
\end{aligned}$$

When $t = 0$, we have

$$\sum_{0\leq i\leq u} \rho(i)\binom{t}{i} = \rho(0)\binom{0}{0} + \sum_{1\leq i\leq u} \rho(i)\binom{0}{i} = 1 + 0 = 1$$

□

Lemma 3.5. *We have $\mathcal{C}^{\pm}(\Omega_{jr})$ for $1 \leq r < k$, $\rho(k-r) = \mp 1$ and $r - 1 \leq j \leq k$.*

Proof. Recall

$$\mathcal{C}^{\pm}(\Omega_{jr}) \iff \forall d \in \underline{\Omega_{jr}} \ \#\left(\Omega_{jr}^{\pm} \cap \overline{d}\right) \geq \#\left(\Omega_{jr}^{\mp} \cap \overline{d}\right)$$

Note

$$\begin{aligned}
&\#\left(\Omega_{jr}^{\pm} \cap \overline{d}\right) - \#\left(\Omega_{jr}^{\mp} \cap \overline{d}\right) \\
&= \sum_{\substack{0\leq i<r-\omega(d) \\ \rho(i)=\pm\rho(k-\omega(d))}} \binom{j-\omega(d)}{i} - \sum_{\substack{0\leq i<r-\omega(d) \\ \rho(i)=\mp\rho(k-\omega(d))}} \binom{j-\omega(d)}{i} \quad \text{by Lemma 3.3} \\
&= \sum_{\substack{0\leq i<r-\omega(d) \\ \rho(i)=-\rho(k-r)\rho(k-\omega(d))}} \binom{j-\omega(d)}{i} - \sum_{\substack{0\leq i<r-\omega(d) \\ \rho(i)=+\rho(k-r)\rho(k-\omega(d))}} \binom{j-\omega(d)}{i} \quad \text{since } \rho(k-r) = \mp 1
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{0\le i<r-\omega(d)\\ \rho(i)=-\rho(r-\omega(d))}} \binom{j-\omega(d)}{i} - \sum_{\substack{0\le i<r-\omega(d)\\ \rho(i)=+\rho(r-\omega(d))}} \binom{j-\omega(d)}{i} \\
&= \sum_{0\le i<r-\omega(d)} -\rho(r-\omega(d))\,\rho(i)\binom{j-\omega(d)}{i} \\
&= -\rho(r-\omega(d)) \sum_{0\le i<r-\omega(d)} \rho(i)\binom{j-\omega(d)}{i} \\
&= -\rho(r-\omega(d)) \begin{cases} \rho(r-\omega(d)-1)\binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d)\ge 1 \\ 1 & \text{if } j-\omega(d)=0 \end{cases} \quad \text{by Lemma 3.4} \\
&= \begin{cases} -\rho(r-\omega(d))\,\rho(r-\omega(d)-1)\binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d)\ge 1 \\ -\rho(r-\omega(d)) & \text{if } j-\omega(d)=0 \end{cases} \\
&= \begin{cases} \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d)\ge 1 \\ -\rho(r-\omega(d)) & \text{if } j-\omega(d)=0 \end{cases}
\end{aligned}
$$

Consider the case $j-\omega(d)=0$: Since $r-1\le j=\omega(d)\le r-1$, we have $\omega(d)=r-1$. Therefore we have

$$
\begin{aligned}
\#\left(\Omega_{jr}^{\pm}\cap\overline{d}\right)-\#\left(\Omega_{jr}^{\mp}\cap\overline{d}\right) &= \begin{cases} \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d)\ge 1 \\ -\rho(1) & \text{if } j-\omega(d)=0 \end{cases} \\
&= \begin{cases} \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d)\ge 1 \\ 1 & \text{if } j-\omega(d)=0 \end{cases} \\
&\ge 0
\end{aligned}
$$

which proves the lemma. □

Now that we have shown that $\mathcal{C}^{\pm}(\Omega_{jr})$ holds, we restrict our choice of B in $\varepsilon^{\pm}$ to Ω_{jr} and simplify the expression.

Lemma 3.6. *We have, for $r-1 \le j \le k$,*

$$\varepsilon^{\pm}(n) \ge \max_{\substack{1\le r<k \\ \rho(k-r)=\mp 1}} \left(\min\{p_{j+1}, n_r\} - \sum_{\substack{d|n_j \\ \omega(d)<r}} \pm\mu(n/d)\ d \right)$$

where p_{k+1} is viewed as ∞.

Proof. Note

$$\begin{aligned}
\varepsilon^{\pm}(n) &= \max_{\substack{B\subsetneq \underline{n}\setminus\{n\} \\ \mathcal{C}^{\pm}(B)}} \left(\min(\underline{n}\setminus\{n\}\setminus B) \ - \ l^{\pm}(B)\right) \\
&\ge \max_{\substack{B\subsetneq \underline{n}\setminus\{n\} \\ \mathcal{C}^{\pm}(B) \\ 1\le r<k \\ \rho(k-r)=\mp 1 \\ B=\Omega_{jr}}} \min(\underline{n}\setminus\{n\}\setminus\Omega_{jr}) - l^{\pm}(\Omega_{jr}) \qquad \text{by restricting the choice of } B \text{ to } \Omega_{jr} \\
&= \max_{\substack{1\le r<k \\ \rho(k-r)=\mp 1 \\ \mathcal{C}^{\pm}(\Omega_{jr})}} \min(\underline{n}\setminus\{n\}\setminus\Omega_{jr}) - l^{\pm}(\Omega_{jr}) \\
&= \max_{\substack{1\le r<k \\ \rho(k-r)=\mp 1}} \min(\underline{n}\setminus\{n\}\setminus\Omega_{jr}) - l^{\pm}(\Omega_{jr}) \ \text{ by Lemma 3.5}
\end{aligned}$$

Note

$$\begin{aligned}
\min(\underline{n}\setminus\{n\}\setminus\Omega_{jr}) &= \min(\underline{n}\setminus\{n\}\setminus\Omega_{jr}) \\
&= \min(\underline{n}\setminus\{n\}\setminus\{c : c|n_j, \omega(c)<r\}) \\
&= \min\{c : c|n, c\ne n \text{ and } (c\nmid n_j \text{ or } \omega(c)\ge r)\} \\
&= \min\left(\min\{c : c|n, c\ne n \text{ and } c\nmid n_j\}, \min\{c : c|n, c\ne n \text{ and } \omega(c)\ge r\}\right) \\
&= \min\left(\min\left\{c : c|n, c\ne n \text{ and } \exists_{i\ge j+1} p_i|c\right\}, n_r\right) \\
&= \min\{p_{j+1}, n_r\}
\end{aligned}$$

Note

$$l^{\pm}\left(\Omega_{jr}\right)=\sum_{d\in\Omega_{jr}}\pm\mu\left(n/d\right)\ d=\sum_{\substack{d\in\overline{n_j}\\ \omega(d)<r}}\pm\mu\left(n/d\right)\ d$$

Hence

$$\varepsilon^{\pm}(n)\geq\max_{\substack{1\leq r<k\\ \rho(k-r)=\mp 1}}\left(\min\left\{p_{j+1},n_r\right\}-\sum_{\substack{d\in\overline{n_j}\\ \omega(d)<r}}\pm\mu\left(n/d\right)\ d\right)$$

□

Lemma 3.7. *We have*

$$\varphi\left(n_r\right)=\sum_{d|n_r}\mu\left(n_r/d\right)\ d$$

Proof. Note

$$\varphi\left(n_r\right)=\left(p_1-1\right)\cdots\left(p_r-1\right)=\left(-1\right)^r\left(1-p_1\right)\cdots\left(1-p_r\right)=\left(-1\right)^r\sum_{d|n_r}\mu\left(d\right)\ d=\sum_{d|n_r}\mu\left(n_r/d\right)\ d$$

□

To prove that $\alpha^{\pm}$ is a lower bound, we set $j=r-1$ as mentioned earlier, and then simplify.

Proof of Theorem 3.1. We set $j=r-1$. Note

$$\varepsilon^{\pm}(n)\geq\max_{\substack{1\leq r<k\\ \rho(k-r)=\mp 1}}\left(\min\left\{p_{r-1+1},n_r\right\}-\sum_{\substack{d|n_{r-1}\\ \omega(d)<r}}\pm\mu\left(n/d\right)\ d\right)\quad\text{by Lemma 3.6}$$

Note that

$$\min\left\{p_{r-1+1},n_r\right\}=\min\left\{p_r,n_r\right\}=p_r$$

Note that

$$\begin{aligned}
\sum_{\substack{d|n_{r-1}\\ \omega(d)<r}} \pm\mu\left(n/d\right)\ d &= \sum_{d|n_{r-1}} \pm\mu\left(n/d\right)\ d \\
&= \sum_{d|n_{r-1}} \pm\mu\left(n/n_{r-1}\right)\mu\left(n_{r-1}/d\right)\ d \\
&= \sum_{d|n_{r-1}} \pm 1\cdot\pm 1\mu\left(n_{r-1}/d\right)\ d \\
&= \sum_{d|n_{r-1}} \mu\left(n_{r-1}/d\right)\ d \\
&= \varphi\left(n_{r-1}\right) \quad \text{by Lemma 3.7}
\end{aligned}$$

Thus

$$\varepsilon^{\pm}(n) \geq \max_{\substack{1\leq r<k\\ \rho(k-r)=\mp 1}} \left(p_r - \varphi\left(n_{r-1}\right)\right) = \max_{\substack{1\leq r<k\\ \rho(k-r)=\mp 1}} \left(p_r - \varphi\left(p_1\cdots p_{r-1}\right)\right) = \alpha^{\pm}(n)$$

Hence

$$g(\Phi_n) \geq \varepsilon^{+}(n) \geq \alpha^{+}(n)$$

$$g(\Psi_n) \geq \varepsilon^{-}(n) \geq \alpha^{-}(n)$$

The theorem has been proved. □

To prove that $\beta^{\pm}$ is a lower bound, we set $j = r$ as mentioned earlier, and then simplify.

Proof of Theorem 3.2. We set $j = r$. Note

$$\varepsilon^{\pm}(n) \geq \max_{\substack{1\leq r<k \\ \rho(k-r)=\mp 1}} \left(\min\{p_{r+1}, n_r\} - \sum_{\substack{d\in \underline{n_r} \\ \omega(d)<r}} \pm\mu(n/d)\ d \right) \quad \text{by Lemma 3.6}$$

Note that

$$\begin{aligned}
\sum_{\substack{d\in \underline{n_r} \\ \omega(d)<r}} \pm\mu(n/d)\ d &= \sum_{d\in \underline{n_r}\setminus\{n_r\}} \pm\mu(n/n_r)\,\mu(n_r/d)\ d \\
&= \sum_{d\in \underline{n_r}\setminus\{n_r\}} \pm 1\cdot\mp 1\cdot\mu(n_r/d)\ d \\
&= -\sum_{d\in \underline{n_r}\setminus\{n_r\}} \mu(n_r/d)\ d \\
&= \mu(n_r/n_r)\ n_r - \sum_{d\in \underline{n_r}} \mu(n_r/d)\ d \\
&= n_r - \sum_{d\mid n_r} \mu(n_r/d)\ d \\
&= n_r - \varphi(n_r) \qquad \text{by Lemma 3.7} \\
&= \psi(n_r)
\end{aligned}$$

Thus

$$\begin{aligned}
\varepsilon^{\pm}(n) &\geq \max_{\substack{1\leq r<k \\ \rho(k-r)=\mp 1}} (\min\{p_{r+1}, n_r\} - \psi(n_r)) \\
&= \max_{\substack{1\leq r<k \\ \rho(k-r)=\mp 1}} (\min\{p_{r+1}, p_1\cdots p_r\} - \psi(p_1\cdots p_r)) \\
&= \beta^{\pm}(n)
\end{aligned}$$

Hence

$$g(\Phi_n) \geq \varepsilon^+(n) \geq \beta^+(n)$$
$$g(\Psi_n) \geq \varepsilon^-(n) \geq \beta^-(n)$$

The theorem has been proved. □

To prove that $\gamma^{\pm}$ is a lower bound, we set $j = k$ as mentioned earlier, and then simplify.

Proof of Theorem 3.3. We set $j = k$. Note

$$\varepsilon^{\pm}(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(\min\{p_{k+1}, n_r\} - \sum_{\substack{d \in \underline{n} \\ \omega(d) < r}} \pm\mu(n/d)\ d \right) \quad \text{by Lemma 3.6}$$

Note

$$\min\{p_{k+1}, n_r\} = \min\{\infty, n_r\} = n_r$$

Thus

$$\begin{aligned} \varepsilon^{\pm}(n) &\geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(n_r - \sum_{\substack{d \in \underline{n} \\ \omega(d) < r}} \pm\mu(n/d)\ d \right) \\ &= \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(p_1 \cdots p_r - \sum_{\substack{d \mid n \\ \omega(d) < r}} \pm\mu(n/d)\ d \right) \\ &= \gamma^{\pm}(n) \end{aligned}$$

Hence

$$g(\Phi_n) \geq \varepsilon^+(n) \geq \gamma^+(n)$$

$$g(\Psi_n) \geq \varepsilon^-(n) \geq \gamma^-(n)$$

The theorem has been proved. □

It is possible to prove Theorem 3.4 in a similar way to the last three theorems, by restricting B as mentioned in Section 5.1, that is,

$$B = \{d : d | p_1 \cdots p_k \text{ and } \omega(d) < k \text{ and } d \neq p_2 \cdots p_k\}$$

However, it is simpler to prove it in a different way. We show that Ψ_n can be written as the sum of a polynomial with that same polynomial, shifted. When the shift is large enough, a gap appears in the middle of Ψ_n.

Lemma 3.8. *We have*

$$\Psi_n(x) = H(x)\left(x^{\frac{n}{p_1}} - 1\right)$$

where $H(x) = \Phi_{n_{k-1}}\left(x^{\frac{n}{n_k}}\right)\Phi_{n_{k-2}}\left(x^{\frac{n}{n_{k-1}}}\right)\cdots\Phi_{n_1}\left(x^{\frac{n}{n_2}}\right)$.

