SOME PROPERTIES OF THE COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

Thesis by

Kau-un Lu

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1968

(Submitted April 5, 1968)

ACKNOWLEDGMENTS

The author wishes to acknowledge his indebtedness to his advisor, Dr. T. M. Apostol, for suggesting the subject matter of this research, and for his guidance and inspiration throughout the course of the research, and for his patient reading and revision of the presentation of this thesis.

During his graduate studies the author has been the recipient of Teaching Assistantships, and summer fellowships. The author wishes to express his appreciation for these gifts.

ABSTRACT

An explicit formula is obtained for the coefficients of the cyclotomic polynomial $F_n(x)$, where n is the product of two distinct odd primes. A recursion formula and a lower bound and an improvement of Bang's upper bound for the coefficients of $F_n(x)$ are also obtained, where n is the product of three distinct primes. The cyclotomic coefficients are also studied when n is the product of four distinct odd primes. A recursion formula and upper bounds for its coefficients are obtained. The last chapter includes a different approach to the cyclotomic coefficients. A connection is obtained between a certain partition function and the cyclotomic coefficients when n is the product of an arbitrary number of distinct odd primes. Finally, an upper bound for the coefficients is derived when n is the product of an arbitrary number of distinct odd primes.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

1.1 Historical Background

The cyclotomic polynomial $F_n(x)$ of order n is defined by the equation

$$F_n(x) = \prod_{j=1}^{\phi(n)} (x - \zeta_j) \quad , \tag{1}$$

where $\zeta_1, \zeta_2, \ldots, \zeta_{\phi(n)}$ are the primitive n^{th} roots of unity. Here $\phi(n)$ is Euler's function which enumerates the number of positive integers $\leq n$ which are relatively prime to n. We can also write

$$F_n(x) = \sum_{k=0}^{\phi(n)} c_k x^k \quad ,$$

where the coefficients $c_0, c_1, \ldots, c_{\phi(n)}$ are integers which we call cyclotomic coefficients. This thesis is a study of some of the properties of these coefficients.

The cyclotomic polynomials appeared first in Gauss's Disquisitiones Arithmeticae (1801) in a study of equations which determine the divisions of the circle. They appeared later in Cauchy's proof of the existence of primitive roots of a prime p (Exercises de math., 1829, 231). In 1854 Kronecker (Journal de math., XIX) and in 1859 V. Lebesgue (Ann. Mat. 2) studied the irreducibility of cyclotomic polynomials. Bang (Tidsskrift for math., (5), 4, 1886) and

Sylvester (Comptes Rendus Paris, 106, 1888) proved the existence of infinitely many primes of the form $m z + 1$ for given m by use of cyclotomic polynomials.

1.2 Some Basic Properties of Cyclotomic Polynomials

This section lists some basic properties of cyclotomic polynomials in the form of six lemmas. The first three lemmas show that $F_n(x)$ is a monic polynomial of degree $\phi(n)$ with integer coefficients. Lemma 4 shows that symmetrically located coefficients are equal. Hence to study the coefficients of the cyclotomic polynomial it suffices to study only half of them. Lemmas 5 and 6 reduce the study to cyclotomic polynomials of an order which is a product of distinct odd primes.

Lemma 1.
$$x^n - 1 = \prod_{d|n} F_d(x) \quad . \tag{2}$$

Proof: This follows from the fact that any nth root of unity is a primitive dth root of unity for some unique divisor d of n.

Lemma 2.
$$F_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \quad . \tag{3}$$

Proof: This follows from Lemma 1 by applying the Möbius inversion formula.

Lemma 3. The cyclotomic polynomial $F_n(x)$ of order n is a monic polynomial of degree $\phi(n)$ with integral coefficients.

Proof: This is easily proved by mathematical induction. The theorem is true for $n = 1$. Now suppose it is true for all $F_k(x)$, where

$k < n$. From (2) we have

$$x^n - 1 = F_n(x) \prod_{\substack{d|n \\ d<n}} F_d(x) = F_n(x)\, G_n(x) \quad ,$$

where
$$G_n(x) = \prod_{\substack{d|n \\ d<n}} F_d(x) \quad .$$

Since $d < n$, each factor $F_d(x)$ is a monic polynomial with integral coefficients by the induction hypothesis. Hence $G_n(x)$ is also a monic polynomial with integral coefficients. Now write

$$F_n(x) = \frac{x^n - 1}{G_n(x)} \quad .$$

Since $G_n(x)$ has leading coefficient 1, the long division produces only integral coefficients, so $F_n(x)$ is also a monic polynomial with integral coefficients.

To conclude the induction we need to prove that the degree of $F_n(x)$ is $\phi(n)$. Let the degree of $F_n(x)$ be v. From the induction hypothesis the degree of $F_d(x)$ is $\phi(d)$ for each $d < n$. Hence by (3) we have

$$n = v + \sum_{\substack{d|n \\ d<n}} \phi(d) = v - \phi(n) + \sum_{d|n} \phi(d) = v - \phi(n) + n \quad ,$$

since $\sum_{d|n} \phi(d) = n$. Hence $v = \phi(n)$ and the lemma is proved.

Lemma 4. Symmetrically located cyclotomic coefficients are equal for $n > 1$.

Proof: Since the degree of $F_n(x)$ is $\phi(n)$, proving the lemma is equivalent to proving that $x^{\phi(n)}\ F_n(1/x) = F_n(x)$. This proof makes use of the two well-known formulas (a) $\sum_{d|n} \mu(d) = 0$ for $n > 1$, and (b) $\sum_{d|n} d\mu(n/d) = \phi(n)$.

From (3) we have

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

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

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

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

by (b). If we change the sign of each factor the product does not change sign since by (a) we have $\sum_{d|n} \mu(n/d) = 0$. Therefore

$$x^{\phi(n)}\, F_n\left(\frac{1}{n}\right) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = F_n(x) \quad .$$

Lemma 5. If $n = p_1^{\alpha_1}\ p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where the α_i are positive integers, let $q = p_1 \ldots p_k$. Then

$$F_n(x) = F_q(x^{n/q}) \quad .$$

Proof: First rewrite (3) as

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

Now $\mu(d) = 0$ unless $d|q$. Hence

$$F_n(x) = \prod_{d|q} (x^{n/d} - 1)^{\mu(d)} = \prod_{d|q} \left\{ (x^{n/q})^{q/d} - 1 \right\}^{\mu(d)} = F_q(x^{n/q}) \ .$$

Lemma 6. If n is odd, $n \geq 3$, we have $F_{2n}(x) = F_n(-x)$.

Proof: By Lemma 2 we have

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

Since n is odd, the divisors d of $2n$ are equal to the divisors d' and $2d'$, where $d'|n$. Hence we have

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

Since $\mu(2n/d')$ and $\mu(n/d')$ have opposite signs for odd $n > 1$ and $d'|n$, we have

$$F_{2n}(x) = \prod_{d'|n} (x^{d'}+1)^{\mu(n/d')}, \quad \text{for} \quad n > 1 .$$

Since n is odd and $d'|n$, we have

$$\begin{aligned} F_{2n}(x) &= \prod_{d'|n} \left(-(-x)^{d'}+1\right)^{\mu(n/d')} \\ &= \prod_{d'|n} \left[\left((-x)^{d'}-1\right)^{\mu(n/d')} (-1)^{\mu(n/d')}\right] \\ &= \left[\prod_{d'|n} \left((-x)^{d'}-1\right)^{\mu(n/d')}\right] (-1)^{\sum_{d'|n} \mu(n/d')}, \quad \text{for} \quad n > 1 . \end{aligned}$$

Since $\sum_{d'|n} \mu(n/d') = 0$, we obtain

$$F_{2n}(x) = F_n(-x), \quad \text{for} \quad n > 1 .$$

1.3 Previous Work on the Cyclotomic Coefficients

In 1883, Migotti [12] proved that the coefficients of $F_{p_1p_2}(x)$ are ± 1 or 0, where p_1 and p_2 are two odd primes. In 1895 Bang [4] proved that no coefficient of $F_{p_1p_2p_3}(x)$ exceeds $p_1 - 1$, where $p_1 < p_2 < p_3$ are odd primes. In 1931, I. Schur proved that there exist cyclotomic polynomials with coefficients arbitrarily large in absolute value. The proof has not been published, but it was given by Emma Lehmer in one of her papers [11]. In 1936 Emma Lehmer [11] proved that as n runs over all products of three distinct primes, the cyclotomic polynomials $F_n(x)$ contain arbitrarily large coefficients. In 1945 Paul Erdös [8] proved there are infinitely many n such that the greatest coefficient of $F_n(x)$ in absolute value exceeds n^k for every k. In 1960 Marion Beiter [5] proved that if we let

$$F_{p_1p_2}(x) = \sum_{n=0}^{\phi(p_1p_2)} c_n x^n ,$$

where $p_1 < p_2$ are odd primes, then

$$c_n = \begin{cases} (-1)^\delta & \text{if } n = \alpha p_1 + \beta p_2 + \delta \text{ in exactly one way} , \\ 0 & \text{otherwise} , \end{cases}$$

where α and β are nonnegative integers and $\delta = 0$ or 1. In 1964 Helen Habermehl, Sharon Richardson, and Mary Ann Szwajkos [9] proved that if we let

$$F_{3\cdot p_2}(x) = \sum_{n=0}^{\phi(3\cdot p_2)} c_n x^n ,$$

where p_2 is a prime greater than 3, then for $n \leq p_2-1$,

$$c_n = \begin{cases} 1 & \text{if } n \equiv 0 \pmod 3 \\ -1 & \text{if } n \equiv 1 \pmod 3 \\ 0 & \text{if } n \equiv 2 \pmod 3 . \end{cases}$$

For $n > p_2-1$, we have $c_n = c_{n'}$, where $n' = 2(p_2-1) - n$.