Proof. Recall the well known property of cyclotomic polynomials

$$\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$$

where p is a prime and not a factor of n. In terms of the inverse cyclotomic polynomial, it can be immediately restated as

$$\Psi_{np}(x) = \Phi_n(x)\Psi_n(x^p)$$

Repeatedly applying the above equality on $\Psi_n(x)$, we have

$$\begin{aligned}\Psi_n(x) &= \Phi_{n_{k-1}}\left(x^{\frac{n}{n_k}}\right)\Psi_{n_{k-1}}\left(x^{\frac{n}{n_{k-1}}}\right)\\ &= \Phi_{n_{k-1}}\left(x^{\frac{n}{n_k}}\right)\Phi_{n_{k-2}}\left(x^{\frac{n}{n_{k-1}}}\right)\Psi_{n_{k-2}}\left(x^{\frac{n}{n_{k-2}}}\right)\end{aligned}$$

$$
\begin{aligned}
&= \cdots \\
&= \Phi_{n_{k-1}}\left(x^{\frac{n}{n_k}}\right)\Phi_{n_{k-2}}\left(x^{\frac{n}{n_{k-1}}}\right)\cdots\Phi_{n_1}\left(x^{\frac{n}{n_2}}\right)\Psi_{n_1}\left(x^{\frac{n}{p_1}}\right) \\
&= H(x)\,\Psi_{n_1}\left(x^{\frac{n}{p_1}}\right)
\end{aligned}
$$

Recall that for a prime p, we have

$$\Psi_p(x) = x - 1$$

Hence

$$\Psi_n(x) = H(x)\left(x^{\frac{n}{p_1}} - 1\right)$$

□

Proof of Theorem 3.4. From Lemma 3.8 we have

$$
\begin{aligned}
\Psi_n(x) &= H(x)\left(x^{\frac{n}{p_1}} - 1\right) \\
&= -H(x) + H(x)\cdot x^{\frac{n}{p_1}}
\end{aligned}
$$

Note

$$
\begin{aligned}
\deg\left(H(x)\right) &= \psi(n) - \frac{n}{p_1} \\
\operatorname{tdeg}\left(H(x)\cdot x^{\frac{n}{p_1}}\right) &= \frac{n}{p_1}
\end{aligned}
$$

We have

$$\frac{n}{p_1} - \left(\psi(n) - \frac{n}{p_1}\right) = 2\,\frac{n}{p_1} - \psi(n) = \delta^-(n)$$

If $\delta^-(n) \leq 0$, then there is nothing to show. If $\delta^-(n) > 0$ then there is a gap in $\Psi_n(x)$ between $x^{\psi(n)-\frac{n}{p_1}}$ and $x^{\frac{n}{p_1}}$. Therefore

$$g(\Psi_n) \geq \delta^-(n)$$

The theorem has been proved. □

3.5 Complexity

In this section, we analyze the bit time complexity of the special lower bounds and the general lower bound. We will see that the general lower bound $\varepsilon^{\pm}$ has a very large computational complexity, so we introduce a new general lower bound, $\tilde{\varepsilon}^{\pm}$ which is defined as follows:

$$\tilde{\varepsilon}^{\pm}(n) = \max_{\substack{b \in \underline{n}^{\pm} \\ B = \underline{n}_b^{\pm} \cup (\underline{n}_b^{\pm})^{\mp} \\ \mathcal{C}^{\pm}(B)}} \left(\min\left(\underline{n} \setminus \{n\} \setminus B\right) - \sum_{d \in B} \pm\mu\left(n/d\right)\ d \right)$$

where $A_b = \{a \in A \ : \ a < b\}$. We conjecture that $\varepsilon^{\pm}(n) = \tilde{\varepsilon}^{\pm}(n)$ for all n. We have verified this conjecture for all $n \leq 15015$. Thus we also analyze the complexity of $\tilde{\varepsilon}^{\pm}$, which we observe to be much less than that of $\varepsilon^{\pm}$.

Table 3.2 below is a summary of the bit time complexities of the various computations.

Table 3.2 Time complexities

computation	complexity	
Φ_n	$O\left(2^{kL}\right)$	operations over $\mathbb{Z}$ [2]
Ψ_n	$O\left(2^{kL}\right)$	operations over $\mathbb{Z}$ [2]
$\alpha^{\pm}$	$O\left(k^2L^2\right)$	
$\beta^{\pm}$	$O\left(k^2L^2\right)$	
$\gamma^{\pm}$	$O\left(2^{(1+\nu)k}L^2\right)$	
δ^{-}	$O\left(kL^2\right)$	
$\varepsilon^{\pm}$	$O\left(2^{(1+\nu)2^k}L^2\right)$	
$\tilde{\varepsilon}^{\pm}$	$O\left(2^{(3+\nu)k}L^2\right)$	

In the above table, $\nu > 0$ is an arbitrarily small number (note that we cannot use the conventional ε since it is already used to denote the lower bound). Observe that the time it takes to compute Φ_n is exponential in both k and L. However, recall from Chapter 2 Section 2.5 that this was an optimistic estimate, since [2] only provides the number of operations in $\mathbb{Z}$, and does not take into account the lengths of the integers in intermediate steps. Thus if one takes them into account the actual time complexity could be even larger.

Since $\alpha^{\pm}$, $\beta^{\pm}$ and δ^{-} are linear or quadratic in k and quadratic in L, we observe that they are much faster to compute. For $\gamma^{\pm}$, $\varepsilon^{\pm}$ and $\tilde{\varepsilon}^{\pm}$, we consider the time complexities when each of k and L is fixed. When k is fixed, Φ_n and Ψ_n are exponential in L and $\gamma^{\pm}$, $\varepsilon^{\pm}$ and $\tilde{\varepsilon}^{\pm}$ are quadratic in L. Thus in this case, they are much faster to compute. When L is fixed, it is more difficult to compare the time it takes to compute the lower bounds and Φ_n and Ψ_n. However, note that when L, which is the length of the largest prime, is fixed, k is dependent on L and cannot grow arbitrarily large. We will not get into that discussion here, since it involves a deeper

examination into the distribution of prime numbers. However, note that it is more common in practice for k, the number of prime factors, to be fixed, and the length of the largest prime to be allowed to grow larger. Thus, in that sense, our lower bounds are much faster to compute than direct computation of the cyclotomic polynomial.

We also remark that the complexities of the lower bounds are based on "brute force" implementations of the formulas. It is likely that the complexities can be reduced by using "smarter" implementations.

Before we get into the formal analysis of the time complexity of the lower bounds, we first state the following assumptions that we make to account for the asymptotically worst case:

1. We assume that all primes in the factorization of n are equal to the largest prime. Therefore, we assume that the bit length of every prime is equal to the bit length of the largest prime, that is, $\log_2(p_i) = L$ for all $1 \leq i \leq k$ where $L = \max_{1 \leq i \leq k} \log_2(p_i)$. This implies $p_i = 2^L$ for all $1 \leq i \leq k$. It follows that

$$n = p_1 \cdots p_k = 2^L \cdots 2^L = \left(2^L\right)^k = 2^{kL}$$
$$\log_2(n) = \log_2(2^{kL}) = kL$$

2. When we take the maximum over $1 \leq r < k$, $\rho(k - r) = \mp 1$, we take the maximum over $1 \leq r \leq k - 1$.

3.5.1 Complexity of shared operations

We list the time complexities for some important operations

1. Compute all divisors of $n = p_1 \cdots p_k$. The following shows the time complexity of computing all the divisors with a given number of prime factors.

divisors	time to compute
$\{p_1, \ldots, p_k\}$	0
$\{p_1p_2, \ldots, p_{k-1}p_k\}$	$\binom{k}{2}L^2$
$\{p_1p_2p_3, \ldots, p_{k-2}p_{k-1}p_k\}$	$\binom{k}{3}2L^2$
$\cdots$	
$\{p_1 \cdots p_{k-1}, \ldots, p_2 \cdots p_k\}$	$\binom{k}{k-1}(k-2)L^2$
n	0

Summing all of these, we get

$$\left(\sum_{i=2}^{k-1}\binom{k}{i}(i-1)\right)L^2 = (k-2)\left(2^{k-1}-1\right)L^2$$

Thus the time to compute all the divisors of n is $O\left(k2^kL^2\right)$. We make an important note here that when we compute $\underline{n}$, we will also compute a graph showing the divisor relationships between the elements in $\underline{n}$. The nodes of the graph will be the elements of $\underline{n}$ and the edges are the divisor relations. Two nodes will be joined by an edge if one element is a divisor of the other. When doing this, we can also determine whether a divisor is in $\underline{n}^+$ or $\underline{n}^-$. Doing so will not take any more computational time and it will allow us to simplify our computations later on in our analysis.

2. Sort $\underline{n}$. The number of comparisons required to do this is $O\left(2^k\log(2^k)\right)$, and the time to compute each of those operations will be the length of the largest number we are comparing, which is kL. Thus we have that the worst case computing time for sorting $\underline{n}$, $T_{\text{sort}}(k, L)$, is given by the following

$$T_{\text{sort}}(k, L) = O\left(2^k\log(2^k)kL\right)$$

$$T_{\text{sort}}(k, L) = O\left(k^2 2^k L\right)$$

Therefore, the time complexity for sorting the divisors is $O\left(k^2 2^k L\right)$.

3.5.2 Complexity of lower bounds

Table 3.3 below is a summary of the complexities of the lower bounds.

Table 3.3 Time complexities of the lower bounds

computation	complexity
$\alpha^{\pm}$	$O\left(k^2 L^2\right)$
$\beta^{\pm}$	$O\left(k^2 L^2\right)$
$\gamma^{\pm}$	$O\left(2^{(1+\nu)k} L^2\right)$
δ^{-}	$O\left(kL^2\right)$
$\varepsilon^{\pm}$	$O\left(2^{(1+\nu)2^k} L^2\right)$
$\tilde{\varepsilon}^{\pm}$	$O\left(2^{(3+\nu)k} L^2\right)$

We give an informal interpretation of the above results, discussing those computations which dominate the complexity:

- For bounds $\alpha^{\pm}$ and $\beta^{\pm}$, we take the maximum over k elements. To compute the numbers of which we are taking the maximum we continually multiply prime factors of n, which gives us $O\left(kL^2\right)$. Thus, in total, we get $O\left(k^2 L^2\right)$.
- For $\gamma^{\pm}$, we compute all divisors of n, which gives us $k2^k L^2$. We then add and subtract them, which gives us another factor of k in the complexity. Thus we get the time complexity $O\left(k^2 2^k L^2\right)$, or $O\left(2^{(1+\nu)k} L^2\right)$

- To compute δ^-, we are not taking the maximum over anything. Essentially, we continually multiply prime factors of n, as we did in $\alpha^{\pm}$ and $\beta^{\pm}$, which gives us $O\left(kL^2\right)$.

- To compute $\varepsilon^{\pm}$, we compute all divisors of n, which gives us $O\left(k2^kL^2\right)$. The comparing and adding numbers gives us an extra 2^k term. The computation that dominates the computation of this lower bound is taking the maximum over 2^{2^k} numbers. Thus we get $O\left(k2^{2^k+2k}L^2\right)$, or $O\left(2^{(1+\nu)2^k}L^2\right)$

- To compute $\tilde{\varepsilon}^{\pm}$, the main operations we perform are to compute $\underline{n}$, sort $\underline{n}$, compare elements in $\underline{n}$ and add elements of $\underline{n}$. All of these combined gives us $O\left(k^22^{2k}L^2\right)$. Taking the maximum over 2^k elements gives us an extra 2^k factor in the complexity, so we end up with $O\left(k^22^{3k}L^2\right)$, or $O\left(2^{(3+\nu)k}L^2\right)$

3.5.2.1 $\alpha^{\pm}$

Recall

$$\alpha^{\pm}(n) = \max_{\substack{1\leq r<k \\ \rho(k-r)=\mp 1}} \left(p_r - \varphi(p_1\cdots p_{r-1})\right)$$

1. We compute $\varphi(p_1\cdots p_{r-1})$ for all $1 \leq r \leq k-1$. The following shows the computational time for each value of r.

r	$\varphi(p_1 \cdots p_{r-1})$	time to compute $\varphi(p_1 \cdots p_{r-1})$
1	1	0
2	$\varphi(p_1) = p_1 - 1$	0
3	$\varphi(p_1 p_2) = \varphi(p_1)(p_2 - 1)$	L^2
4	$\varphi(p_1 p_2 p_3) = \varphi(p_1 p_2)(p_3 - 1)$	$2L^2$
5	$\varphi(p_1 p_2 p_3 p_4) = \varphi(p_1 p_2 p_3)(p_4 - 1)$	$3L^2$
	$\cdots$	
$k-1$	$\varphi(p_1 \cdots p_{k-2}) = \varphi(p_1 \cdots p_{k-3})(p_{k-2} - 1)$	$(k-3)L^2$

For each value of r, we multiply $\varphi(p_1 \cdots p_{r-2})$, which has length $(r-2)L$, and $(p_{r-1} - 1)$, which has length L, so the time to compute $\varphi(p_1 \cdots p_{r-1})$ is $(r-2)L^2$.

Summing all of these, we get

$$\sum_{r=1}^{k-3} rL^2 = \frac{(k-3)(k-4)}{2} L^2 = O\left(k^2 L^2\right)$$

2. We subtract p_r and $\psi(p_1 \cdots p_{r-1})$. We assume that the largest length of two numbers we are subtracting is kL. Thus the subtraction will take $O(kL)$ time. Since we do this for all $1 \leq r \leq k-1$, in total, this will take $O\left(k^2 L\right)$ time.

3. We take the maximum over r. We assume that we have k things to take the maximum of, each with bit length kL. It will take $O\left(k^2 L\right)$ time to compute the maximum.