CHAPTER II

THE CYCLOTOMIC POLYNOMIAL $F_n(x)$ WHERE n IS A PRODUCT OF TWO DISTINCT ODD PRIMES

Theorem 1 gives a formula for the coefficients of $F_{p_1p_2}(x)$ where p_1 and p_2 are two distinct odd primes greater than 3. In corollary 1 we show that the coefficients are ±1 or 0 by means of the formula in Theorem 1. It agrees with the known results.

2. 1 Explicit Formulas for the Coefficients

Theorem 1: Let p_1 and p_2 be two primes with $p_2 > p_1 > 3$. Let

$$F_{p_1p_2}(x) = \sum_{n=0}^{\phi(p_1p_2)} c_n x^n$$

and let

$$N = \left[\frac{\phi(p_1p_2)}{2p_2} \right] .$$

For each $k = 0, 1, 2, \ldots, N$, let

$$c_n(k) = \begin{cases} 0 & \text{if } 0 \leq n < kp_2 \\ 1 & \text{if } kp_2 \leq n \leq \dfrac{\phi(p_1p_2)}{2} , \quad n \equiv kp_2 \pmod{p_1} \\ -1 & \text{if } kp_2 \leq n \leq \dfrac{\phi(p_1p_2)}{2} , \quad n \equiv kp_2+1 \pmod{p_1} \\ 0 & \text{otherwise} . \end{cases}$$

Then we have

$$\text{(A)} \quad c_n = c_n(0) + c_n(1) + \ldots + c_n(N) \qquad \text{if} \quad 0 \leq n \leq \frac{\phi(p_1p_2)}{2} \quad ,$$

$$\text{(B)} \quad c_n = c_{\phi(p_1p_2)-n} \qquad \text{if} \quad \frac{\phi(p_1p_2)}{2} < n \leq \phi(p_1p_2) \quad .$$

2. 2 An Example

Before we prove the theorem 1, we consider the example $F_{35}(x)$. Here $p_1 = 5$, $p_2 = 7$. From the formula (3) of Lemma 2 we have

$$F_{35}(x) = \prod_{d|35} (x^d - 1)^{\mu(35/d)}$$

$$= \frac{(x-1)\ (x^{35}-1)}{(x^5-1)\ (x^7-1)} \quad .$$

Dividing out we have

$$F_{35}(x) = 1 - x + x^5 - x^6 + x^7 - x^8 + x^{10} - x^{11} + x^{12} - \ldots + x^{24} \quad .$$

To compute the coefficients by Theorem 1 we first determine

$$N = \left[\frac{(5-1)\ (7-1)}{2 \cdot 7} \right] = 1 \ , \qquad \text{and} \qquad \frac{\phi(5 \cdot 7)}{2} = 12 \quad .$$

The calculations for Theorem 1 can be arranged in tabular form as follows:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$c_n(0)$	1	-1	0	0	0	1	-1	0	0	0	1	-1	0
$c_n(1)$	0	0	0	0	0	0	0	1	-1	0	0	0	1
c_n	1	-1	0	0	0	1	-1	1	-1	0	1	-1	1

2.3 Proof of Theorem 1

From Lemma 1 we have

$$x^{p_1p_2} - 1 = F_1(x)\, F_{p_1}(x)\, F_{p_2}(x)\, F_{p_1p_2}(x)$$

$$= (x-1)\left(x^{p_2-1} + \ldots + x + 1\right)\left(x^{p_1-1} + \ldots + x + 1\right) F_{p_1p_2}(x)$$

$$= \left(x^{p_2} - 1\right)\left(x^{p_1-1} + \ldots + x + 1\right) F_{p_1p_2}(x) \quad .$$

Dividing by $\left(x^{p_2} - 1\right)$ we have

$$\left(x^{p_1-1} + x^{p_1-2} + \ldots + x + 1\right) F_{p_1p_2}(x)$$

$$= 1 + x^{p_2} + x^{2p_2} + \ldots + x^{(p_1-1)p_2} \quad .$$

Now we multiply out and make an appropriate change of the indices to obtain

$$\sum_{n=p_1-1}^{\phi(p_1p_2)+(p_1-1)} c_{n-(p_1-1)}\, x^n + \sum_{n=p_1-2}^{\phi(p_1p_2)+(p_1-2)} c_{n-(p_1-2)}\, x^n + \ldots$$

$$\ldots + \sum_{n=0}^{\phi(p_1p_2)} c_n\, x^n = 1 + x^{p_2} + \ldots + x^{(p_1-1)p_2} \quad . \qquad (4)$$

We shall prove (A) by equating the coefficients of like powers of x in (4). Part (B) then follows from the symmetry property of lemma 4.

We will prove (A) by mathematical induction on t where $tp_2 \leq n < (t+1)p_2$.

1) We consider the case $t = 0$, which means $0 \leq n < p_2$. Since for each $k = 1, 2, \ldots, N$ we have $c_n(k) = 0$ for $0 \leq n < kp_2$, to prove that (A) is true for $0 \leq n < p_2$ is equivalent to proving $c_n = c_n(0)$ for $0 \leq n < p_2$.

Equating the coefficients of like powers of x in (6) we find:

$$x^o \quad ; \quad c(0) = 1 = c_0(0) .$$

$$x^1 \quad ; \quad c_1 + c_0 = 0 \; ; \text{ hence } c_1 = -c_o = -1 = c_1(0) .$$

$$x^2 \quad ; \quad c_2 + c_1 + c_0 = 0 \; ; \text{ hence } c_2 = 0 = c_2(0) .$$

$$\cdot$$
$$\cdot$$
$$\cdot$$

$$x^i \quad ; \quad c_i + c_{i-1} + \ldots + c_1 + c_0 = 0 \; ; \text{ hence } c_i = 0 = c_i(0)$$

$$\text{where} \quad i \leq p_1 - 1 .$$

$$\cdot$$
$$\cdot$$
$$\cdot$$

$$x^{p_1} \quad ; \quad c_{p_1} + c_{p_1 - 1} + \ldots + c_2 + c_1 = 0 \; ; \text{ hence}$$

$$c_{p_1} + \left(c_{p_1 - 1} + \ldots + c_1 + c_0\right) - c_0 = 0 \; ; \text{ hence}$$

$$c_{p_1} = c_0 = c_0(0) = c_{p_1}(0) .$$

This proves that $c_n = c_n(0)$ for $0 \leq n \leq p_1$.

Next we show that $c_{m+1} = c_{m+1}(0)$ on the assumption that $c_m = c_m(0)$ where $p_1 \leq m < p_2$. This will prove that $c_n = c_n(0)$ for $0 \leq n < p_2$.

Equating the coefficients of x^{m+1} in (4) we find:

$$c_{m+1} + c_m + \ldots + c_{m+1-(p_1 - 1)} = 0 .$$

Hence

$$c_{m+1} - c_{m+1}(0) + \left(c_{m+1}(0) + c_m(0) + \dots + c_{m+1-(p_1-1)}(0)\right) = 0 \ . \qquad (5)$$

Now we shall prove, by induction on n, that we have

$$c_n(0) + c_{n-1}(0) + \dots + c_{n-(p_1-1)}(0) = 0 \qquad \text{for} \ \ p_1 - 1 \leq n < \frac{\phi(p_1 p_2)}{2} \ . \qquad (6)$$

Since $c_0(0) = 1$, $c_1(0) = -1$ and $c_i(0) = 0$ for $2 \leq i \leq p_1 - 1$, we have

$$c_{p_1-1}(0) + c_{p_1-2}(0) + \dots + c_1(0) + c_0(0) = 0 \ .$$

Hence (6) is true for $n = p_1 - 1$. Next we suppose it is true for $n = m$ and show it is true for $n = m+1$. We have

$$c_{m+1}(0) + c_m(0) + \dots + C_{m+1-(p_1-1)}(0)$$

$$= c_{m+1}(0) + \left(c_m(0) + c_{m-1}(0) + \dots + c_{m-(p_1-1)}(0)\right) - c_{m-(p_1-1)}(0) \ . \qquad (7)$$

By the assumption that (6) is true for $n = m$ the right member of (7) simplifies to

$$c_{m+1}(0) - c_{m-(p_1-1)}(0) \quad .$$

By the definition of the $c_n(0)$'s, this difference is 0. Hence we have proved (6).

By (6), equation (5) becomes

$$c_{m+1} - c_{m+1}(0) = 0 \quad .$$

Hence

$$c_{m+1} = c_{m+1}(0) \quad .$$

Hence we have shown that $c_n = c_n(0)$ for $0 \le n < p_2$.

2) Now we assume (A) is true for all n in the interval $tp_2 \le n < (t+1)p_2$ and try to show it is true for all n in the interval $(t+1)p_2 \le n < (t+2)p_2$ and $n \le \frac{\phi(p_1p_2)}{2}$.

Equating the coefficients of like powers of x in (4) we find

$$c_{(t+1)p_2} + c_{(t+1)p_2-1} + \dots + c_{(t+1)p_2-(p_1-1)} = 1 \quad .$$

By the induction hypothesis we have

$$c_{(t+1)p_2} + \left(c_{(t+1)p_2-1}(0) + c_{(t+1)p_2-1}(1) + \dots + c_{(t+1)p_2-1}(N)\right)$$
$$+ \dots + \left(c_{(t+1)p_2-(p_1-1)}(0)\right.$$
$$\left. + c_{(t+1)p_2-(p_1-1)}(1) + \dots + c_{(t+1)p_2-(p_1-1)}(N)\right) = 1.$$

Hence we have

$$c_{(t+1)p_2}(0) + \left(c_{(t+1)p_2-1}(0) + c_{(t+1)p_2-2}(0) + \dots + c_{(t+1)p_2-(p_1-1)}(0)\right)$$
$$+ \left(c_{(t+1)p_2-1}(1) + \dots + c_{(t+1)p_2-(p_1-1)}(1)\right) + \dots$$
$$\dots + \left(c_{(t+1)p_2-1}(N) + \dots + c_{(t+1)p_2-(p_1-1)}(N)\right) = 1 \quad .$$

Adding and subtracting $c_{(t+1)p_2}(0) + \dots + c_{(t+1)p_2}(N)$ on the left we obtain

$$c_{(t+1)p_2} - \left(c_{(t+1)p_2}(0) + \ldots + c_{(t+1)p_2}(N)\right)$$

$$+ \left(c_{(t+1)p_2}(0) + c_{(t+1)p_2-1}(0) + \ldots + c_{(t+1)p_2-(p_1-1)}(0)\right) + \ldots$$

$$\ldots + \left(c_{(t+1)p_2}(N) + \ldots + c_{(t+1)p_2-(p_1-1)}(N)\right) = 1 \quad . \qquad (8)$$

Now we shall prove, by induction on n, that for each $k = 1, 2, \ldots, N$ we have

$$c_n(k) + c_{n-1}(k) + \ldots + c_{n-(p_1-1)}(k) = 0 \quad , \qquad (9)$$

where n is such that $(k+1)p_2 \leq n \leq \dfrac{\phi(p_1 p_2)}{2}$.

Since $c_{(k+1)p_2}(k) = 1$ and $c_{(k+1)p_2-(p_1-1)} = -1$, we have

$$c_{(k+1)p_2}(k) + c_{(k+1)p_2-1}(k) + \ldots + c_{(k+1)p_2-(p_1-1)}(k) = 0 \quad .$$

This proves (9) for $n = (k+1)p_2$. Now we suppose (9) is true for $n = m$, where $(k+1)p_2 \leq m < \dfrac{\phi(p_1 p_2)}{2}$ and show it is also true for $n = m+1$. We have

$$c_{m+1}(k) + c_m(k) + \ldots + c_{m+1-(p_1-1)}(k)$$

$$= c_{m+1}(k) + \left(c_m(k) + \ldots + c_{m-(p_1-1)}(k)\right) - c_{m-(p_1-1)}(k) \quad . \qquad (10)$$

By the hypothesis that (9) is true for $n = m$, the right member of (10) simplifies to

$$c_{m+1}(k) - c_{m-(p_1-1)}(k) = 0 \quad .$$

This proves (9).

Now we return to (8). Since by (6) we have

$$c_{(t+1)p_2}(0) + c_{(t+1)p_2-1}(0) + \dots + c_{(t+1)p_2-(p_1-1)}(0) = 0 \quad ,$$

(8) simplifies to

$$\begin{aligned} c_{(t+1)p_2} &- \left(c_{(t+1)p_2}(0) + \dots + c_{(t+1)p_2}(N)\right) \\ &+ \left(c_{(t+1)p_2}(1) + c_{(t+1)p_2-1}(1) + \dots + c_{(t+1)p_2-(p_1-1)}(1)\right) + \dots \\ &\dots + \left(c_{(t+1)p_2}(N) + \dots + c_{(t+1)p_2-(p_1-1)}(N)\right) = 1 \quad . \end{aligned} \tag{11}$$

Since we have $c_n(i) = 0$ for $0 \leq n < ip_2$, (11) simplifies to

$$\begin{aligned} c_{(t+1)p_2} &- \left(c_{(t+1)p_2}(0) + \dots + c_{(t+1)p_2}(N)\right) \\ &+ \left(c_{(t+1)p_2}(1) + \dots + c_{(t+1)p_2-(p_1-1)}(1)\right) + \dots \\ &\dots + \left(c_{(t+1)p_2}(t) + \dots + c_{(t+1)p_2}(t)\right) + c_{(t+1)p_2}(t+1) = 1 \quad . \end{aligned} \tag{12}$$

Since we have

$$c_{(t+1)p_2}(j) + \dots + c_{(t+1)p_2-(p_1-1)}(j) = 0 \quad ,$$

where $1 \leq j \leq t$, by (9), equation (12) simplifies to

$$\begin{aligned} c_{(t+1)p_2} &- \left(c_{(t+1)p_2}(0) + \dots + c_{(t+1)p_2}(N)\right) \\ &+ c_{(t+1)p_2}(t+1) = 1 \quad . \end{aligned} \tag{13}$$

Since $c_{(t+1)p_2}(t+1) = 1$, equation (13) becomes

$$c_{(t+1)p_2} = c_{(t+1)p_2}(0) + c_{(t+1)}(1) + \dots + c_{(t+1)p_2}(N) \quad . \qquad (14)$$

Equating coefficients of $x^{(t+1)p_2+1}$ we also have

$$c_{(t+1)p_2+1} + c_{(t+1)p_2} + \dots + c_{(t+1)p_2-p_1} = 0 \quad .$$

By an argument similar to that used in the derivation of (8), we have

$$\begin{aligned} c_{(t+1)p_2+1} &- \left(c_{(t+1)p_2+1}(0) + \dots + c_{(t+1)p_2+1}(N)\right) \\ &+ \left(c_{(t+1)p_2+1}(0) + \dots + c_{(t+1)p_2-p_1}(0)\right) + \dots \\ &\dots + \left(c_{(t+1)p_2+1}(N) + \dots + c_{(t+1)p_2-p_1}(N)\right) = 0 \quad . \qquad (15) \end{aligned}$$

Similarly, by (6) and (9) and the definition of the $c_n(k)$'s we have

$$\begin{aligned} c_{(t+1)p_2-1} &- \left(c_{(t+1)p_2+1}(0) + \dots + c_{(t+1)p_2+1}(N)\right) \\ &+ c_{(t+1)p_2+1}(t+1) + c_{(t+1)p_2}(t+1) = 0 \quad . \end{aligned}$$

Since $c_{(t+1)p_2+1}(t+1) = -1$, $c_{(t+1)p_2}(t+1) = 1$, we have

$$c_{(t+1)p_2+1} = c_{(t+1)p_2+1}(0) + \dots + c_{(t+1)p_2+1}(N) \quad .$$

Similarly we have

$$\begin{aligned} c_{(t+1)p_2+2} &= c_{(t+1)p_2+2}(0) + \dots + c_{(t+1)p_2+2}(N) \\ &\vdots \\ c_{(t+1)p_2+(p_1-1)} &= c_{(t+1)p_2+(p_1-1)}(0) + \dots + c_{(t+1)p_2+(p_1-1)}(N) \; . \end{aligned}$$

This proves (A) is true for n in the interval $(t+1)p_2 \leq n \leq (t+1)p_2 + (p_1 - 1)$. To finish the remaining cases we can assume that for all $0 \leq k \leq s$, we have

$$c_{(t+1)p_2+k} = c_{(t+1)p_2+k}(0) + \dots + c_{(t+1)p_2+k}(N) \quad ,$$

where s is such that $p_1 - 1 \leq s < p_2 - 1$ and $(t+1)p_2 + s < \dfrac{\phi(p_1 p_2)}{2}$, and show that

$$c_{(t+1)p_2+s+1} = c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(N) \quad .$$

Equating the coefficients of $x^{(t+1)p_2+s+1}$ we find

$$c_{(t+1)p_2+s+1} + \dots + c_{(t+1)p_2+s+1-(p_1-1)} = 0$$

By an argument similar to the derivation of (8) we obtain

$$\begin{aligned} c_{(t+1)p_2+s+1} &- \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(N)\right) \\ &+ \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1-(p_1-1)}(0)\right) + \dots \\ &\dots + \left(c_{(t+1)p_2+s+1}(N) + \dots + c_{(t+1)p_2+s+1-(p_1-1)}(N)\right) \\ &= 0 \end{aligned}$$

Since $c_n(i) = 0$ for $0 \leq n < ip_2$, we simplify the above equations to

$$\begin{aligned} c_{(t+1)p_2+s+1} &- \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(N)\right) \\ &+ \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1-(p_1-1)}(0)\right) + \dots \\ &\dots + \left(c_{(t+1)p_2+s+1}(t+1) + \dots + c_{(t+1)p_2+s+1-(p_1-1)}(t+1)\right) \\ &= 0. \end{aligned}$$

By the definition of $c_n(i)$'s again, we have

$$\begin{aligned} c_{(t+1)p_2+s+1} &- \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(N)\right) \\ &+ \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(0)\right) + \dots \\ &\dots + \left(c_{(t+1)p_2+s+1}(t) + \dots + c_{(t+1)p_2+s+1}(t)\right) = 0 \ . \end{aligned}$$

By (6) and (9), we find that

$$c_{(t+1)p_2+s+1} - \left(c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(N)\right) = 0 \ .$$

Hence we have

$$c_{(t+1)p_2+s+1} = c_{(t+1)p_2+s+1}(0) + \dots + c_{(t+1)p_2+s+1}(N) \ .$$

This completes the proof of Theorem 1.