Combining all of the time complexities, we get that the complexity of computing $\alpha^{\pm}$ is $O\left(k^2 L^2\right)$.

3.5.2.2 $\beta^{\pm}$

$$\beta^{\pm}(n) = \max_{\substack{1 \le r < k \\ \rho(k-r) = \mp 1}} \left(\min \left\{ p_{r+1}, p_1 \cdots p_r \right\} - \psi(p_1 \cdots p_r) \right)$$

1. We compute $p_1 \cdots p_r$ and $\psi(p_1 \cdots p_r)$ for all $1 \le r \le k-1$. The following shows the computation time for each value of r. Recall that $\psi(n) = n - \varphi(n)$.

r	$p_1 \cdots p_r$	$\varphi(p_1 \cdots p_r)$	time to compute $\psi(p_1 \cdots p_r)$
1	p_1	$p_1 - 1$	0
2	$p_1 p_2$	$\varphi(p_1)(p_2 - 1)$	$L^2 + L^2 = 2L^2$
3	$p_1 p_2 p_3$	$\varphi(p_1 p_2)(p_3 - 1)$	$2L^2 + 2L^2 = 4L^2$
4	$p_1 p_2 p_3 p_4$	$\varphi(p_1 p_2 p_3)(p_4 - 1)$	$3L^2 + 3L^2 = 6L^2$
		$\cdots$	
$k-1$	$p_1 \cdots p_{k-1}$	$\varphi(p_1 \cdots p_{k-2})(p_{k-1} - 1)$	$(k-2)L^2 + (k-2)L^2 = 2(k-2)L^2$

   Summing all of these, we get

$$\sum_{r=1}^{k-2} 2rL^2 = 2\frac{(k-2)(k-3)}{2} L^2 = O\left(k^2 L^2\right)$$

2. We take the minimum of p_{r+1} and $p_1 \cdots p_r$. We have two things to take the maximum of and we assume that the largest length of the two is kL. Thus taking the maximum will take $O(kL)$ time. Since we do this for all $1 \le r \le k-1$, in total, this will be $O(k^2 L)$.

3. We subtract the minimum of p_{r+1} and $p_1 \cdots p_r$ and $\psi(p_1 \cdots p_r)$. We assume that the largest length of two numbers we are subtracting is kL. Thus the subtraction will be $O(kL)$. Since we do this for all $1 \le r \le k-1$, in total, this will be $O\left(k^2 L\right)$.

4. Finally, we take the maximum over all $1 \leq r \leq k-1$. We assume that we are taking the maximum of k numbers, each of which have length kL. This will be $O\left(k^2L\right)$.

Combining all of the time complexities, we see that the complexity of computing $\beta^{\pm}$ is $O\left(k^2L^2\right)$.

3.5.2.3 $\gamma^{\pm}$

$$\gamma^{\pm}(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(p_1 \cdots p_r - \sum_{\substack{d|n \\ \omega(d) < r}} \pm \mu\left(n/d\right)\ d \right)$$

1. We compute the divisors of n which is $O\left(k2^kL^2\right)$.

2. We order the divisors of n based on their number of prime factors. That is, we order all divisors with one prime factor, two prime factors, and so on. The time that takes is $O\left(k^22^kL\right)$.

3. We do the following operations for all $1 \leq r \leq k-1$

   (a) We compute $p_1 \cdots p_r$. This will not take any time since these numbers were already calculated when we found the divisors of n.

   (b) We find the alternating sum $\sum_{\substack{d|n \\ \omega(d) < r}} \mu\left(n/d\right)\ d$. We calculate this in the following manner: Consider the largest d such that $\mu(n/d) = +1$. Subtract divisors e of n such that $\mu(n/e) = -1$ up until the point where the difference would be less than zero. Note that the resulting number, call it s_1, will be less than n. Then add to s_1 the next largest number d such that $\mu(n/d) = +1$. Since $d < n$, the resulting sum will be less than $2n$. Again, subtract divisors e of n such that $\mu(n/e) = -1$ up until the point where the difference would be less than zero. Note that the resulting number, call it s_2, will be less than n. Then add to s_2 the next largest number d such that

$\mu(n/d) = +1$. Since $d < n$, the resulting sum will be less than $2n$. We continue adding and subtracting numbers in this manner until we have accounted for all divisors of n such that $\omega(d) < r$. In summary, what we have done is add and subtract numbers that are never larger than $2n$, and the number of additions and subtractions we perform is at most 2^k. The computational time of this is $O\left(2^k \cdot (2kL)\right)$, or $O\left(k2^k L\right)$.

4. We take the maximum over all $1 \leq r \leq k-1$. We assume that we are taking the maximum of k numbers, each of which have length kL. This will take $O\left(k^2 L\right)$.

Combining all of the time complexities, we get that the time to compute $\gamma^{\pm}$, $T_{\gamma^{\pm}}(k, L)$, is the following

$$\begin{aligned} T_{\gamma^{\pm}}(k, L) &= O\left(k2^k L^2 + k^2 2^k L + k(k2^k L) + k^2 L\right) \\ T_{\gamma^{\pm}}(k, L) &= O\left(k^2 2^k L^2\right) \\ T_{\gamma^{\pm}}(k, L) &= O\left(2^{(1+\nu)k} L^2\right) \end{aligned}$$

for some $\nu > 0$.

3.5.2.4 δ^-

$$\delta^-(n) = 2\frac{n}{p_1} - \psi(n)$$

In order to compute $\frac{n}{p_1} = p_2 \cdots p_k$, we need to compute p_2, $p_2 p_3$, $p_2 p_3 p_4$ and so on. In order to compute $\psi(n)$, we need to compute $\varphi(p_1)$, $\varphi(p_1 p_2)$, $\varphi(p_1 p_2 p_3)$ and so on. We analyze the time these take to compute in the following:

r	$p_2 \cdots p_r$	$\varphi(p_1 \cdots p_r)$	time to compute $p_2 \cdots p_r$ and $\psi(p_1 \cdots p_r)$
1		$\varphi(p_1)$	0
2	p_2	$\varphi(p_1 p_2)$	$0 + L^2 = L^2$
3	$p_2 p_3$	$\varphi(p_1 p_2)(p_3 - 1)$	$L^2 + 2L^2 = 3L^2$
4	$p_2 p_3 p_4$	$\varphi(p_1 p_2 p_3)(p_4 - 1)$	$2L^2 + 3L^2 = 5L^2$
		$\cdots$	
k	$p_2 \cdots p_k$	$\varphi(p_1 \cdots p_{k-1})(p_k - 1)$	$(k-2)L^2 + (k-1)L^2 = (2(k-1)-1)L^2$

Summing all of the computational times, we get

$$\sum_{r=2}^{k-1} \left(2(r-1)-1\right) L^2 = (k-2)^2 L^2 = O\left(k^2 L^2\right)$$

Therefore, the complexity of computing δ^- is $O\left(k^2 L^2\right)$.

3.5.2.5 $\varepsilon^{\pm}$

$$\varepsilon^{\pm}(n) = \max_{\substack{B \subsetneq \underline{n} \setminus \{n\} \\ \mathcal{C}^{\pm}(B)}} \left(\min\left(\underline{n} \setminus \{n\} \setminus B\right) \; - \; \sum_{d \in B} \pm\mu\left(n/d\right) \; d \right)$$

1. We compute $\underline{n}$. The number of computations will be $O\left(k 2^k L^2\right)$. Recall that when we compute $\underline{n}$, we also compute a graph showing the divisor relationships between the elements in $\underline{n}$.

2. We consider all proper subsets B of $\underline{n} \setminus \{n\}$. There are $2^{2^k - 1}$ such sets.

   (a) We check the condition $\mathcal{C}^{\pm}(B)$. Recall that to check this, for every element in $\underline{B}$ we need to see how many elements in $B^{\pm}$ and $B^{\mp}$ are multiples of that element. Since we already computed the graph of divisor relations, we do not need to do any

arithmetic at this step. We iterate through the graph, only looking at edges. Thus this requires at most 2^k operations, and we do this for every element in B, which will at most be 2^k, so the time complexity at this step is $O\left(2^k 2^k\right)$, or $O\left(2^{2k}\right)$.

(b) We find $\min\left(\underline{n} \setminus \{n\} \setminus B\right)$. We need to make at most 2^k comparisons of numbers with length at most kL. Thus this will be $O\left(k2^k L\right)$.

(c) We consider now the alternating sum of elements in B. The number of computations to compute this is the number of computations it takes to add all the elements of B. As a worst case scenario, assume $\#B = \#\underline{n} = 2^k$, and the length of each number is kL. Thus we are adding 2^k numbers, each with length kL. By Lemma 2.2, the time to compute this will be $O\left(k2^k L + 2^{2k}\right)$.

3. We now take the maximum of 2^{2^k-1} numbers, each of which has length at most kL. This is $O\left(k2^{2^k-1}L\right)$.

Combining all of the above computations, we get that the time to compute $\varepsilon^{\pm}$, $T_{\varepsilon^{\pm}}(k, L)$ is the following:

$$
\begin{aligned}
T_{\varepsilon^{\pm}}(k,L) &= O\left(k2^k L^2 + 2^{2^k-1}\left(2^{2k} + k2^k L + k2^k L + 2^{2k}\right) + k2^{2^k-1}L\right) \\
T_{\varepsilon^{\pm}}(k,L) &= O\left(k2^k L^2 + 2^{2^k+2k} + k2^{2^k+k}L + k2^{2^k+k}L + 2^{2^k+2k} + k2^{2^k-1}L\right) \\
T_{\varepsilon^{\pm}}(k,L) &= O\left(k2^k L^2 + 2^{2^k+2k} + k2^{2^k+k}L\right) \\
T_{\varepsilon^{\pm}}(k,L) &= O\left(k2^{2^k+2k}L^2\right) \\
T_{\varepsilon^{\pm}}(k,L) &= O\left(2^{(1+\nu)2^k}L^2\right)
\end{aligned}
$$

for some $\nu > 0$. Therefore, the complexity of computing $\varepsilon^{\pm}$ is $O\left(2^{(1+\nu)2^k}L^2\right)$.

3.5.2.6 $\tilde{\varepsilon}^{\pm}$

Let $A_b = \{a \in A \ : \ a < b\}$.

$$\tilde{\varepsilon}^{\pm}(n) = \max_{\substack{b \in \underline{n}^{\pm} \\ B = \underline{n}_b^{\pm} \cup (\underline{n}_b^{\pm})^{\mp} \\ \mathcal{C}^{\pm}(B)}} \left(\min\left(\underline{n} \setminus \{n\} \setminus B\right) - \sum_{d \in B} \pm\mu\left(n/d\right) \ d \right)$$

1. We compute $\underline{n}$, which is $O\left(k2^k L^2\right)$.
2. We sort $\underline{n}$, which is $O\left(k^2 2^k L\right)$.
3. Note that we have to do the following operations 2^{k-1} times.
   (a) We consider the time it takes to compute B, given b.
      i. First we consider all elements in $\underline{n}^{\pm}$ that are less than b. To do this, we iterate through $\underline{n}^{\pm}$, and check if we have reached b. In the worst case, we will have to iterate through all elements of $\underline{n}^{\pm}$, which is 2^{k-1}. This requires at most 2^{k-1} operations, each taking kL. Thus, the time complexity is $O\left(2^{k-1}kL\right)$, or $O\left(k2^k L\right)$.
      ii. Then we consider the set of divisors of those elements, but only those that are in $\underline{n}^{\mp}$. Since we have already computed the graph of divisor relations, we do not need to do any arithmetic at this step. We iterate through the graph, only looking at edges from b. Thus this requires at most 2^{k-1} operations, so the time complexity at this step is $O\left(2^{k-1}\right)$, or $O\left(2^k\right)$.
   (b) We consider now checking the condition $\mathcal{C}^{\pm}(B)$. Recall that to check this, for every element in $\underline{B}$ we need to see how many elements in $B^{\pm}$ and $B^{\mp}$ are multiples of that element. Since we already computed the graph of divisor relations, we do not need to do any arithmetic at this step. We iterate through the graph, only looking

at edges. Thus this requires at most 2^k operations, and we do this for every element in B, which will at most be 2^k, so the time complexity at this step is $O\left(2^k 2^k\right)$, or $O\left(2^{2k}\right)$.

(c) We consider now finding $\min\left(\underline{n} \setminus \{n\} \setminus B\right)$. Note that when we found B, we could have also found $\min\left(\underline{n} \setminus \{n\} \setminus B\right)$ without increasing the time complexity. Thus we have a sorted set, and to find the minimum we simply need to look at the first element. This will not take any time to do.

(d) We consider now the alternating sum of elements in B. The number of computations to compute this is the number of computations it takes to add all the elements of B. As a worst case scenario, assume $\#B = \#\underline{n} = 2^k$, and the length of each number is kL. Thus we are adding 2^k numbers, each with length kL. By Lemma 2.2, the time to compute will be $O\left(k2^k L + 2^{2k}\right)$.

4. We then take the maximum of 2^{k-1} numbers, each with length at most kL. This is $O\left(k2^k L\right)$.

Combining all of the above computations, we get that the time to compute $\tilde{\varepsilon}^{\pm}$, $T_{\tilde{\varepsilon}^{\pm}}(k, L)$, is given by the following

$$
\begin{aligned}
T_{\tilde{\varepsilon}^{\pm}}(k,L) &= O\left(k2^k L^2 + k^2 2^k L + 2^{k-1}\left(k2^k L + 2^k + 2^{2k} + k2^k L + 2^{2k}\right) + k2^k L\right) \\
T_{\tilde{\varepsilon}^{\pm}}(k,L) &= O\left(k2^k L^2 + k^2 2^k L + k2^{2k} L + 2^{2k} + 2^{3k} + k2^{2k} L + 2^{3k} + k2^k L\right) \\
T_{\tilde{\varepsilon}^{\pm}}(k,L) &= O\left(k2^k L^2 + k^2 2^k L + k2^{2k} L + 2^{3k}\right) \\
T_{\tilde{\varepsilon}^{\pm}}(k,L) &= O\left(k^2 2^{3k} L^2\right) \\
T_{\tilde{\varepsilon}^{\pm}}(k,L) &= O\left(2^{(3+\nu)k} L^2\right)
\end{aligned}
$$

for some $\nu > 0$. Therefore, the complexity of computing $\tilde{\varepsilon}^{\pm}$ is $O\left(2^{(3+\nu)k} L^2\right)$.