<u>Corollary 1</u>: Let p_1 and p_2 be two primes such that $p_2 > p_1 > 3$. Let

$$F_{p_1p_2}(x) = \sum_{n=0}^{\phi(p_1p_2)} c_n x^n \ .$$

Then c_n is ± 1 or 0.

Proof: From Theorem 1 we have

$$c_n = c_n(0) + c_n(1) + \dots + c_n(N) \quad , \tag{16}$$

where $c_n(k)$ is ± 1 or 0, for each $k = 0, 1, \dots, N$. Hence to prove c_n is ± 1 or 0 it is sufficient to prove the following two statements:

(a) If one of the $c_n(k)$ in (16) is 1 then none of the other $c_n(k)$ in (16) can be 1.

(b) If one of the $c_n(k)$ in (16) is -1 then none of the other $c_n(k)$ in (16) can be -1.

We prove (a) by assuming the contrary. This means there exist two distinct integers k_1 and k_2 between 0 and N such that

$$c_n(k_1) = c_n(k_2) = 1 \quad .$$

According to Theorem 1, we have

$$n \equiv k_1 p_2 \pmod{p_1} \quad ,$$

where $k_1 p_2 \leq n \leq \dfrac{\phi(p_1 p_2)}{2}$, and

$$n \equiv k_2 p_2 \pmod{p_1} \quad ,$$

where $k_2 p_2 \leq n \leq \dfrac{\phi(p_1 p_2)}{2}$. Hence we can write

$$n = k_1 p_2 + m_1 p_1$$

and

$$n = k_2 p_2 + m_2 p_1 \quad ,$$

where m_1 and m_2 are two distinct integers between 0 and $N' = \left[\frac{\phi(p_1p_2)}{2p_1}\right]$. Subtracting the last two equations we have

$$(k_1 - k_2)p_2 = (m_2 - m_1)p_1 \quad .$$

Since p_1 and p_2 are two distinct primes, we have

$$p_2 | (m_2 - m_1) \quad .$$

But $0 \leq m_1, \; m_2 < \frac{p_2 - 1}{2}$, so we must have

$$0 \leq |m_2 - m_1| < \frac{p_2 - 1}{2} \quad .$$

Hence we conclude that

$$m_1 = m_2 \quad .$$

This also implies

$$k_1 = k_2 \quad .$$

This contradiction proves (a).

Now assume the contrary to (b). There exist two distinct integers k_1 and k_2 such that

$$c_n(k_1) = c_n(k_2) = -1 \quad .$$

According to Theorem 1, we have

$$n \equiv k_1p_2 + 1 \pmod{p_1} \quad ,$$

$$n \equiv k_2p_2 + 1 \pmod{p_1} \quad .$$

Hence we can write

$$n = k_1p_2 + m_1p_1 + 1 \quad ,$$

$$n = k_2p_2 + m_2p_1 + 1 \quad ,$$

where m_1 and m_2 are two integers between 0 and N'. Subtracting the last two equations we have

$$(k_1 - k_2)p_2 = (m_2 - m_1)p_1 \quad .$$

Again as in the proof of (a), this leads to a contradiction. This completes the proof of the corollary.

CHAPTER III

THE CYCLOTOMIC POLYNOMIAL $F_n(x)$ WHERE n IS THE PRODUCT OF THREE DISTINCT ODD PRIMES

3.1 Upper and Lower Bounds for the Largest Coefficient

The coefficients of a cyclotomic polynomial whose order is a product of three distinct odd primes are no longer ± 1 or 0. In fact, the coefficient of x^7 in $F_{3\cdot 5\cdot 7}(x)$ is -2. In 1895 Bang proved that no coefficient of $F_{p_1p_2p_3}(x)$ exceeds p_1-1 if $p_1 < p_2 < p_3$ are odd primes. In 1936 Emma Lehmer proved that for a given odd prime p_1 if we construct primes p_2 and p_3 such that $p_2 = kp_1 + 2$ and $p_3 = (m\, p_1p_2-1)/2$, then the coefficient of x^h is $(p_1-1)/2$, where $h = (p_1-3)(p_2p_3+1)/2$. Theorem 3 shows that for a given odd prime p_1 if we construct primes p_2 and p_3 such that $p_2 = kp_1 + 2$ and $p_3 = (m\, p_1p_2-1)/2$, then the coefficient of x^h is $(p_1+1)/2$, where $h = (p_1-1)(p_2p_3+1)/2$. Hence $(p_1-1)/2$ is not an upper bound for the coefficients of $F_{p_1p_2p_3}(x)$. Theorem 4 shows that under certain conditions Bang's upper bound (p_1-1) for the coefficients of $F_{p_1p_2p_3}(x)$ can be improved.

First we obtain a recursion formula for the coefficients of $F_{p_1p_2p_3}(x)$.

3.2 A Recursion Formula for the Cyclotomic Coefficients

<u>Theorem 2:</u> Let

$$F_{p_1p_2p_3}(x) = \sum_{n=0}^{\phi(p_1p_2p_3)} c_n x^n ,$$

where $p_1 < p_2 < p_3$ are three distinct odd primes. Let $T = \phi(p_1p_2) + \phi(p_1p_3) + (p_1-1)$, and define $e_0, e_1, \ldots, e_{T/2}$ by the relation

$$F_{p_1p_3}(x) = \sum_{n=0}^{\phi(p_1p_3)} e_n x^n \quad ,$$

and $e_n = 0$ if $\phi(p_1p_3) < n \leq T/2$. Define $f_0, f_1, \ldots, f_T$ as follows:

(a) For each $s = 0, 1, \ldots, (p_1-2)$,

$$f_n = e_{n-sp_2} + e_{n-(s-1)p_2} + \ldots + e_n \quad \text{if} \quad sp_2 \leq n < (s+1)p_2 \ ,$$

(b) $$f_n = e_{n-(p_1-1)p_2} + e_{n-(p_1-2)p_2} + \ldots + e_n$$

$$\text{if} \quad (p_1-1)p_2 \leq n \leq T/2 \ ,$$

(c) $f_n = f_{T-n}$ if $T/2 < n \leq T$.

Then we have

(A) For $0 \leq n < T$,

$$f_0c_n + f_1c_{n-1} + \ldots + f_nc_0 = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{p_2p_3} \\ 0 & \text{if } n \not\equiv 0 \pmod{p_2p_3} \end{cases} \ ,$$

(B) For $T \leq n \leq \phi(p_1p_2p_3)/2$,

$$f_0c_n + f_1c_{n-1} + \ldots + f_Tc_{n-T} = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{p_2p_3} \\ 0 & \text{if } n \not\equiv 0 \pmod{p_2p_3} \end{cases} \ ,$$

(C) For $\phi(p_1p_2p_3)/2 < n \leq \phi(p_1p_2p_3)$

$$c_n = c_{\phi(p_1p_2p_3)-n} \ .$$

Proof: By Lemma 1 we have

$$x^{p_1p_2p_3} - 1$$

$$= (x-1)\, F_{p_1}(x)\, F_{p_2}(x)\, F_{p_3}(x)\, F_{p_1p_2}(x)\, F_{p_1p_3}(x)\, F_{p_2p_3}(x)\, F_{p_1p_2p_3}(x)$$

$$= \left\{(x-1)\, F_{p_2}(x)\, F_{p_3}(x)\, F_{p_2p_3}(x)\right\} F_{p_1}(x)\, F_{p_1p_2}(x)\, F_{p_1p_3}(x)\, F_{p_1p_2p_3}(x)$$

$$= \left(x^{p_2p_3} - 1\right) F_{p_1}(x)\, F_{p_1p_2}(x)\, F_{p_1p_3}(x)\, F_{p_1p_2p_3}(x) \quad .$$

Dividing by $\left(x^{p_2p_3} - 1\right)$ we find

$$F_{p_1}(x)\, F_{p_1p_2}(x)\, F_{p_1p_3}(x)\, F_{p_1p_2p_3}(x)$$

$$= 1 + x^{p_2p_3} + x^{2p_2p_3} + \ldots + x^{(p_1-1)p_2p_3} \quad . \qquad (17)$$

We obtain the conclusion of this theorem by equating coefficients of like powers of x in (17). Let's consider

$$F_{p_1}(x)\, F_{p_1p_2}(x) = \frac{\left(x^{p_1} - 1\right)}{\left(x - 1\right)} \frac{\left(x - 1\right)\left(x^{p_1p_2} - 1\right)}{\left(x^{p_1} - 1\right)\left(x^{p_2} - 1\right)}$$

$$= 1 + x^{p_2} + x^{2p_2} + \ldots + x^{(p_1-1)p_2} \quad .$$

If we let

$$F_{p_1}(x)\, F_{p_1p_2}(x) = \sum_{n=0}^{(p_1-1)p_2} a_n\, x^n \quad ,$$

then we have

$$a_n = \begin{cases} 1 & \text{if} \quad n = kp_2 \ , \quad \text{where} \quad k = 0,\ 1,\ \ldots,\ (p_1-1) \\ 0 & \text{otherwise} \end{cases} \quad .$$