Chapter 4

Exact Cyclotomic

In this chapter, we present a conjecture for an exact expression for $g(\Phi_n)$, along with supporting evidence that the conjecture is true for infinitely many families of n. We then prove the conjecture in a specific case of the ternary cyclotomic polynomial.

Introduction

Consider Figure 4.1 below, which shows plots of $g(\Phi_n)$ where $n = mp$, m is fixed and p is an odd prime.

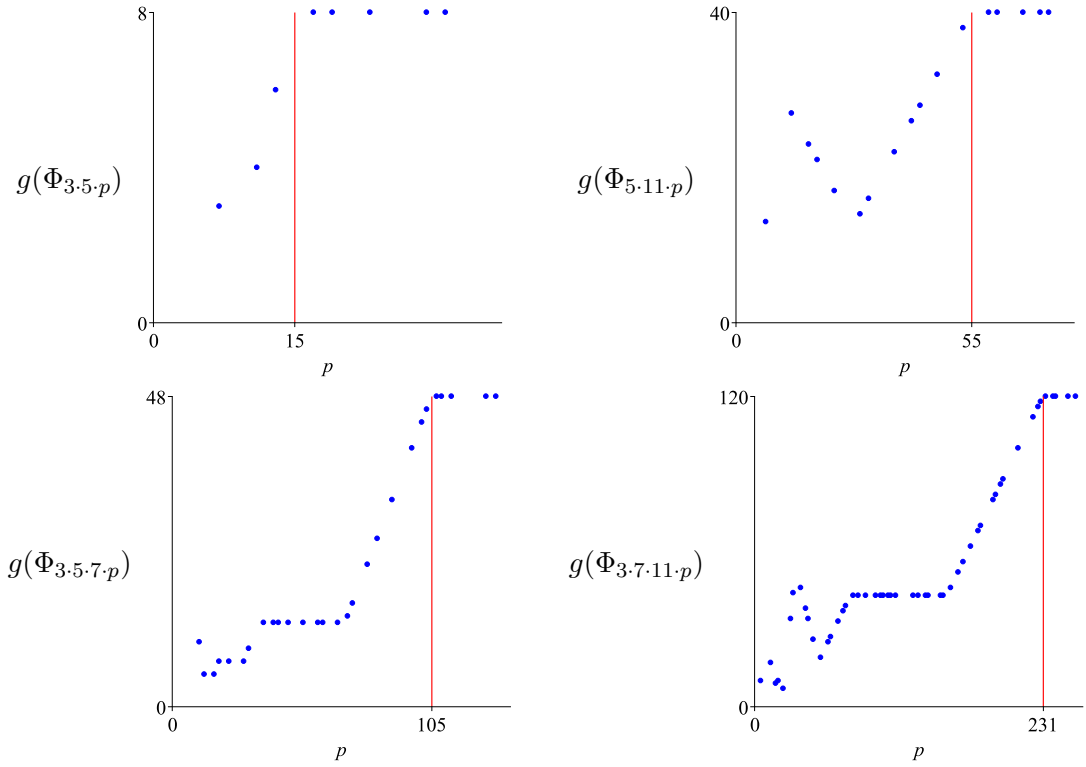


Figure 4.1 Plots of $g(\Phi_{mp})$ for various values of m

An immediate observation in all these plots is that when $p > m$, we have $g(\Phi_{mp}) = \varphi(m)$. After studying these and many more plots, we conjectured that $g(\Phi_{p_1 \cdots p_k}) = \varphi(p_1 \cdots p_{k-1})$ if and only if $p_k > p_1 \cdots p_{k-1}$ (Conjecture 4.1). It is a natural generalization of the result in [23]: $g(\Phi_{p_1 p_2}) = p_1 - 1 = \varphi(p_1)$. The conjecture has been already verified for $m = p_1 \cdots p_{k-1} < 1000$ and arbitrary p_k (Theorem 4.3). The verification technique is based on a structural result that $g(\Phi_{mp_k})$ only depends on m and $\mathrm{rem}(p_k, m)$ (Theorem 4.2). Thus, given m, we only need to check finitely many p_k values in order to check the conjecture for infinitely many p_k. We organized it into an algorithm (Algorithm 4.1) and ran it for all odd square-free $m < 1000$.

We prove the conjecture for a specific case of the ternary cyclotomic polynomial. Given

$n = p_1p_2p_3$ where $p_3 \equiv_{p_1p_2} +1$ and $p_2 \equiv_{p_1} \pm 1$, we prove that $g(\Phi_{p_1p_2p_3}) = \varphi(p_1p_2)$. This class of the ternary cyclotomic polynomials is of particular interest because it is flat; that is, their largest coefficient is no more than 1 in magnitude.

4.1 Main Results

Conjecture 4.1 (Equivalent condition on $g(\Phi_n)$)**.** *We have*

$$g(\Phi_n) = \varphi(p_1 \cdots p_{k-1}) \quad \textit{if and only if} \quad p_k > p_1 \cdots p_{k-1}$$

Theorem 4.1 (Exact formula in certain ternary cyclotomic case)**.** *We have*

$$g(\Phi_{p_1p_2p_3}) = \varphi(p_1p_2)$$

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

4.2 Evidence for equivalent condition on $g(\Phi_n)$

Note that the conjecture is trivially true for $k = 1$. In [23], the conjecture is proved for $k = 2$. For $k \geq 3$ the conjecture is still open. One way to check (support or disprove) the conjecture is to compute Φ_n for many n with $k \geq 3$ and to check whether the maximum gap is $\varphi(p_1 \cdots p_{k-1})$ or not. We did this for n up to $40,000$, without finding any counter-example. However, this method only shows that the conjecture is true for finitely many such n.

In this section, we will describe an algorithm (Algorithm 4.1) which allows the conjecture to be checked for infinitely many such n and we will report that we have done so (Theorem 4.3). For the sake of notational simplicity, let $m = p_1 \cdots p_{k-1}$ and $p = p_k$. Then the above conjecture can be restated as: $g(\Phi_{mp}) = \varphi(m)$ if and only if $p > m$. The algorithm (which will be given

later) is based on the following theorem.

Theorem 4.2 (Invariance)**.** *Let m be odd square-free. Let $p, p' > m$ be primes such that $p \equiv_m p'$. Then*

$$g(\Phi_{mp}) = g(\Phi_{mp'})$$

Proof. Let m be odd square-free. Let $p > m$ be prime. We will divide the proof into several steps.

1. Let $q = \operatorname{quo}(p, m)$ and $r = \operatorname{rem}(p, m)$. Let

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

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

   We recall the following results from [1]: For all $0 \le i \le \varphi(m) - 1$, we have

   (C1) $f_{m,p,i,0} = \cdots = f_{m,p,i,q-1}$

   (C2) $f_{m,p,i,q} = \operatorname{rem}(f_{m,p,i,0}, x^r)$

   (C3) $f_{m,p,i,0} = f_{m,p',i,0}$ if $p \equiv_m p'$

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

$$g(\Phi_{mp}) = \max\left\{ \max_{0 \le i \le \varphi(m)-1} g(f_{m,p,i}),\ \max_{0 \le i \le \varphi(m)-2} (p + \operatorname{tdeg}(f_{m,p,i+1}) - \deg(f_{m,p,i})) \right\} \tag{4.1}$$

3. From $f_{m,p,i} = \sum_{j=0}^{q} f_{m,p,i,j} x^{jp}$ and (C1) and (C2), we have

$$\begin{aligned} g(f_{m,p,i}) &= \max\{g(f_{m,p,i,0}),\ g(f_{m,p,i,q}),\ m + \operatorname{tdeg}(f_{m,p,i,0}) - \deg(f_{m,p,i,0})\} \\ &= \max\{g(f_{m,p,i,0}),\ m + \operatorname{tdeg}(f_{m,p,i,0}) - \deg(f_{m,p,i,0})\} \end{aligned} \tag{4.2}$$

4. From $p - qm = r$, we have

$$p + \mathrm{tdeg}(f_{m,p,i+1}) - \deg(f_{m,p,i}) = \begin{cases} p + \mathrm{tdeg}(f_{m,p,i+1,0}) - ((q-1)m + \deg(f_{m,p,i,0})) & \text{if } f_{m,p,i,q} = 0 \\ p + \mathrm{tdeg}(f_{m,p,i+1,0}) - (qm + \deg(f_{m,p,i,q})) & \text{else} \end{cases}$$
$$= \begin{cases} r + m + \mathrm{tdeg}(f_{m,p,i+1,0}) - \deg(f_{m,p,i,0}) & \text{if } f_{m,p,i,q} = 0 \\ r + \mathrm{tdeg}(f_{m,p,i+1,0}) - \deg(\mathrm{rem}\,(f_{m,p,i,0}, x^r)) & \text{else} \end{cases} \tag{4.3}$$

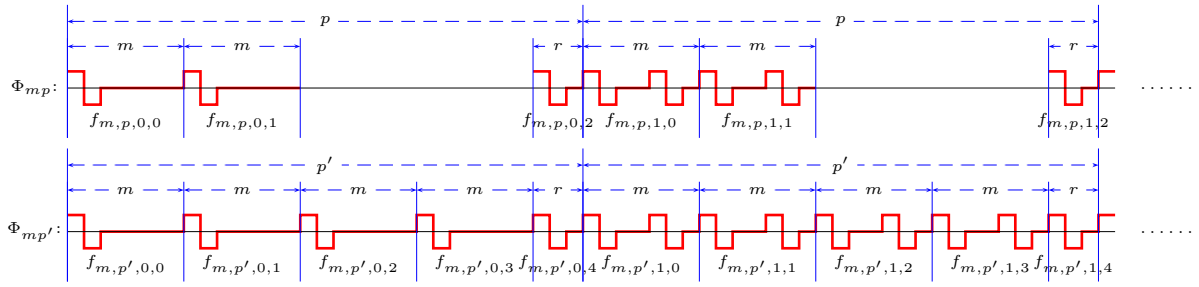
5. Combining the equalities (4.1), (4.2) and (4.3), we see $g(\Phi_{mp})$ depends *only on* m, r and $f_{m,p,i,0}$.

6. Let $p' > m$ be a prime other than p. Then $g(\Phi_{mp'})$ also depends *only on* m, r' and $f_{m,p',i,0}$.

7. Suppose $p \equiv_m p'$. Then obviously $r = r'$. Furthermore from (C3), we have $f_{m,p,i,0} = f_{m,p',i,0}$. Thus $g(\Phi_{mp}) = g(\Phi_{mp'})$.

□

The above proof can be visualized in the following example: We visualize a polynomial by a graph where the horizonal axis stands for the exponents and the vertical axis stands for the corresponding coefficients. Let $m = 7$, $p = 17$ and $p' = 31$. Then $\varphi(m) - 1 = 6$, $q = 2$, $q' = 4$ and $r = 8$. The partition of the coefficients of Φ_{mp} and $\Phi_{mp'}$ into $f_{m,p,i,j}$'s is illustrated by the following diagram. Note that the space in Φ_{mp} with no red line serves the purpose of aligning the two polynomials; it does not represent a gap in the exponents.



We observe the following characteristics in the above diagram, as expected from the results in [1]:

(C1) $f_{m,p,i,0} = \cdots = f_{m,p,i,q-1}$

(C2) $f_{m,p,i,q} = \mathrm{rem}(f_{m,p,i,0}, x^r)$

(C3) $f_{m,p,i,0} = f_{m,p',i,0}$

After considering the diagram and these properties, we see visually why it is true that $g(\Phi_{mp}) = g(\Phi_{mp'})$.
From the above theorem (Theorem 4.2) we immediately obtain the following algorithm.

Algorithm 4.1 (Checking the conjecture)**.**

In: *m, odd square-free, say $m = p_1 \cdots p_{k-1}$ and $p_1 < \cdots < p_{k-1}$*

Out: *truth of the claim that* $\underset{prime\ p > p_{k-1}}{\forall} [\ g(\Phi_{mp}) = \varphi(m) \iff p > m\ ]$

1. *for p from $p_{k-1}+1$ to $m-1$, p prime, do*

   (a) $F \leftarrow \Phi_{mp}$

   (b) $g \leftarrow$ *the maximum gap of* F

   (c) *if* $g = \varphi(m)$ *then return false*

2. *for r from 1 to $m-1$, where* $\gcd(m, r) = 1$*, do*

   (a) $p \leftarrow$ *the smallest prime larger than m such that* $\mathrm{rem}(m, p) = r$

   (b) $F \leftarrow \Phi_{mp}$

   (c) $g \leftarrow$ *the maximum gap of* F

(d) if $g \neq \varphi(m)$ then return false

3. return true

We have implemented the above algorithm in C language. The cyclotomic polynomials were computed using the algorithm called Sparse Power Series (Algorithm 4 in [2]) because it is the fastest known algorithm for inputs where p is not very big compared to m. The code for the algorithm has been kindly provided by Andrew Arnold, one of the authors of [2]. By executing the program, so far we have proved the following.

Theorem 4.3 (Evidence of the conjecture for infinitely many primes)**.** *For all primes p and $m < 1000$, we have*

$$g(\Phi_{mp}) = \varphi(m) \quad \textit{if and only if} \quad p > m$$

In other words, for all k and for all $p_1, \ldots, p_k$ such that $p_1 \cdots p_{k-1} < 1000$, we have

$$g(\Phi_{p_1 \cdots p_k}) = \varphi(p_1 \cdots p_{k-1}) \quad \textit{if and only if } p_k > p_1 \cdots p_{k-1}.$$

The above computation took 86 minutes on a MacBook Pro (CPU: 2.4 GHz Intel Core i5, Memory: 16 GB 1600 MHz DDR3). Of course, one could continue to check larger m values using larger computing resources.