If we let

$$F_{p_1}(x)\, F_{p_1p_2}(x)\, F_{p_1p_3}(x) = \sum_{n=0}^{T} b_n x^n \quad ,$$

then we have

$$b_n = a_n e_0 + a_{n-1} e_1 + \ldots + a_0 e_n \quad .$$

Substituting the value for a_n into the above equation, we obtain

$$b_n = e_n \qquad \text{if} \quad 0 \leq n < p_2 \ ,$$

$$b_n = e_{n-p_2} + e_n \qquad \text{if} \quad p_2 \leq n < 2p_2 \ ,$$

$$\cdot$$
$$\cdot$$
$$\cdot$$

$$b_n = e_{n-sp_2} + e_{n-(s-1)p_2} + \ldots + e_{n-p_2} + e_n \qquad \text{if} \quad sp_2 \leq n < (s+1)p_2$$

and $0 \leq s < p_1 - 1$.

$$b_n = e_{n-(p_1-1)p_2} + e_{n-(p_1-2)p_2} + \ldots + e_n \qquad \text{if} \quad (p_1-1)p_2 \leq n \leq \frac{T}{2} \ .$$

Since the symmetrically located coefficients of $F_{p_1}(x)\, F_{p_1p_2}(x)\, F_{p_1p_3}(x)$ are equal, we have

$$b_n = b_{n-T/2} \qquad \text{if} \quad \frac{T}{2} < n \leq T \quad .$$

Hence we see that

$$f_n = b_n \qquad \text{if} \quad 0 \leq n \leq T \quad .$$

Then (14) becomes

$$\left(\sum_{n=0}^{T} f_n x^n\right)\left(\sum_{n=0}^{\phi(p_1p_21_3)} c_n x^n\right) = 1 + x^{p_2p_3} + x^{2p_2p_3} + \ldots + x^{(p_1-1)p_2p_3} \ .$$

Equating the coefficients of like powers of x we find:

For $0 \leq n < T$,

$$f_0c_n + f_1c_{n-1} + \ldots + f_nc_o = \begin{cases} 1 & \text{if} \quad n \equiv 0 \pmod{p_2p_3} \\ 0 & \text{if} \quad n \not\equiv 0 \pmod{p_2p_3} \end{cases}.$$

For $T \leq n \leq \phi(p_1p_2p_3)/2$,

$$f_0c_n + f_1c_{n-1} + \ldots + f_Tc_{n-T} = \begin{cases} 1 & \text{if} \quad n \equiv 0 \pmod{p_2p_3} \\ 0 & \text{if} \quad n \not\equiv 0 \pmod{p_2p_3} \end{cases}.$$

For $\phi(p_1p_2p_3)/2 < n \leq \phi(p_1p_2p_3)$,

$$c_n = c_{\phi(p_1p_2p_3) - n}$$

by the symmetry of the coefficients of $F_{p_1p_2p_3}(x)$.

Hence we complete the proof of this theorem.

Theorem 3: There exist integers n, the product of three distinct odd primes greater than 3, such that the cyclotomic polynomial $F_n(x)$ contains a coefficient which is equal to $(p_1+1)/2$, where p_1 is the smallest prime factor of n.

Proof: Given a prime $p_1 > 3$, by Dirichlet's theorem on primes in arithmetic progressions there is an integer k such that $p_2 = kp_1 + 2$ is prime. Since p_1p_2 and $(p_1p_2-1)/2$ are relatively prime, there is an integer m' such that $p_3 = m'p_1p_2 + (p_1p_2-1)/2$ is prime. Let $m = 2m' + 1$. Then $p_3 = (mp_1p_2 - 1)/2$.

From the definition of p_2, p_3 we obtain the following lemma.

Lemma 7: $p_2p_3 \equiv -1 \pmod{p_1}$; $kp_1p_3 \equiv 1 \pmod{p_2}$; $m\,p_1p_2 \equiv 1 \pmod{p_3}$; $p_2 \equiv 2 \pmod{p_1}$; $p_3 \equiv -1/2 \pmod{p_1p_2}$, that is, $2p_3 \equiv -1 \pmod{p_1p_2}$.

Proof of Lemma 7:

$$p_2p_3 = (kp_1+2)\frac{(m\,p_1p_2-1)}{2} \equiv -1 \pmod{p_1} \quad .$$

$$kp_1p_3 = kp_1\left(\frac{m\,p_1p_2-1}{2}\right) = (p_2-2)\left(\frac{m\,p_1p_2-1}{2}\right) \equiv 1 \pmod{p_2} \ .$$

$$m\,p_1p_2 = 2p_3+1 \equiv 1 \pmod{p_3} \ .$$

$$p_2 = kp_1+2 \equiv 2 \pmod{p_1} \ .$$

$$p_3 = \frac{(m\,p_1p_2-1)}{2} \equiv \frac{-1}{2} \pmod{p_1p_2} \ .$$

This completes the proof of Lemma 7.

Now let

$$h = \frac{(p_1-1)(p_2p_3+1)}{2} \quad .$$

We will show that the coefficient of x^h is $(p_1+1)/2$.

By Lemma 2 we have

$$F_{p_1p_2p_3}(x)$$

$$= \frac{\left(x^{p_1p_2p_3}-1\right)\left(x^{p_1}-1\right)\left(x^{p_2}-1\right)\left(x^{p_3}-1\right)}{\left(x^{p_2p_3}-1\right)\left(x^{p_1p_3}-1\right)\left(x^{p_1p_2}-1\right)\left(x-1\right)}$$

$$= \left\{\frac{1-x^{p_1p_2p_3}}{1-x^{p_2p_3}} \cdot \frac{1}{1-x^{p_1p_3}} \cdot \frac{1}{1-x^{p_1p_2}}\right\}\left\{\frac{1-x^{p_1}}{1-x}\right\}\left\{\left(1-x^{p_2}\right)\left(1-x^{p_3}\right)\right\}$$

$$= \left(\sum x^{i_1p_2p_3+i_2p_1p_3+i_3p_1p_2}\right)\left(\sum_{j=0}^{p_1-1} x^j\right)\left(1-x^{p_2}-x^{p_3}+x^{p_2+p_3}\right) .$$

Consider the diophantine equation

$$i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2 + j + ep_2 + fp_3 = \frac{(p_1-1)(p_2p_3+1)}{2} = h , \quad (18)$$

subject to the restrictions

$$0 \leq i_1p_2p_3 \leq h , \quad 0 \leq i_2p_1p_3 \leq h ,$$

$$0 \leq i_3p_1p_2 \leq h , \quad 0 \leq j < p_1 , \quad e = 0 \text{ or } 1 , \quad \text{and } f = 0 \text{ or } 1 . \quad (19)$$

The coefficient of x^h is the number of solutions of (18) with $e = f$, minus the number of solutions of (18) with $e \neq f$.

Now we reduce equation (18) modulo p_1, p_2, p_3 respectively, using the lemma. This gives us

$$i_1p_2p_3 + j + ep_2 + fp_3 \equiv 0 \pmod{p_1} ; \quad \text{since} \quad p_2p_3 \equiv -1 \pmod{p_1} .$$

$$i_2p_1p_3 + j + fp_3 \equiv \frac{(p_1-1)}{2} \pmod{p_2} .$$

$$i_3p_1p_2 + j + ep_2 \equiv \frac{(p_1-1)}{2} \pmod{p_3} .$$

Multiplying the last two congruences by k and m, respectively, and using Lemma 7 again, we obtain

$$j \equiv i_1 - 2e + \frac{f}{2} \qquad (\mathrm{mod}\ p_1) \quad . \tag{20}$$

$$i_2 \equiv k\left(\frac{p_1-1}{2} - j + \frac{f}{2}\right) \qquad (\mathrm{mod}\ p_2) \quad . \tag{21}$$

$$i_3 \equiv m\left(\frac{p_1-1}{2} - j - ep_2\right) \quad (\mathrm{mod}\ p_3) \quad . \tag{22}$$

Now we will show that: for $e = f = 0$, (18) has $(p_1+1)/2$ solutions; for $c = f = 1$, (18) has no solution; for $e \neq f$, (18) has no solution. This will prove that the coefficient of x^h is $(p_1+1)/2$.