4.3 Proof

The proof of Theorem 4.1 is structured as follows:

1. In Theorem 4.4, we state an important theorem on the structure of the ternary cyclotomic polynomial found in [1]

2. In Lemma 4.1 we use Theorem 4.4 to break down $g(\Phi_{p_1 p_2 p_3})$ into the maximum of two parts

3. In Subsections 4.3 and 4.3, we prove that each of the parts is less than or equal to $\varphi(p_1p_2)$

4. In Subsection 4.3, we prove Theorem 4.1

We recall the following result due to [1], which we presented in Chapter 2, Theorem 2.13.

Theorem 4.4 (Structure Theorem)**.** *Let* $p_3 \equiv_{p_1p_2} +1$ *and* $p_2 \equiv_{p_1} \pm 1$*. We have*

$$\Phi_n(x) = \sum_{a=0}^{\varphi(p_1p_2)-1} f_a(x)\, x^{ap_3} \qquad \deg f_a < p_3$$

$$f_a(x) = \sum_{b=0}^{q_3} f_{a,b}(x)\, x^{bp_1p_2} \qquad \deg f_{a,b} < p_1p_2$$

$$f_{a,0}(x) = \cdots = f_{a,q_3-1}(x)$$

$$= \begin{cases} +A(x) & & -x^{p_2}A(x) & & \text{if } a = 0 \\ +B(x) & -x^{(u+1)p_2-a} & -x^{p_2}B(x) & +x^{p_1p_2-a} & \text{if } a > 0,\ w \le u \text{ and } \neg\mathcal{D}(a) \\ +C(x) & & -x^{p_2}B(x) & +x^{p_1p_2-a} & \text{if } a > 0,\ w \le u \text{ and } \mathcal{D}(a) \\ -D(x) & -x^{(u+1)p_2-a} & +x^{p_2}D(x) & +x^{p_1p_2-a} & \text{if } a > 0,\ w > u \text{ and } \neg\mathcal{D}(a) \\ -x^{(u+1)p_2-a} & -D(x) & +x^{p_2}D(x) & +x^{p_1p_2-a} & \text{if } a > 0,\ w > u \text{ and } \mathcal{D}(a) \end{cases}$$

$$f_{a,q_3}(x) = \begin{cases} 1 & \text{if } a = 0 \\ 0 & \text{if } a > 0 \end{cases}$$

where

$$A(x) = \sum_{k=0}^{p_1-1} x^k, \qquad B(x) = \sum_{k=u+1-w}^{p_1-1-w} x^k, \qquad C(x) = \sum_{k=u+1-w}^{p_1-2-w} x^k, \qquad D(x) = \sum_{k=p_1-w}^{p_1+u-w} x^k$$

$$u := \operatorname{quo}(a, \overline{p_2})$$

$$v := \operatorname{quo}(\operatorname{rem}(a, \overline{p_2}), p_1)$$

$$w := \operatorname{rem}(\operatorname{rem}(a, \overline{p_2}), p_1)$$

$$q_3 := \operatorname{quo}(p_3, p_1p_2)$$

$$\overline{p_2} := \begin{cases} p_2 - 1 & \text{if } p_2 \equiv_{p_1} +1 \\ p_2 & \text{if } p_2 \equiv_{p_1} -1 \end{cases}$$

$$\mathcal{D}(a) :\Leftrightarrow p_2 \equiv_{p_1} -1 \ \wedge \ v = q_2$$

In the following lemma, we break down $g(\Phi_{p_1p_2p_3})$ based off of the previous theorem.

Lemma 4.1. *We have*

$$g(\Phi_{p_1p_2p_3}) = \max\left\{ \max_{0\le a\le h} \left\{ g(f_a),\, p_3 + \operatorname{tdeg}(f_{a+1}) - \deg(f_a) \right\} \right\}$$

where $h = \frac{\varphi(p_1p_2)}{2}$.

Proof. By Theorem 4.4, we have

$$\begin{aligned} g\left(\Phi_{p_1p_2p_3}\right) &= g\left(\sum_{a=0}^{\varphi(p_1p_2)-1} f_a x^{ap_3} \right) \\ &= \max\left\{ \max_{0\le a\le \varphi(p_1p_2)-1} g(f_{p_1p_2,p_3,a}),\ \max_{0\le a\le \varphi(p_1p_2)-2} \left\{ p_3 + \operatorname{tdeg}(f_{a+1}) - \deg(f_a) \right\} \right\} \end{aligned}$$

Since

$$\begin{aligned} \deg(x^{hp_3} f_h) &= hp_3 + \deg(f_h) \\ &= \frac{\varphi(p_1p_2)}{2} p_3 + \deg(f_h) \\ &> \frac{\varphi(p_1p_2p_3)}{2} \end{aligned}$$

and since $\Phi_{p_1p_2p_3}$ is symmetric, we have the following equality

$$g(\Phi_{p_1p_2p_3}) = g\left(\sum_{a=0}^{h} f_a x^{ap_3}\right)$$

Thus we have

$$g(\Phi_{p_1p_2p_3}) = \max\left\{\max_{0\le a\le h}\left\{g(f_a),\, p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)\right\}\right\}$$

which proves the lemma. □

Therefore, in order to prove $g(\Phi_{p_1p_2p_3}) = \varphi(p_1p_2)$, we will show the following:

(G1) $\max\limits_{0\le a\le h} g(f_a) = \varphi(p_1p_2)$

(G2) $\max\limits_{0\le a\le h} (p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)) \le \varphi(p_1p_2)$

The following lemmas will be used to prove both parts.

Lemma 4.2. *We have*

$$\deg(f_{a,0}) = \begin{cases} p_2(p_1-1) & \text{if } a = 0 \\ p_1p_2 - a & \text{if } a > 0 \end{cases}$$

$$\mathrm{tdeg}(f_{a,0}) = \begin{cases} u+1-w & \text{if } a>0 \text{ and } w \le u \\ p_1 - w & \text{if } a>0 \text{ and } w > u \text{ and } \neg\mathcal{D}(a) \\ (u+1)p_2 - a & \text{if } a>0 \text{ and } w > u \text{ and } \mathcal{D}(a) \end{cases}$$

Proof. Obvious from Theorem 4.4. □

Lemma 4.3. *We have*

$$f_{0,0} = -\Psi_{p_1p_2}$$

$$f_{1,0} = -x^{p_1-1} - x^{p_2-1} + x^{p_1+p_2-1} + x^{p_1p_2-1}$$

Proof. If $a = 0$, then by Theorem 4.4 we have

$$\begin{aligned} f_{a,0} &= \sum_{k=0}^{p_1-1} x^k - x^{p_2} \sum_{k=0}^{p_1-1} x^k \\ &= -\Psi_{p_1p_2} \end{aligned}$$

If $a = 1$, then $u = 0$ and $w = 1$, so by Theorem 4.4 we have

$$\begin{aligned} f_{1,0} &= -\sum_{k=p_1-1}^{p_1-1} x^k - x^{(1)p_2-1} + x^{p_2} \sum_{k=p_1-1}^{p_1-1} x^k + x^{p_1p_2-1} \\ &= -x^{p_1-1} - x^{p_2-1} + x^{p_1+p_2-1} \end{aligned}$$

which proves the lemma. □

Lemma 4.4. *We have that $u \leq p_1 - 2$ for all $1 \leq a \leq h + 1$.*

Proof. Note

$$u = \begin{cases} \text{quo}(a, p_2 - 1) & \text{if } p_2 \equiv_{p_1} +1 \\ \text{quo}(a, p_2) & \text{if } p_2 \equiv_{p_1} -1 \end{cases}$$

In both cases, $u \leq \frac{a}{p_2-1}$. Thus we observe the following

1. $a \leq \dfrac{\varphi(p_1p_2)}{2} + 1$
2. $u \leq \dfrac{a}{p_2 - 1}$
3. $\frac{1}{2}(p_1 - 1) \leq p_1 - 2$

By (1) and (2), we have $u \leq \frac{1}{2}(p_1 - 1) + \frac{1}{p_2-1}$. Since u is an integer, $u \leq \frac{1}{2}(p_1 - 1)$. Then by (3), we have $u \leq p_1 - 2$. □

Proof of G1

Lemma 4.5 (G1)**.** *We have*

$$\max_{0\le a\le h} g(f_a) = \varphi(p_1p_2)$$

Before we can prove this, we first need to prove several other lemmas.

Lemma 4.6. *We have*

$$g(f_a) = \begin{cases} \varphi(p_1p_2) & \text{if } a = 0 \\ \max\left\{g(f_{a,0}),\, p_1p_2 + \operatorname{tdeg}(f_{a,0}) - \deg(f_{a,0})\right\} & \text{if } 1 \le a \le h \end{cases}$$

Proof. By Theorem 4.4, we have

$$\begin{aligned} g\left(f_a\right) &= g\left(\sum_{j=0}^{q_3} f_{a,j}x^{jp_1p_2}\right) \\ &= \max\left\{g(f_{a,0}),\, g(f_{a,q_3}),\, p_1p_2 + \operatorname{tdeg}(f_{a,0}) - \deg(f_{a,0})\right\} \\ &= \max\left\{g(f_{a,0}),\, p_1p_2 + \operatorname{tdeg}(f_{a,0}) - \deg(f_{a,0})\right\} \end{aligned}$$

From Lemma 4.3 we have $f_{0,0} = -\Psi_{p_1p_2}$, so

$$\begin{aligned} g(f_0) &= \max\left\{g(f_{0,0}),\, p_1p_2 + \operatorname{tdeg}(f_{0,0}) - \deg(f_{0,0})\right\} \\ &= \max\left\{p_2 - p_1 + 1,\, p_1p_2 + 0 - \psi(p_1p_2))\right\} \\ &= \max\left\{p_2 - p_1 + 1,\, \varphi(p_1p_2)\right\} \\ &= \varphi(p_1p_2) \end{aligned}$$

which proves the lemma.

□

By Lemma 4.6 we see that in order to prove Lemma 4.5, we must prove the following:

(G1-a) $\max_{1\le a\le h} g(f_{a,0}) \le \varphi(p_1p_2)$

(G1-b) $\max_{1\le a\le h} (p_1p_2 + \mathrm{tdeg}(f_{a,0}) - \deg(f_{a,0})) \le \varphi(p_1p_2)$

Lemma 4.7 (G1-a)**.** *We have*

$$\max_{1\le a\le h} g(f_{a,0}) \le \varphi(p_1p_2)$$

Proof. We break the proof into four cases, and prove the lemma for each.

1. Case: $w \le u$ and $\neg\mathcal{D}(a)$. By Theorem 4.4 we have

$$f_{a,0} = \sum_{k=u+1-w}^{p_1-1-w} x^k - x^{(u+1)p_2-a} - x^{p_2} \sum_{k=u+1-w}^{p_1-1-w} x^k + x^{p_1p_2-a}$$

Thus

$$\begin{aligned} g(f_{a,0}) &= \max\big\{(u+1)p_2 - a - (p_1 - 1 - w), \\ &\qquad p_2 + u + 1 - w - ((u+1)p_2 - a), \\ &\qquad p_1p_2 - a - (p_2 + p_1 - 1 - w)\big\} \\ &= \max\big\{up_2 + p_2 + w + 1 - a - p_1, \\ &\qquad u + a + 1 - w - up_2, \\ &\qquad p_1p_2 + w + 1 - a - p_2 - p_1\big\} \end{aligned}$$

We have

$$\begin{aligned} up_2 + p_2 + w + 1 - a - p_1 &= up_2 + p_2 + w + 1 - (u\overline{p_2} + vp_1 + w) - p_1 \\ &= u(p_2 - \overline{p_2}) + p_2 - p_1(v+1) + 1 \\ &\le u + p_2 + 1 \qquad \text{since } p_2 - \overline{p_2} \le 1 \end{aligned}$$

$$\begin{aligned} &\leq p_1 + p_2 - 1 && \text{by Lemma 4.4} \\ &\leq \varphi(p_1 p_2) \end{aligned}$$

$$\begin{aligned} u + a + 1 - w - up_2 &\leq u + a + 1 && \text{by Lemma 4.4} \\ &\leq p_1 - 1 + a \\ &\leq \varphi(p_1 p_2) && \text{since } a \leq \tfrac{\varphi(p_1 p_2)}{2} \end{aligned}$$

$$p_1 p_2 + w + 1 - a - p_2 - p_1 \leq \varphi(p_1 p_2) \qquad \text{since } w \leq a$$

2. Case: $w > u$ and $\neg\mathcal{D}(a)$. By Theorem 4.4 we have

$$f_{a,0} = -\sum_{k=p_1-w}^{p_1+u-w} x^k - x^{(u+1)p_2-a} + x^{p_2} \sum_{k=p_1-w}^{p_1+u-w} x^k + x^{p_1 p_2 - a}$$

Thus

$$\begin{aligned} g(f_{a,0}) &= \max\big\{(u+1)p_2 - a - (p_1 + u - w), \\ &\qquad p_2 + p_1 - w - ((u+1)p_2 - a), \\ &\qquad p_1 p_2 - a - (p_2 + p_1 + u - w)\big\} \\ &= \max\big\{up_2 + p_2 + w - u - a - p_1, \\ &\qquad a + p_1 - w - up_2, \\ &\qquad p_1 p_2 + w - a - u - p_2 - p_1\big\} \end{aligned}$$

We have

$$up_2 + p_2 + w - a - p_1 = up_2 + p_2 + w - (u\overline{p_2} + vp_1 + w) - p_1$$

$$
\begin{aligned}
&= u(p_2 - \overline{p_2}) + p_2 - p_1(v+1) \\
&\le u + p_2 && \text{since } p_2 - \overline{p_2} \le 1 \\
&\le p_1 + p_2 - 2 && \text{by Lemma 4.4} \\
&\le \varphi(p_1 p_2)
\end{aligned}
$$

$$
\begin{aligned}
a + p_1 - w - up_2 &\le a + p_1 \\
&\le \varphi(p_1 p_2)
\end{aligned}
$$

$$
p_1 p_2 + w - a - u - p_2 - p_1 \le \varphi(p_1 p_2) \qquad \text{since } w \le a
$$

3. Case: $w \le u$ and $\mathcal{D}(a)$. By Theorem 4.4 we have

$$
f_{a,0} = \sum_{k=u+1-w}^{p_1-2-w} x^k - x^{p_2} \sum_{k=u+1-w}^{p_1-1-w} x^k + x^{p_1 p_2 - a}
$$

Thus

$$
\begin{aligned}
g(f_{a,0}) &= \max\big\{p_2 + u + 1 - w - (p_1 - 2 - w), \\
&\qquad p_1 p_2 - a - (p_2 + p_1 - 1 - w)\big\} \\
&= \max\big\{p_2 + u + 3 - p_1, \\
&\qquad p_1 p_2 + w + 1 - a - p_2 - p_1\big\}
\end{aligned}
$$

We have

$$
\begin{aligned}
p_2 + u + 3 - p_1 &\le p_2 + p_1 + 1 \\
&\le \varphi(p_1 p_2)
\end{aligned}
$$

$$p_1p_2 + w + 1 - a - p_2 - p_1 \leq \varphi(p_1p_2) \qquad \text{since } w \leq a$$

4. Case: $w > u$ and $\mathcal{D}(a)$. By Theorem 4.4 we have

$$f_{a,0} = -x^{(u+1)p_2-a} - \sum_{k=p_1-w}^{p_1+u-w} x^k + x^{p_2} \sum_{k=p_1-w}^{p_1+u-w} x^k + x^{p_1p_2-a}$$

Thus

$$\begin{aligned} g(f_{a,0}) &= \max\big\{p_1 - w - ((u+1)p_2 - a), \\ &\qquad p_2 + p_1 - w - (p_1 + u - w), \\ &\qquad p_1p_2 - a - (p_2 + p_1 + u - w)\big\} \\ &= \max\big\{a + p_1 - w - up_2 - p_2, \\ &\qquad p_2 - u, \\ &\qquad p_1p_2 + w - a - u - p_2 - p_1\big\} \end{aligned}$$

We have

$$\begin{aligned} a + p_1 - w - up_2 - p_2 &\leq a + p_1 \\ &\leq \varphi(p_1p_2) \end{aligned}$$

$$\begin{aligned} p_2 - u &\leq p_2 \\ &\leq \varphi(p_1p_2) \end{aligned}$$

$$p_1p_2 + w - a - u - p_2 - p_1 \leq \varphi(p_1p_2) \qquad \text{since } w \leq a$$

Therefore, in all four cases we have shown that $g(f_{a,0}) \leq \varphi(p_1p_2)$, which proves the lemma. □

Lemma 4.8 (G1-b)**.** *We have*

$$\max_{1\leq a\leq h} (p_1p_2 + \mathrm{tdeg}(f_{a,0}) - \deg(f_{a,0})) \leq \varphi(p_1p_2)$$

Proof. Note that proving

$$p_1p_2 + \mathrm{tdeg}(f_{a,0}) - \deg(f_{a,0}) \leq \varphi(p_1p_2)$$

is equivalent to proving

$$\deg(f_{a,0}) - \mathrm{tdeg}(f_{a,0}) - (p_1 + p_2 - 1) \geq 0$$

Recall from Lemma 4.2 that $\deg(f_{a,0}) = p_1p_2 - a$ for all $a > 0$. We break the proof into three cases.

1. Case: $w \leq u$. By Lemma 4.2, we have

$$\begin{aligned}
&\deg(f_{a,0}) - \mathrm{tdeg}(f_{a,0}) - (p_1 + p_2 - 1) \\
&= p_1p_2 - a - (u + 1 - w) - (p_1 + p_2 - 1) \\
&= \varphi(p_1p_2) + w - a - u - 1 \\
&\geq \varphi(p_1p_2) - a - u - 1 \\
&\geq \varphi(p_1p_2) - a - p_1 + 1 && \text{by Lemma 4.4} \\
&\geq 0 && \text{since } a \leq \tfrac{\varphi(p_1p_2)}{2}
\end{aligned}$$

2. Case: $w > u$ and $\neg\mathcal{D}(a)$. By Lemma 4.2, we have

$$\begin{aligned}
&\deg(f_{a,0}) - \mathrm{tdeg}(f_{a,0}) - (p_1 + p_2 - 1) \\
&= p_1p_2 - a - (p_1 - w) - (p_1 + p_2 - 1) \\
&= \varphi(p_1p_2) + w - a - p_1 \\
&\geq \varphi(p_1p_2) - a - u \\
&\geq \varphi(p_1p_2) - a - p_1 + 2 && \text{by Lemma 4.4} \\
&\geq 0 && \text{since } a \leq \tfrac{\varphi(p_1p_2)}{2}
\end{aligned}$$

3. Case: $w > u$ and $\mathcal{D}(a)$. By Lemma 4.2, we have

$$\begin{aligned}
&\deg(f_{a,0}) - \mathrm{tdeg}(f_{a,0}) - (p_1 + p_2 - 1) \\
&= p_1p_2 - a - ((u+1)p_2 - a) - (p_1 + p_2 - 1) \\
&= \varphi(p_1p_2) - (u+1)p_2
\end{aligned}$$

Note that in this case,

$$\begin{aligned}
a &= up_2 + vp_1 + w \\
a &= up_2 + qp_1 + w \\
a &= up_2 + p_2 - p_1 + 1 + w \\
a &= (u+1)p_2 - p_1 + 1 + w
\end{aligned}$$

Thus

$$\deg(f_{a,0}) - \mathrm{tdeg}(f_{a,0}) - (p_1 + p_2 - 1) = \varphi(p_1p_2) - (u+1)p_2$$

$$
\begin{aligned}
&= \varphi(p_1p_2) - (a + p_1 - 1 - w) \\
&\geq \varphi(p_1p_2) - a - p_1 \\
&\geq 0 && \text{since } a \leq \tfrac{\varphi(p_1p_2)}{2}
\end{aligned}
$$

□

Proof of Lemma 4.5 (G1). By Lemma 4.6, we have

$$
g(f_a) = \begin{cases} \varphi(p_1p_2) & \text{if } a = 0 \\ \max\left\{g(f_{a,0}),\, p_1p_2 + \mathrm{tdeg}(f_{a,0}) - \deg(f_{a,0})\right\} & \text{if } 1 \leq a \leq h \end{cases}
$$

By Lemma 4.7, we have

$$
\max_{1 \leq a \leq h} g(f_{a,0}) \leq \varphi(p_1p_2)
$$

By Lemma 4.8, we have

$$
\max_{1 \leq a \leq h} (p_1p_2 + \mathrm{tdeg}(f_{a,0}) - \deg(f_{a,0})) \leq \varphi(p_1p_2)
$$

Therefore,

$$
\max_{0 \leq a \leq h} g(f_a) = \varphi(p_1p_2)
$$

which proves the lemma. □

Proof of G2

Lemma 4.9 (G2)**.** *We have*

$$
\max_{0 \leq a \leq h} (p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)) \leq \varphi(p_1p_2)
$$

Before we can prove this, we first need to prove several other lemmas.

Lemma 4.10. *We have*

$$p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)$$
$$= \begin{cases} p_1 & \textit{if } a = 0 \\ p_1p_2 + 1 + \mathrm{tdeg}(f_{a+1,0}) - \deg(f_{a,0}) & \textit{else} \end{cases}$$

Proof. By Theorem 4.4, we have

$$\mathrm{tdeg}(f_{a+1}) = \mathrm{tdeg}(f_{a+1,0})$$
$$\deg(f_a) = \begin{cases} q_3p_1p_2 & \text{if } a = 0 \\ (q_3 - 1)p_1p_2 + \deg(f_{a,0}) & \text{else} \end{cases}$$

Since $p_3 - q_3p_1p_2 = r = 1$, we have

$$p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)$$
$$= \begin{cases} p_3 + \mathrm{tdeg}(f_{1,0}) - q_3p_1p_2 & \text{if } a = 0 \\ p_3 + \mathrm{tdeg}(f_{a+1,0}) - (q_3 - 1)p_1p_2 - \deg(f_{a,0}) & \text{else} \end{cases}$$
$$= \begin{cases} \mathrm{tdeg}(f_{1,0}) + 1 & \text{if } a = 0 \\ p_1p_2 + 1 + \mathrm{tdeg}(f_{a+1,0}) - \deg(f_{a,0}) & \text{else} \end{cases}$$

Recall from Lemma 4.3,

$$f_{1,0} = -x^{p_1-1} - x^{p_2-1} + x^{p_1+p_2-1} + x^{p_1p_2-1}$$

Hence,

$$\mathrm{tdeg}(f_{1,0}) + 1 = p_1$$

which proves the lemma. □

Lemma 4.11. *We have*

$$\max_{1 \le a \le h} (p_1 p_2 + 1 + \mathrm{tdeg}(f_{a+1,0}) - \deg(f_{a,0})) \le \varphi(p_1 p_2)$$

Proof. Note that proving

$$p_1 p_2 + 1 + \mathrm{tdeg}(f_{a+1,0}) - \deg(f_{a,0}) \le \varphi(p_1 p_2)$$

is equivalent to proving

$$\deg(f_{a,0}) - \mathrm{tdeg}(f_{a+1,0}) - (p_1 + p_2) \ge 0$$

Recall that $\deg(f_{a,0}) = p_1 p_2 - a$, for all $a > 0$. Thus we wish to show that

$$p_1 p_2 - a - \mathrm{tdeg}(f_{a+1,0}) - (p_1 + p_2) \ge 0$$
$$\varphi(p_1 p_2) - a - 1 - \mathrm{tdeg}(f_{a+1,0}) \ge 0$$

By Lemma 4.2, we have

$$\mathrm{tdeg}(f_{a+1,0}) = \begin{cases} u' + 1 - w' & \text{if } w' \le u' \\ p_1 - w' & \text{if } w' > u' \text{ and } \neg\mathcal{D}(a+1) \\ (u'+1)p_2 - (a+1) & \text{if } w' > u' \text{ and } \mathcal{D}(a+1) \end{cases}$$

where

$$u' = \mathrm{quo}(a+1, \overline{p_2})$$
$$w' = \mathrm{rem}(\mathrm{rem}(a+1, \overline{p_2}), p_1)$$

We break the rest of the proof into three cases:

1. Case: $w' \leq u'$. Then

$$\begin{aligned}
\varphi(p_1p_2) - a - 1 - \mathrm{tdeg}(f_{a+1,0}) &= \varphi(p_1p_2) - a - 1 - (u' + 1 - w') \\
&= \varphi(p_1p_2) - a - 2 - u' + w' \\
&\geq \varphi(p_1p_2) - a - 2 - u' \\
&\geq \varphi(p_1p_2) - a - p_1 && \text{by Lemma 4.4} \\
&\geq 0 && \text{since } a \leq \tfrac{\varphi(p_1p_2)}{2}
\end{aligned}$$

2. Case: $w' > u'$ and $\neg\mathcal{D}(a+1)$. Then

$$\begin{aligned}
\varphi(p_1p_2) - a - 1 - \mathrm{tdeg}(f_{a+1,0}) &= \varphi(p_1p_2) - a - 1 - (p_1 - w') \\
&= \varphi(p_1p_2) - a - 1 - p_1 + w' \\
&\geq \varphi(p_1p_2) - a - 1 - p_1 \\
&\geq 0 && \text{since } a \leq \tfrac{\varphi(p_1p_2)}{2}
\end{aligned}$$

3. Case: $w' > u'$ and $\mathcal{D}(a+1)$. Then

$$\begin{aligned}
\varphi(p_1p_2) - a - 1 - \mathrm{tdeg}(f_{a+1,0}) &= \varphi(p_1p_2) - a - 1 - ((u'+1)p_2 - (a+1)) \\
&= \varphi(p_1p_2) - (u'+1)p_2
\end{aligned}$$

Let $v' = \mathrm{quo}(\mathrm{rem}(a+1, \overline{p_2}), p_1)$. Note that since $\mathcal{D}(a+1)$,

$$\begin{aligned} a+1 &= u'p_2 + v'p_1 + w' \\ a+1 &= u'p_2 + qp_1 + w' \\ a+1 &= u'p_2 + p_2 - p_1 + 1 + w' \\ a+1 &= (u'+1)p_2 - p_1 + 1 + w' \end{aligned}$$

Thus

$$\begin{aligned} \varphi(p_1p_2) - a - 1 - \mathrm{tdeg}(f_{a+1,0}) &= \varphi(p_1p_2) - (u'+1)p_2 \\ &= \varphi(p_1p_2) - (a + 1 + p_1 - 1 - w') \\ &\geq \varphi(p_1p_2) - a - p_1 \\ &\geq 0 \qquad \text{since } a \leq \tfrac{\varphi(p_1p_2)}{2} \end{aligned}$$

□

Proof of Lemma 4.9 (G2). By Lemma 4.10, we have

$$\begin{aligned} & p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a) \\ &= \begin{cases} p_1 & \text{if } a = 0 \\ p_1p_2 + 1 + \mathrm{tdeg}(f_{a+1,0}) - \deg(f_{a,0}) & \text{else} \end{cases} \end{aligned}$$

By Lemma 4.11, we have

$$\max_{1 \leq a \leq h} (p_1p_2 + 1 + \mathrm{tdeg}(f_{a+1,0}) - \deg(f_{a,0})) \leq \varphi(p_1p_2)$$

Since $p_1 \leq \varphi(p_1 p_2)$, we have

$$\max_{0 \leq a \leq h} (p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)) \leq \varphi(p_1 p_2)$$

□

Proof of Theorem 4.1

Now that we have proved (G1) and (G2), we are ready to prove the main theorem.