Assume $e = f = 0$. Then (20) gives $j \equiv i_1 \pmod{p_1}$. Since $j \leq (p_1-1)$ and $i_1 < p_1$, we obtain $j = i_1$. Substituting $j = i_1$ into the equations (21) and (22), we have

$$i_2 \equiv k\left(\frac{p_1-1}{2} - i_1\right) \quad (\mathrm{mod}\ p_2) \quad . \tag{23}$$

$$i_3 \equiv m\left(\frac{p_1-1}{2} - i_1\right) \quad (\mathrm{mod}\ p_3) \quad . \tag{24}$$

Since $i_1p_2p_3 \leq h$, we have

$$i_1 \leq \frac{\left((p_1-1)/2\right)(p_2p_3+1)}{p_2p_3} = \frac{(p_1-1)}{2}\left(1 + \frac{1}{p_2p_3}\right) = \frac{p_1-1}{2} + \frac{(p_1-1)}{2p_2p_3} \quad .$$

Since i_1 is an integer, we obtain $i_1 \leq (p_1-1)/2$. Since $p_2 = kp_1+2$, we have $k(p_1-1)/2 < p_2$. Since $p_1p_3i_2 \leq h$, we have

$$i_2 \leq \frac{\left((p_1-1)/2\right)(p_2p_3+1)}{p_1p_3} = \frac{(p_1-1)}{2p_1}\left(p_2 + \frac{1}{p_3}\right)$$

$$= \frac{(p_1-1)}{2p_1}\,p_2 + \frac{p_1-1}{2p_1p_3} < p_2 \quad .$$

Therefore we conclude that (23) is an equality,

$$i_2 = k\left(\frac{p_1-1}{2} - i_1\right) . \tag{23'}$$

Since $p_3 = \dfrac{m\,p_1p_2-1}{2}$, we have $\dfrac{m(p_1-1)}{2} < p_3$. Since $p_1p_2i_3 \leq h$, we have

$$i_3 \leq \frac{\left[(p_1-1)/2\right](p_2p_3+1)}{p_1p_2} = \left(\frac{p_1-1}{2p_1}\right)\left(p_3 + \frac{1}{p_2}\right) = \frac{(p_1-1)}{2p_1}\,p_3 + \frac{p_1-1}{2p_2p_1} < p_3 \quad .$$

Hence we conclude that (24) is an equality,

$$i_3 = m\left(\frac{p_1-1}{2} - i_1\right) . \tag{24'}$$

Since $0 \leq i_1 \leq \dfrac{(p_1-1)}{2}$, there are $(p_1+1)/2$ choices of values for i_1. If we can show that for each choice of i_1 we have $i_2p_1p_3 \leq h$ and $i_3p_1p_2 \leq h$, then we can conclude that (18) has $(p_1+1)/2$ solutions in the case $e = f = 0$. By (23') we have $i_2 \leq \dfrac{k(p_1-1)}{2}$. Hence we have

$$i_2p_1p_3 \leq kp_1p_3\,\frac{(p_1-1)}{2} = (p_1-2)\;p_3\,\frac{(p_1-1)}{2} < \frac{p_1-1}{2}\cdot(p_2p_3) < h \quad .$$

Since we have $i_3 \leq \dfrac{m(p_1-1)}{2}$ by (21'), we have

$$i_3p_1p_3 \leq m\,p_1p_2\,\frac{(p_1-1)}{2} = \frac{(2p_3+1)(p_1-1)}{2} < h \quad .$$

Next assume $e = 1$, $f = 0$: (20) becomes $j \equiv i_1 - 2 \pmod{p_1}$.

Hence we obtain $j = i_1 - 2$ if $i_1 \neq 0, 1$; $j = p_1 - 1$ if $i_1 = 1$; $j = p_1 - 2$ if $i_1 = 0$. For the last two cases we can use (21) to get

$$i_2 \equiv k\left(\frac{p_1-1}{2} - j\right) \equiv \begin{cases} -k\dfrac{(p_1-1)}{2} \pmod{p_2}; & \text{if } j = p_1 - 1 \\ -k\dfrac{(p_1-3)}{3} \pmod{p_2}; & \text{if } j = p_1 - 2 \end{cases} .$$

Hence we have

$$i_2 = \left\{\begin{matrix} p_2 - \dfrac{k(p_1-1)}{2} \\ \\ p_2 - \dfrac{k(p_1-3)}{2} \end{matrix}\right\} \geq p_2 - \frac{k(p_1-1)}{2} .$$

Hence we have

$$\begin{aligned} i_2p_1p_3 &\geq p_1p_2p_3 - \frac{kp_1p_3(p_1-1)}{2} = p_1p_2p_3 - \frac{(p_2-2)p_3(p_1-1)}{2} \\ &= p_1p_2p_3 - p_2p_3\,\frac{p_1-1}{2} + p_3(p_1-1) = p_2p_3\frac{p_1+1}{2} + p_3(p_1-1) > h . \end{aligned}$$

For the case $j = i_1 - 2$: Since $i_1 \leq \frac{p_1-1}{2}$, we have $j \leq \frac{p_1-5}{2}$. We are still in the case $e = 1$, $f = 0$. Hence (22) becomes

$$i_3 \equiv m\left(\frac{p_1-1}{2} - j - p_2\right) \pmod{p_3} .$$

Hence we obtain

$$\begin{aligned} i_3 &= p_3 + m\left(\frac{p_1-1}{2} - j - p_2\right) \\ &\geq p_3 + m\left(\frac{p_1-1}{2} - \frac{p_1-5}{2} - p_2\right) \\ &= p_3 + m(2-p_2) \quad . \end{aligned}$$

Hence, since $m p_1 p_2 = 2p_3 + 1$, we have

$$\begin{aligned} i_3 p_1 p_2 &= p_1 p_2 p_3 + m p_1 p_2 (2-p_2) \\ &= p_1 p_2 p_3 + (2p_3+1)(2-p_2) \\ &= (p_2 p_3 + 1)(p_1 - 2) + (4p_3 - p_2 + p_1 + 4) \\ &> (p_2 p_3 + 1)(p_1 - 2) \\ &> h \quad . \end{aligned}$$

Hence for $e = 1$, $f = 0$, (19) is violated. Hence we conclude that (18) has no solution for $e = 1$, $f = 0$.

Assume $e = 0$, $f = 1$. Then from (20) we have $j = i_1 + \dfrac{(p_1+1)}{2}$. Substituting this value of j into (22), we have

$$\begin{aligned} i_3 &\equiv m\left(\frac{p_1-1}{2} - i_1 - \frac{p_1+1}{2}\right) \pmod{p_3} \\ &\equiv -m(1+i_1) \pmod{p_3} \quad . \end{aligned}$$

Hence we obtain

$$\begin{aligned} i_3 &= p_3 - m(1+i_1) \\ &\geq p_3 - m\left(1 + \frac{p_1-1}{2}\right) \\ &= p_3 - \frac{m\cdot(p_1+1)}{2} \quad . \end{aligned}$$

Hence we have

$$i_3p_1p_2 = p_1p_2p_3 - m\,p_1p_2\,\frac{(p_1-1)}{2}$$

$$= p_1p_2p_3 - (2p_3+1)\,\frac{(p_1+1)}{2}$$

$$= \frac{2p_1p_2p_3 - 2p_1p_3 - 2p_3 - p_1 - 1}{2} \quad .$$

Assume

$$\frac{2p_1p_2p_3 - 2p_1p_3 - 2p_2 - p_1 - 1}{2} \leq h = \frac{(p_1-1)(p_2p_3+1)}{2} \quad .$$

Then we have

$$2p_1p_2p_3 - 2p_1p_3 - 2p_2 - p_1 - 1 \leq p_1p_2p_3 - p_2p_3 + p_1 - 1 \quad .$$

Hence we obtain

$$p_1p_2p_3 + p_2p_3 - 2p_1p_3 - 2p_2 - 2p_1 \leq 0$$

or $$(p_1p_2p_3 - 2p_1p_3) + (p_2p_3 - 2p_2 - 2p_1) \leq 0 \quad . \qquad (*)$$

Since $p_2 > 2$ and $p_2p_3 - 2p_2 - 2p_1 > p_2p_3 - 4p_2 = p_2(p_3-4) > 0$ we have proved that the inequality (*) is not true. Hence we conclude that

$$i_2p_1p_2 = \frac{2p_1p_2p_3 - 2p_1p_3 - 2p_3 - p_1 - 1}{2} > h \quad .$$

Hence for $e = 1$, $f = 0$, (19) is violated. Hence (18) has no solution for $e = 1$, $f = 0$.

Assume $e = f = 1$. Then from (20) we have $j \equiv i_1 - 2 - \frac{1}{2} \equiv i_1 - \frac{3}{2} \pmod{p_1}$. Hence we have $j = i_1 + (p_1-3)/2$. Substituting into (21) and (22), we have

$$i_3 \equiv m\left(\frac{p_1-1}{2} - i_1 - \frac{p_1-3}{2} - p_2\right) \pmod{p_3}$$

$$\equiv m\Big((1 - i_1) - p_2\Big) \pmod{p_3} \quad .$$

Hence we have

$$i_3 = p_3 - m\Big(p_2 - (i_1-1)\Big) \geq p_3 - m(p_2+1) \quad .$$

$$i_3p_1p_2 \geq p_1p_2p_3 - m\,p_1p_2\,(p_2+1)$$

$$= p_1p_2p_3 - (2p_3+1)\,(p_2+1)$$

$$= p_1p_2p_3 - 2p_2p_3 - 2p_3 - p_2 - 1 \quad .$$

Assume

$$p_1p_2p_3 - 2p_2p_3 - 2p_3 - p_2 - 1 \leq h = \frac{(p_1-1)(p_2p_3+1)}{2} \quad .$$

Then we have

$$2p_1p_2p_3 - 4p_2p_3 - 4p_3 - 2p_2 - 2 \leq p_1p_2p_3 - p_2p_3 + p_1 - 1 \quad .$$

Hence we obtain

$$p_1p_2p_3 - 3p_2p_3 - 4p_3 - 2p_2 - p_1 - 1 \leq 0 \quad . \qquad (**)$$

But

$$p_2p_3(p_1-3) - 4p_3 - 2p_2 - p_1 - 1 > p_2p_3(p_1-3) - 8p_3$$

$$= p_3\Big(p_2(p_1-3) - 8\Big) > 0 \text{ since } p_1 > 3 \quad .$$

Hence (**) is not true. Hence

$$i_3p_1p_2 = p_1p_2p_3 - 2p_2p_3 - 2p_3 - p_2 - 1 > h \quad .$$

Hence for $e = f = 1$, (15) has no solution. This proves that the coefficient of x^h is $(p_1+1)/2$, where $h = (p_1-1)(p_2p_3+1)/2$.

3.3 Improvement of Bang's Upper Bound

Theorem 4: Let

$$F_{p_1p_2p_3}(x) = \sum_{n=0}^{\phi(p_1p_2p_3)} c_n x^n ,$$

where p_1, p_2, p_3 are three distinct odd primes. If there exists an integer m such that for each integer k satisfying $1 \leq k \leq m < \frac{p_1-1}{4} + 1$, the diophantine inequality

$$|kp_2p_3 + s_2p_1p_3 + s_3p_1p_2| \leq p_1 - 1$$

has no solution in the domain $|s_2| \leq \frac{p_2-1}{2} - 1$ and $|s_3| \leq \frac{p_3-1}{2} - 1$, then

$$|c_n| \leq -2\left[\frac{-(p_1-1)}{2(m+1)}\right] .$$

Note: The upper bound for $|c_n|$ does not exceed p_1-1. The upper bound is equal to p_1-1 when $m=0$. This is the case proved by Bang.

Proof: By Lemma 1 we have

$$F_{p_1p_2p_3}(x) = \frac{\left(x^{p_1p_2p_3} - 1\right)\left(x^{p_1} - 1\right)\left(x^{p_2} - 1\right)\left(x^{p_3} - 1\right)}{\left(x^{p_1p_2} - 1\right)\left(x^{p_1p_3} - 1\right)\left(x^{p_2p_3} - 1\right)\left(x - 1\right)}$$

$$= \frac{x^{p_1p_2p_3} - 1}{x^{p_2p_3} - 1} \cdot \frac{1}{x^{p_1p_3} - 1} \cdot \frac{1}{x^{p_1p_2} - 1} \cdot \frac{x^{p_1} - 1}{x - 1}\left(x^{p_2} - 1\right)\left(x^{p_3} - 1\right)$$

$$= \left(\sum x^{i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2}\right)\left(\sum_{j=0}^{p_1-1} x^j\right)\left(1 - x^{p_2} - x^{p_3} + x^{p_2+p_3}\right).$$

If we let $\sum x^{i_1p_2p_3+i_2p_1p_3+i_3p_1p_2} = \sum a_n x^n$ then we obtain

$$F_{p_1p_2p_3}(x) = \left(\sum a_n x^n\right)\left(\sum_{j=0}^{p_1-1} x^j\right)\left(1-x^{p_2}-x^{p_3}+x^{p_2+p_3}\right) .$$

If we let

$$\left(\sum a_n x^n\right)\left(\sum_{j=0}^{p_1-1} x^j\right) = \sum b_n x^n ,$$

then we obtain

$$F_{p_1p_2p_3}(x) = \left(\sum b_n x^n\right)\left(1-x^{p_2}-x^{p_3}+x^{p_2+p_3}\right) = \sum c_n x^n , \qquad (***)$$

where $b_n = a_n + a_{n-1} + \dots + a_{n-(p_1-1)}$, $a_i = 0$ if $i < 0$.

Since a_n and b_n are nonnegative, from (***) we can see that $|c_n| \le 2 \max_n |b_n|$. Hence we need to find a bound for $\max_n |b_n|$.

Since we need only to consider those c_n's such that $n \le \phi(p_1p_2p_3)/2$, we have

$$0 \le i_1 \le \frac{p_1-1}{2} - 1 , \quad 0 \le i_2 \le \frac{p_2-1}{2} - 1 , \quad 0 \le i_3 \le \frac{p_3-1}{2} - 1 . \qquad (25)$$

Assertion 1: For a given $n \le \phi(p_1p_2p_3)/2$ we have $a_n = 1$, if $n = i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2$ has solution; $a_n = 0$, if $n = i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2$ has no solution.

Proof: From its definition, a_n is the number of solutions of

$$n = i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2 . \qquad (26)$$

Hence to prove the assertion we need to prove that for a given n (26) has at most one solution.

Suppose (26) has two solutions (i_1, i_2, i_3) and (i_1', i_2', i_3'). Then we have

$$0 = (i_1 - i_1')\, p_2p_3 + (i_2 - i_2')\, p_1p_3 + (i_3 - i_3')\, p_1p_2 \quad . \qquad (27)$$

Hence we obtain

$$p_1 \mid (i_1 - i_1')\, p_2p_3 \quad .$$

Since p_1, p_2, p_3 are three distinct primes, we have

$$p_1 \mid (i_1 - i_1') \quad .$$

Since $0 \leq i_1,\ i_1' \leq \frac{(p_1 - 1)}{2} - 1$, we also have

$$i_1 - i_1' = 0 \quad ,$$

or

$$i_1 = i_1' \quad .$$

Substituting into (27), we have

$$0 = (i_2 - i_2')\, p_1p_3 + (i_3 - i_3')\, p_1p_2 \quad .$$

Hence we obtain

$$p_2 \mid (i_2 - i_2') \quad .$$

Since $0 \leq i_2,\ i_2' \leq \frac{(p_2 - 1)}{2} - 1$, we conclude that

$$i_2 = i_2' \quad .$$

Hence we also have

$$i_3 = i_3' \quad .$$

This completes the proof of the assertion.

From $b_n = a_n + a_{n-1} + \dots + a_{n-(p-1)}$ and assertion 1 we conclude that for a given $n \leq \phi(p_1p_2p_3)/2$ the coefficient b_n is the number of the following equations which have a solution:

$$\begin{aligned} n &= i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_3 \\ n-1 &= i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2 \\ &\vdots \\ n-(p_1-1) &= i_1p_2p_3 + i_2p_1p_3 + i_3p_1p_2 \ , \end{aligned} \tag{28}$$

where the equations with left-hand side negative are omitted.

<u>Assertion 2</u>: If two equations in (28) have solutions, their values for i_1 must be different.

<u>Proof</u>: Suppose not. Then we have

$$\begin{aligned} n-i &= e_1p_2p_3 + e_2p_1p_3 + e_3p_1p_2 \ , \\ n-j &= e_1p_2p_3 + e_2'p_1p_3 + e_3'p_1p_2 \ , \end{aligned}$$

where $i \neq j$ and $0 \leq i, j \leq p_1 - 1$. Hence we obtain

$$i-j = (e_2 - e_2')\, p_1p_3 + (e_3 - e_3')\, p_1p_2 \ .$$

Hence we have

$$p_1 \mid (i-j) \ .$$

Since $0 \leq i, j \leq p_1 - 1$, this implies

$$i = j \ ,$$

a contradiction. This proves assertion 2.

Using the inequalities $0 \leq i_1 \leq \frac{p_1-1}{2} - 1$ and assertion 2, we conclude that in (28) there are at most $(p_1-1)/2$ equations which have solutions and their values for i_1 are distinct. We can rearrange them according to increasing values of i_1 as follows:

$$\begin{aligned} n-j_0 &= 0\, p_2p_3 + i_2p_1p_3 + i_3p_1p_2 \\ n-j_1 &= 1\, p_2p_3 + i_2p_1p_3 + i_3p_1p_2 \\ &\vdots \\ n-j_{\frac{(p_1-1)}{2}-1} &= \left(\frac{p_1-1}{2} - 1\right) p_2p_3 + i_2p_1p_3 + i_3p_1p_2 \ , \end{aligned} \tag{29}$$

where $\left(j_0, j_1, \ldots, j_{\frac{p_1-1}{2}-1}\right)$ is a subset of $0, 1, \ldots, (p_1-1)$.

The coefficient b_n is the number of equations in (29) which have a solution. Hence we have $\max|b_n| \leq (p_1-1)/2$ and $|c_n| \leq p_1-1$, which is Bang's bound.

Notice that if $p_1 > 3$, the system (29) contains more than one equation.