Proof of Theorem 4.1. By Lemma 4.1, we have

$$g(\Phi_{p_1 p_2 p_3}) = \max \left\{ \max_{0 \leq a \leq h} \left\{ g(f_a),\, p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a) \right\} \right\}$$

In Lemma 4.5, we showed

$$\max_{0 \leq a \leq h} g(f_a) = \varphi(p_1 p_2)$$

In Lemma 4.9, we showed

$$\max_{0 \leq a \leq h} (p_3 + \mathrm{tdeg}(f_{a+1}) - \deg(f_a)) \leq \varphi(p_1 p_2)$$

Therefore, we have shown that

$$g(\Phi_{p_1 p_2 p_3}) = \varphi(p_1 p_2)$$

which proves the theorem. □

Chapter 5

Exact Inverse Cyclotomic

Introduction

We provide a sufficient condition that $g(\Psi_n) = \delta^-$ (Theorem 5.1). It is a straightforward generalization of a result in [23] for the case $k = 3$. We also show that, for every fixed p_1, the sufficient condition holds "almost always" in a certain sense (Theorem 5.1).

5.1 Main Results

Theorem 5.1 (Sufficient condition on $g(\Psi_n)$)**.** *We have*

1. $g(\Psi_n) = \delta^-(n)$ *if* $\delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}$.

2. *For every* $k \geq 2$ *and every odd prime* p*, we have*

$$\lim_{b\to\infty} \frac{\#\left\{n \ : \ p_k \leq b,\, p_1 = p,\, \delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}\right\}}{\#\left\{\, n \ : \ p_k \leq b,\, p_1 = p \,\right\}} = 1$$

5.2 Examples for sufficient condition on $g(\Psi_n)$

Example 5.1. *Let $n = 3 \cdot 7 \cdot 11$. Then $\delta^-(n) = 43$. Consider*

$$\frac{1}{2}\left(\frac{3 \cdot 7 \cdot 11}{3}\right) = \frac{77}{2} \leq \delta^-(n)$$

Computation of Ψ_n shows that $g(\Psi_n) = 43$, as expected from the theorem.

Example 5.2. *Let $n = 3 \cdot 5 \cdot 7$. Then $\delta^-(n) = 13$. Consider*

$$\frac{1}{2}\left(\frac{3 \cdot 5 \cdot 7}{3}\right) = \frac{35}{2} > \delta^-(n)$$

Computation of Ψ_n shows that $g(\Psi_n) = 13$. Therefore, the condition is sufficient but not necessary.

Example 5.3. *Let $n = 7 \cdot 11 \cdot 13$. Then $\delta^-(n) = 5$. Consider*

$$\frac{1}{2}\left(\frac{7 \cdot 11 \cdot 13}{7}\right) = \frac{143}{2} > \delta^-(n)$$

Computation of Ψ_n shows that $g(\Psi_n) = 6$. Thus $\delta^-(n) \neq g(\Psi_n)$.

5.3 Quality of sufficient condition on $g(\Psi_n)$

The following plots in Figure 5.1 show the following ratio r for various values of k and p.

$$r = \frac{\#\left\{n \ : \ p_k \leq b,\, p_1 = p,\, \delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}\right\}}{\#\left\{\, n \ : \ p_k \leq b,\, p_1 = p\right\}}$$

We observe that in all cases, the ratio goes to 1, as expected from the theorem.

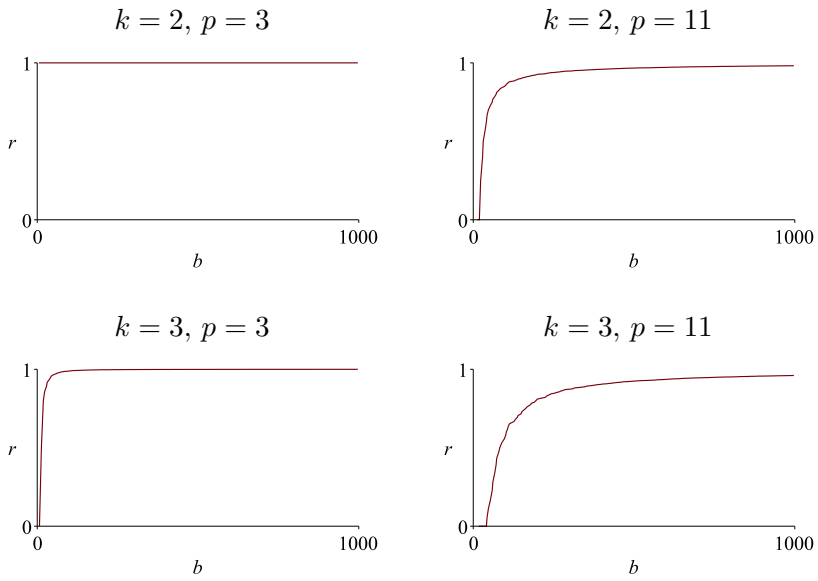


Figure 5.1 Plots validating Theorem 5.1

5.4 Proof

There are two claims in Theorem 5.1. We will prove them one by one.

Proof of Theorem 5.1 Claim 1. We will prove that $g(\Psi_n) = \delta^-(n)$ if $\delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}$. From Lemma 3.8 we have

$$\Psi_n(x) = -H(x) + H(x) \cdot x^{\frac{n}{p_1}}$$

Let

$$\delta^-(n) = \operatorname{tdeg}\left(H(x) \cdot x^{\frac{n}{p_1}}\right) - \deg(H(x))$$

Note that if $\delta^-(n) \geq \deg(H(x))$, then we obviously have $g(\Psi_n) = \delta^-(n)$. In the following we simplify the expression $\delta^-(n)$ and the condition $\delta^-(n) \geq \deg(H(x))$. First, we simplify the

expression $\delta^{-}(n)$.

$$\begin{aligned}\delta^{-}(n) &= \operatorname{tdeg}\left(H(x)\cdot x^{\frac{n}{p_1}}\right) - \deg\left(H(x)\right)\\ &= \frac{n}{p_1} - \left(\psi(n) - \frac{n}{p_1}\right)\\ &= 2\frac{n}{p_1} - \psi(n)\end{aligned}$$

Next, we simplify the condition $\delta^{-}(n) \geq \deg\left(H(x)\right)$.

$$\begin{aligned}\delta^{-}(n) \geq \deg\left(H(x)\right) &\iff 2\frac{n}{p_1} - \psi(n) \geq \psi(n) - \frac{n}{p_1}\\ &\iff 3\,\frac{n}{p_1} - 2\,\psi(n) \geq 0\\ &\iff \frac{3}{2}\,\frac{n}{p_1} - \psi(n) \geq 0\\ &\iff 2\,\frac{n}{p_1} - \psi(n) \geq \frac{1}{2}\,\frac{n}{p_1}\\ &\iff \delta^{-}(n) \geq \frac{1}{2}\,\frac{n}{p_1}\end{aligned}$$

Therefore we have shown if $\delta^{-}(n) \geq \frac{1}{2}\,\frac{n}{p_1}$ then $g(\Psi_n) = \delta^{-}(n)$ which proves the first claim of the theorem. □

We visualize the above proof as a diagram. We represent the inverse cyclotomic polynomial as a horizontal block. A black box (block) represents that the exponent(s) appears in the polynomial, a gray box (block) represents that the exponent(s) may or may not appear in the polynomial, and a white box (block) represents that the exponent(s) does not appear. Recall from the above proof that $\delta^{-}(n) \geq \frac{1}{2}\frac{n}{p_1}$ if and only if $\delta^{-}(n) \geq \deg(H(x))$. If this is the case, then the inverse cyclotomic polynomial is as follows:

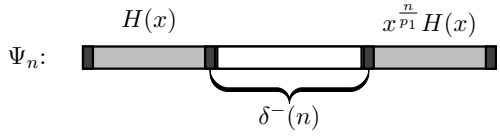


Figure 5.2 Diagram showing $\delta^-(n)$ in Ψ_n

From Figure 5.2, it is clear that if $\delta^-(n) \geq \deg(H(x))$, then $g(\Psi_n) = \delta^-(n)$.

The idea for the proof of the second claim is as follows: in Lemma 5.1, we weaken the condition in Claim 1 to only depend on p_1, p_2 and k. Then we show that given k, when the first prime p_1 is fixed, the numerator and denominator are combinatorial expressions that are dominated by the same terms; thus, the limit of their quotient is one. We first prove a technical lemma.

Lemma 5.1. *If* $p_2 > (k-1)(2p_1 - 3)$ *then* $\delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}$.

Proof. Note

$$\begin{aligned}
\delta^-(n) &\geq \frac{1}{2}\frac{n}{p_1} \\
\iff \frac{3}{2}\frac{n}{p_1} &\geq \psi(n) \\
\iff \frac{3}{2}\frac{n}{p_1} &\geq n - \varphi(n) \\
\iff \frac{3}{2}\frac{1}{p_1} &\geq 1 - \frac{\varphi(n)}{n} \\
\iff \frac{3}{2}\frac{1}{p_1} &\geq 1 - \left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\
\iff \frac{1}{2}\frac{1}{p_1} &\geq 1 - \frac{1}{p_1} - \left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\
\iff \frac{1}{2}\frac{1}{p_1} &\geq \left(1 - \frac{1}{p_1}\right)\left(1 - \left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\right)
\end{aligned}$$

$$
\begin{aligned}
&\iff \frac{1}{2} \;\geq\; (p_1-1)\cdot\left(1-\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\right)\\
&\impliedby \frac{1}{2} \;\geq\; (p_1-1)\cdot\left(1-\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_2+1}\right)\cdots\left(1-\frac{1}{p_2+k-2}\right)\right)\\
&\iff \frac{1}{2} \;\geq\; (p_1-1)\cdot\left(1-\left(\frac{p_2-1}{p_2}\right)\left(\frac{p_2}{p_2+1}\right)\left(\frac{p_2+1}{p_2+2}\right)\cdots\left(\frac{p_2+k-3}{p_2+k-2}\right)\right)\\
&\iff \frac{1}{2} \;\geq\; (p_1-1)\cdot\left(1-\frac{p_2-1}{p_2+k-2}\right)\\
&\iff \frac{1}{2} \;\geq\; (p_1-1)\cdot\frac{k-1}{p_2+k-2}\\
&\iff \frac{p_2+k-2}{2} \;\geq\; (k-1)\,(p_1-1)\\
&\iff p_2+k-2 \;\geq\; (k-1)\,(2p_1-2)\\
&\iff p_2 \;\geq\; (k-1)\,(2p_1-2)-(k-2)\\
&\iff p_2 \;\geq\; (k-1)\,(2p_1-3)+1\\
&\iff p_2 \;>\; (k-1)\,(2p_1-3)
\end{aligned}
$$

Therefore, if $p_2 > (k-1)\,(2p_1-3)$, then $\delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}$. □

Proof of Theorem 5.1 Claim 2. We will prove

$$\lim_{b\to\infty} \frac{\#\left\{n \;:\; p_k \leq b,\, p_1 = p,\, \delta^-(n) \geq \frac{1}{2}\frac{n}{p_1}\right\}}{\#\left\{\, n \;:\; p_k \leq b,\, p_1 = p \,\right\}} = 1$$

Let q_i be the i-th odd prime, that is, $q_1 = 3,\ q_2 = 5,\ q_3 = 7,\ q_4 = 11$, etc. Let $k \geq 2$. Let $p = q_v$ and $b = q_w$. Then we have

$$
\begin{aligned}
&\#\left\{n \;:\; p_k \leq b,\, p_1 = p\right\}\\
&= \#\left\{(p_1,\ldots,p_k) \;:\; p_1 < \cdots < p_k \leq b,\, p_1 = p\right\}\\
&= \#\left\{(q_{i_1},\ldots,q_{i_k}) \;:\; q_{i_1} < \cdots < q_{i_k} \leq q_w,\ q_{i_1} = q_v\right\}\\
&= \#\left\{(i_1, i_2, \ldots, i_k) \;:\; i_1 < i_2 < \cdots < i_k \leq w,\, i_1 = v\right\}
\end{aligned}
$$

$$
\begin{aligned}
&= \#\left\{(i_2, \ldots, i_k) \ : \ v+1 \le i_2 < \cdots < i_k \le w\right\} \\
&= \#\left\{(i_2, \ldots, i_k) \ : \ v+1 \le i_2 < \cdots < i_k \le v + (w-v)\right\} \\
&= \binom{w-v}{k-1}
\end{aligned}
$$

Thus

$$
\#\left\{n \ : \ p_k \le b,\, p_1 = p\right\} = \binom{w-v}{k-1}
$$

Note

$$
\begin{aligned}
&\#\left\{n \ : \ p_k \le b,\, p_1 = p,\, \delta^-(n) \ge \ \frac{1}{2}\frac{n}{p_1}\right\} \\
&= \#\left\{(p_1, \ldots, p_k) \ : \ p_k \le b,\, p_1 = p,\ \delta^-(p_1 \cdots p_k) \ge \ \frac{1}{2}\frac{p_1 \cdots p_k}{p_1}\right\} \\
&\ge \#\{(p_1, \ldots, p_k) \ : \ p_k \le b,\, p_1 = p,\ \ p_2 > (k-1)(2p_1 - 3)\} \quad \text{(from Lemma 5.1)} \\
&= \#\{(q_{i_1}, \ldots, q_{i_k}) \ : \ q_{i_1} < \cdots < q_{i_k} \le q_w,\, q_{i_1} = q_v,\, q_{i_2} > (k-1)(2q_v - 3)\} \\
&= \#\{(q_{i_1}, \ldots, q_{i_k}) \ : \ q_{i_1} < \cdots < q_{i_k} \le q_w,\, q_{i_1} = q_v,\, q_{i_2} \ge q_y\} \ \text{ where } y = \operatorname*{argmin}_{q_i > (k-1)(2q_v-3)} i \\
&= \#\{(i_1, \ldots, i_k) \ : \ i_1 < \cdots < i_k \le w,\, i_1 = v,\, i_2 \ge y\} \\
&= \#\{(i_2, \ldots, i_k) \ : \ v+1 \le i_2 < \cdots < i_k \le w,\, i_2 \ge y\} \\
&= \#\{(i_2, \ldots, i_k) \ : \ \max\{v+1,\, y\} \le i_2 < \cdots < i_k \le w\} \\
&= \#\{(i_2, \ldots, i_k) \ : \ y \le i_2 < \cdots < i_k \le w\} \quad \text{(since } y \ge v+1\text{)} \\
&= \binom{w-y+1}{k-1}
\end{aligned}
$$

Thus we have

$$
\#\left\{n \ : \ p_k \le b,\, p_1 = p,\, \delta^-(n) \ge \ \frac{1}{2}\frac{n}{p_1}\right\} \ge \binom{w-y+1}{k-1}
$$

Note

$$\lim_{b\to\infty} \frac{\#\left\{n \ : \ p_k \leq b,\, p_1 = p,\, \delta^-(n) \geq \ \frac{1}{2}\frac{n}{p_1}\right\}}{\#\left\{n \ : \ p_k \leq b,\, p_1 = p\right\}} \geq \lim_{w\to\infty} \frac{\binom{w-y+1}{k-1}}{\binom{w-v}{k-1}} = \lim_{w\to\infty} \frac{\frac{1}{(k-1)!}w^{k-1} + \cdots}{\frac{1}{(k-1)!}w^{k-1} + \cdots} = 1$$

Since

$$\lim_{b\to\infty} \frac{\#\left\{n \ : \ p_k \leq b,\, p_1 = p,\, \delta^-(n) \geq \ \frac{1}{2}\frac{n}{p_1}\right\}}{\#\left\{n \ : \ p_k \leq b,\, p_1 = p\right\}} \leq 1$$

we can conclude

$$\lim_{b\to\infty} \frac{\#\left\{n \ : \ p_k \leq b,\, p_1 = p,\, \delta^-(n) \geq \ \frac{1}{2}\frac{n}{p_1}\right\}}{\#\left\{n \ : \ p_k \leq b,\, p_1 = p\right\}} = 1$$

which proves the second claim of the theorem. □

BIBLIOGRAPHY

[1] Ala'a Al-Kateeb, Hoon Hong, and Eunjeong Lee. Structure of cyclotomic polynomials and several applications. *ArXiv*, 2017.

[2] Andrew Arnold and Michael Monagan. Calculating cyclotomic polynomials. *Mathematics of Computation*, 2011.

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

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

[5] J. P. Buhler, H. W. Lenstra, and Carl Pomerance. *Factoring integers with the number field sieve*, pages 50–94. Springer Berlin Heidelberg, 1993.

[6] David Burton. *Elementary number theory*. McGraw-Hill Education, 7th edition edition, 2010.

[7] Bartlomiej Bzdega. Bounds on ternary cyclotomic coefficients. *Acta Arith.*, 144:5–16, 2010.

[8] Bartlomiej Bzdega. On the height of cyclotomic polynomials. *Acta Arith.*, 152:349–359, 2012.

[9] Bartlomiej Bzdega. Jumps of ternary cyclotomic coefficients. *Acta Arith.*, 163:203–213, 2014.

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

[11] Oana-Maria Camburu, Emil-Alexandru Ciolan, Florian Luca, Pieter Moree, and Igor E. Shparlinski. Cyclotomic coefficients: gaps and jumps. *J. Number Theory*, 163:211–237, 2016.

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

[13] Cristian Cobeli, Yves Gallot, Pieter Moree, and Alexandru Zaharescu. Sister beiter and kloosterman: a tale of cyclotomic coefficients and modular inverses. *Indag. Math. (N.S.)*, 24:915–929, 2013.

[14] Gregory P. Dresden. On the middle coefficient of a cyclotomic polynomial. *Amer. Math. Monthly*, 111:531–533, 2004.

[15] Underwood Dudley. *Elementary number theory*. Dover Publiations, 2nd edition, 2008.

[16] J. Fintzen. Cyclotomic polynomial coefficients $a(n, k)$ with n and k in prescribed residue classes. *J. Number Theory*, 131:1852–1863, 2011.

[17] Etienne Fouvry. On binary cyclotomic polynomials. *Algebra Number Theory*, 5:1207–1223, 2013.

[18] Y. Gallot and P. Moree. Ternary cyclotomic polynomials having a large coefficient. *J. Reine Angew. Math.*, 632:105–125, 2009.

[19] Yves Gallot and Pieter Moree. Neighboring ternary cyclotomic coefficients differ by at most one. *J. Ramanujan Math. Soc.*, 24:235–248, 2009.

[20] Yves Gallot, Pieter Moree, and Robert Wilms. The family of ternary cyclotomic polynomials with one free prime. *Involve*, 4:317–341, 2011.

[21] Shay Gueron and Ran Tessler. 86.18 infinitely many primes in arithmetic progressions: The cyclotomic polynomial method. *The Mathematical Gazette*, 86(505):110–114, 2002.

[22] Hoon Hong, Eunjeong Lee, and Hyang-Sook Lee. Explicit formula for optimal ate pairing over cyclotomic family of elliptic curves. *Finite Fields and Their Applications*, 34:45–74, 2015.

[23] Hoon Hong, Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. Maximum gap in (inverse) cyclotomic polynomials. *J. of Number Theory*, 2012.

[24] Hoon Hong, Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. Simple and exact formula for minimum loop length in ate_i pairing based on brezing-weng curves. *Des. Codes Cryptogr.*, 2013:271–292, 2013.

[25] Nathan Kaplan. Flat cyclotomic polynomials of order three. *J. Number Theory*, 127:118–126, 2007.

[26] Devin Kuh. Constructible regular n-gons. *Senior Project Archive*, pages 1–36, 2013.

[27] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. Efficient and generalized pairing computation on abelian varieties. *IEEE Trans. Inform. Theory*, 55:17931803, 2009.

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

[29] Arjen K. Lenstra. Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields. *Australasian Conference on Information Security and Privacy*, pages 126–128, 1997. Springer Berlin Heidelberg.

[30] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1994.

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

[32] Pieter Moree. Numerical semigroups, cyclotomic polynomials and bernoulli numbers. *Amer. Math Monthly*, 121:890–902, 2014.

[33] Pieter Moree and Eugenia Rosu. Non-beiter ternary cyclotomic polynomials with an optimally large set of coefficients. *Int. J. Number Theory*, 8:1883–1902, 2012.

[34] Kenneth H Rosen. *Elementary number theory and its applications*. Pearson, 6th edition, 2010.

[35] Satoru Tanaka and Ken Nakamula. Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials. *International Conference on Pairing-Based Cryptography*, pages 136–145, 2008. Springer Berlin Heidelberg.

[36] R. Thangadurai. On the coefficients of cyclotomic polynomials. *Cyclotomic Fields and Related Topics, Pune*, pages 311–322, 2000.

[37] Bin Zhang. Remarks on the maximum gap in binary cyclotomic polynomials. *Bull. Math. Soc. Sci. Math. Roumanie Tome*, 59:109–115, 2015.

[38] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang. A note on the ate pairing. *Int. J. Inf. Secur.*, 7:379–382, 2008.

APPENDIX

Appendix A

Maple Codes

A.1 Utilities

```
restart:
with(numtheory):
with(ListTools):
with(combinat):
with(plots):
with(Statistics):
unprotect(D):

psi := n-> n - phi(n):

icyc := proc(n,x)
  local f;
  f := cyclotomic(n,x);
  divide(x^n-1,f,'f');
  return f;
end:

exps_cyc := proc(n)
  local f,E;
  f := cyclotomic(n,x);
  coeffs(f,x,'E');
  E := map(degree,sort([E]),x);
  if nops(E) > 2 then E := E[1..ceil(nops(E)/2)]; fi;
  return E;
end:
```

```
exps_icyc := proc(n)
  local f,E;
  f := icyc(n,x);
  coeffs(f,x,'E');
  E := map(degree,sort([E]),x);
  if nops(E) > 2 then E := E[1..ceil(nops(E)/2)+1]; fi;
  return E;
end:

max_gap_cyc := proc(n)
  local E,F,g;
  E := exps_cyc(n);
  F := [seq(E[j+1]-E[j],j=1..nops(E)-1)];
  g := max(F);
  return g;
end:

max_gap_icyc := proc(n)
  local E,F,g;
  E := exps_icyc(n);
  F := [seq(E[j+1]-E[j],j=1..nops(E)-1)];
  g := max(F);
  return g;
end:

# returns all the divisors of C (C can be a number or a set)
div_set := proc(C)
  local D,d;
  D := {seq(op(divisors(d)),d in C)};
  return D;
end:

# returns number of prime factors
omega := proc(n)
  return nops(factorset(n));
end:

# returns parity
rho := proc(n)
  if type(n,even) then return 1; else return -1 fi;
end:
```

```
# returns all elements d in D such that mu(n/d) = pm 1
set_D_pm := proc(n,D,pm)
  local S,d;
  S := select(d->mobius(n/d) = pm*1,D);
  return S;
end:

# returns l^{pm}(D)
lower_D_pm := proc(n,D,pm)
  local l,a,b;
  l := pm*add(d*mobius(n/d),d in D);
  return l;
end:

# returns u^{pm}(D)
upper_D := proc(n,D)
  local u;
  u := min(D);
  return min(u);
end:

# returns C^{pm}(D)
c_D_pm := proc(n,D,pm)
  local c,Dp,Dm,num_Dp,num_Dm,d,m;
  c := true;
  Dp := set_D_pm(n,D,+1);
  Dm := set_D_pm(n,D,-1);
  for d in div_set(D) do
    num_Dp := nops(select(m->evalb(irem(m,d)=0),Dp));
    num_Dm := nops(select(m->evalb(irem(m,d)=0),Dm));
    if pm*num_Dp < pm*num_Dm then c := false; break fi;
  od;
  return c;
end:
```

A.2 Algorithms for lower bounds

```
alpha_pm := proc(n,pm)
  local ps,gs,r,nr_1,k;
  ps := factorset(n);
```

```
  k  := nops(ps);
  if k=1 then return 1 fi; if k=2 and pm=-1 then return 1 fi;
  gs := [];
  for r from 1 to k-1 do
    if rho(k-1-r) <> pm then next fi; r;
    nr_1 := mul(ps[i],i=1..r-1);
    gs := [op(gs), ps[r] - phi(nr_1)];
  od;
  return max(gs);
end:

beta_pm := proc(n,pm)
  local ps,gs,r,nr,k;
  ps := factorset(n);
  k  := nops(ps);
  if k=1 then return 1 fi; if k=2 and pm=-1 then return 1 fi;
  gs := [];
  for r from 1 to k-1 do
    if rho(k-1-r) <> pm then next fi; r;
    nr := mul(ps[i],i=1..r);
    gs := [op(gs), min(nr,ps[r+1]) - psi(nr)];
  od;
  return max(gs);
end:

gamma_pm := proc(n,pm)
  local gs,n_k,B,r,l,u,div_n,ps,k,n_r;
  gs := [];
  div_n := div_set(n);
  ps := [op(factorset(n))];
  k  := nops(ps);
  if k = 1 or k=2 and pm = -1 then return 1 fi;
  for r from 1 to k-1 do
    if rho(k-1-r) <> pm then next fi;
    B := select(d->omega(d) <= r-1, div_n);
    n_r := mul(ps[i],i=1..r);
    l := lower_D_pm(n,B,pm);
    gs := [op(gs), n_r - l];
  od;
  return max(gs);
end:
```

```
delta_m := proc(n)
  local ps;
  ps := factorset(n);
  return 2*n/ps[1] - (n-phi(n));
end:

epsilon_pm := proc(n,pm)
  local gs, D, Sp, Sm, A, B, l, u;
  gs := [];
  D  := div_set(n) minus {n};
  for A in powerset(D) minus {{}} do
    B := D minus A;
    if not c_D_pm(n,B,pm) then next fi;
    l := lower_D_pm(n,B,pm); u := upper_D(n,A);
    gs := [op(gs), u - l];
  od;
  return max(gs);
end:

# returns true if n satisfies the sufficient condition for delta_m
suff := n -> evalb(delta_m(n) >= 1/2*n/(factorset(n)[1])):

# returns the smallest prime larger than (p0+1-r)/m such that p = q*m + r
findprime := proc(p0,m,r)
  local q,p,P;
  for q from ceil((p0+1-r)/m) to 1000 do
    p := q*m + r;
    if isprime(p) then return p fi;
  od:
  print("findprime: FAIL"):
end:

epsilon_tilde_pm := proc(n,pm)
  local div_n,div_n_pm,div_n_mp,b,B1,B2,B,A,u,l,gs;
  div_n   := div_set(n);
  div_n_pm := set_D_pm(n,div_n,pm);
  div_n_mp := set_D_pm(n,div_n,-1*pm);
  gs      := [];
  for b in div_n_pm do
    B1 := select(m-> m < b,div_n_pm);
```

```
    B2 := set_D_pm(n,div_set(B1),-1*pm);
    B  := B1 union B2;
    A  := div_n minus B;
    u  := upper_D(n,A); l := lower_D_pm(n,B,pm);
    gs := [op(gs),u-l];
  od;
  return max(gs);
end:
```

A.3 Algorithm to check the conjecture

```
algorithm_one := proc(m)
  local p,r,g;
  for p from factorset(m)[-1] + 1 to m-1 do
    if not isprime(p) then next fi;
    if phi(m) = max_gap_cyc(m*p) then return false fi;
  od;
  for r from 1 to m-1 do
    if gcd(m,r) <> 1 then next fi;
    p := findprime(m,m,r);
    g := max_gap_cyc(m*p);
    if phi(m) <> g then return false fi;
  od;
  return true;
end:

algorithm := proc(ell)
  local m;
  for m from 3*5 to ell do
    if not issqrfree(m) or type(m,even) or omega(m) < 2 then next fi;
    if not algorithm_one(m) then return false fi;
  od;
  return true;
end:

algorithm(1000);
```