If we subtract each equation from its predecessor in (29), we have

$$j_t - j_{t-1} = p_2p_3 + s_2p_1p_3 + s_3p_1p_2$$

or

$$|p_2p_3 + s_2p_1p_3 + s_3p_1p_2| \leq p_1 - 1 \quad , \tag{30}$$

where

$$|s_2| \leq \frac{p_2-1}{2} - 1 \quad \text{and} \quad |s_3| \leq \frac{p_3-1}{2} - 1 \quad .$$

Hence if (30) does not have a solution, then the maximal number of solvable equations in system (29) is reduced to:

$$\frac{p_1-1}{2\cdot 2}\ , \qquad \text{when} \quad \frac{p_1-1}{2} \quad \text{is even ;}$$

$$\frac{p_1-1}{2\cdot 2}+1\ , \quad \text{when} \quad \frac{p_1-1}{2} \quad \text{is odd .}$$

Putting this into one formula, we find that the maximal number of solvable equations in system (29) is reduced to

$$-\left[-\frac{p_1-1}{2\cdot 2}\right] \ .$$

If we subtract each equation from its second predecessor in (29), we have

$$|2p_2p_3 + s_2p_1p_3 + s_3p_1p_2| \leq p_1 - 1 \quad , \tag{31}$$

where

$$|s_2| \leq \frac{p_2-1}{2} - 1 \qquad \text{and} \qquad |s_3| \leq \frac{p_3-1}{2} - 1 \ .$$

Hence if (30) and (31) do not have a solution, then the maximal number of solvable equations in system (29) is reduced to

$$-\left[-\frac{(p_1-1)}{2\cdot 3}\right] \ .$$

This process continues. Since there are only $(p_1-1)/2$ equations in (29), we will reach a largest integer $m \leq (p_1-1)/4 + 1$ such that for each k satisfying $1 \leq k \leq m < (p_1-1)/4 + 1$ the diophantine inequality

$$|kp_2p_3 + s_2p_1p_3 + s_3p_1p_2| \leq p_1 - 1$$

has no solution in the domain

$$|s_2| \leq \frac{p_2-1}{2} - 1 \quad \text{and} \quad |s_3| \leq \frac{p_3-1}{2} - 1 \ .$$

Then the maximal number of solvable equations in (29) is reduced to

$$-\left[\frac{-(p_1-1)}{2(m+1)}\right] \ .$$

This completes the proof of this theorem.

CHAPTER IV

THE CYCLOTOMIC POLYNOMIAL $F_n(x)$ WHERE n IS THE PRODUCT OF FOUR DISTINCT ODD PRIMES

This chapter develops properties of $F_{p_1p_2p_3p_4}(x)$, where $p_1 < p_2 < p_3 < p_4$ are odd primes. Theorem 5 gives recursion formulas for the cyclotomic coefficients. Theorems 6 and 7 give upper bounds for the coefficients derived from Theorem 5.

4. 1 A Recursion Formula for the Coefficients

From Lemma 2 we have

$$F_{p_1p_2p_3p_4}(x)$$

$$= \frac{\left(x^{p_1p_2p_3p_4}-1\right)\left(x^{p_1p_2}-1\right)\left(x^{p_1p_3}-1\right)\left(x^{p_1p_4}-1\right)\left(x^{p_2p_3}-1\right)\left(x^{p_2p_4}-1\right)\left(x-1\right)}{\left(x^{p_1p_2p_3}-1\right)\left(x^{p_1p_3p_4}-1\right)\left(x^{p_1p_2p_4}-1\right)\left(x^{p_2p_3p_4}-1\right)\left(x^{p_1}-1\right)\left(x^{p_2}-1\right)\left(x^{p_3}-1\right)\left(x^{p_4}-1\right)}$$

$$= \frac{1-x^{p_1p_2p_3p_4}}{1-x^{p_2p_3p_4}} \cdot \frac{1}{1-x^{p_1p_3p_4}} \cdot \frac{1}{1-x^{p_1p_2p_4}} \cdot \frac{1}{1-x^{p_1p_2p_3}} \cdot \frac{1-x^{p_1p_2}}{1-x^{p_1}}$$

$$\cdot \frac{1-x^{p_2p_3}}{1-x^{p_2}} \cdot \frac{1-x^{p_1p_3}}{1-x^{p_3}} \cdot \frac{1-x^{p_1p_4}}{1-x^{p_4}} \cdot \left(1-x^{p_2p_4}\right)\left(1-x^{p_3p_4}\right)\left(1-x\right)$$

$$= \left(\sum_{i_1=0}^{p_1-1} x^{i_1p_2p_3p_4}\right)\left(\sum_{i_2=0}^{p_2-1} x^{i_2p_1p_3p_4}\right)\left(\sum_{i_3=0}^{p_3-1} x^{i_3p_1p_2p_4}\right)\left(\sum_{i_4=0}^{p_4-1} x^{i_4p_1p_2p_3}\right)$$

$$\cdot \left(\sum_{j_1 -0}^{p_2-1} x^{j_1 p_1}\right)\left(\sum_{j_2=0}^{p_3-1} x^{j_2 p_2}\right)\left(\sum_{j_3=0}^{p_1-1} x^{j_3 p_3}\right)\left(\sum_{j_4=0}^{p_1-1} x^{j_4 p_4}\right)$$

$$\cdot \left(1 - x - x^{p_2p_4} + x^{p_2p_4+1} - x^{p_3p_4} + x^{p_3p_4+1} + x^{p_2p_4+p_3p_4} - x^{p_2p_4+p_3p_4+1}\right).$$

Let

$$\left(\sum_{i_1=0}^{p_1-1} x^{i_1 p_2 p_3 p_4}\right)\left(\sum_{i_2=0}^{p_2-1} x^{i_2 p_1 p_3 p_4}\right)\left(\sum_{i_3=0}^{p_3-1} x^{i_3 p_1 p_2 p_4}\right)$$

$$\left(\sum_{i_4=0}^{p_4-1} x^{i_4 p_1 p_2 p_3}\right) = \Sigma\, a_n x^n \quad .$$

Then a_n is equal to the number of solutions of $n = i_1p_2p_3p_4 + i_2p_1p_3p_4 + i_3p_1p_2p_4 + i_4p_1p_2p_3$. Now we will prove that:

$$a_n = 1 \quad \text{if} \quad n = i_1p_2p_3p_4 + i_2p_1p_3p_4 + i_3p_1p_2p_4 + i_4p_1p_2p_3 \tag{33}$$

has a solution in the range $0 \leq i_1 \leq p_1-1$,
$0 \leq i_2 \leq p_2-1$, $0 \leq i_3 \leq p_3-1$, $0 \leq i_4 \leq p_4-1$;

$a_n = 0$ otherwise.

It is sufficient to prove that if $a_n \neq 0$ then $a_n = 1$. Suppose not. That is, assume there are two solutions for some n, say

$$n = i_1p_2p_3p_4 + i_2p_1p_3p_4 + i_3p_1p_2p_4 + i_4p_1p_2p_3$$
$$= i_1'p_2p_3p_4 + i_2'p_1p_3p_4 + i_3'p_1p_2p_4 + i_4'p_1p_2p_3 \quad ,$$

where $(i_1, i_2, i_3, i_4) \neq (i_1', i_2', i_3', i_4')$ with i_j and i_j' lying in the specified intervals. Then we obtain

$$(i_1 - i_1') \, p_2p_3p_4 + (i_2 - i_2') \, p_1p_3p_4 + (i_3 - i_3') \, p_1p_2p_4 + (i_4 - i_4') \, p_1p_2p_3 = 0 \quad . \tag{34}$$

Hence

$$p_1 | (i_1 - i_1') \quad .$$

Since $|i_1 - i_1'| \leq p_1 - 1$, we conclude that

$$i_1 = i_1' \quad .$$

Then (34) becomes

$$(i_2 - i_2') \, p_3p_4 + (i_3 - i_3') \, p_2p_4 + (i_4 - i_4') \, p_2p_3 = 0 \quad . \tag{35}$$

Hence

$$p_2 | (i_2 - i_2') \quad .$$

Since $|i_2 - i_2'| \leq p_2 - 1$, we conclude that

$$i_2 = i_2' \quad .$$

Then (35) becomes

$$(i_3 - i_3') \, p_4 + (i_4 - i_4') \, p_3 = 0 \quad .$$

Hence

$$p_3 | (i_3 - i_3') \quad .$$

Since $|i_3 - i_3'| \leq p_3 - 1$, we conclude that

$$i_3 = i_3' \quad .$$

Hence we also have

$$i_4 = i_4' \quad ,$$

contrary to the relation $(i_1, i_2, i_3, i_4) \neq (i_1', i_2', i_3', i_4')$. This proves (33).

Let

$$\left(\sum_{j_1=0}^{p_2-1} x^{j_1p_1}\right)\left(\sum_{j_3=0}^{p_1-1} x^{j_3p_3}\right) = \sum_{n=0}^{(p_2-1)p_1+(p_1-1)p_3} b_n x^n .$$

If we consider that b_n's are obtained by multiplying each term in

$$\sum_{j_1=0}^{p_2-1} x^{j_1p_1} \quad \text{with} \quad \sum_{j_3=0}^{p_1-1} x^{j_3p_3} ,$$

we have

$$\begin{aligned} b_n &= 1 \quad \text{if} \quad n \equiv kp_1 \pmod{p_3} \ \text{and} \ kp_1 \leq n \leq kp_1 + (p_1-1)\,p_3 \\ &\qquad \text{where} \ \ 0 \leq k \leq p_2-1 \ ; \qquad (36) \\ b_n &= 0 \quad \text{otherwise} . \end{aligned}$$

Let

$$\left(\sum_{j_2=0}^{p_3-1} x^{j_2p_2}\right)\left(\sum_{j_4=0}^{p_1-1} x^{j_4p_4}\right) = \sum_{n=0}^{(p_3-1)p_2+(p_1-1)p_4} d_n x^n .$$

Then we obtain, as above,

$$\begin{aligned} d_n &= 1 \quad \text{if} \quad n \equiv kp_2 \pmod{p_4} \ \text{and} \ kp_2 \leq n \leq kp_2 + (p_1-1)\,p_4 \\ &\qquad \text{where} \ \ 0 \leq k \leq p_3-1 \ ; \qquad (37) \\ d_n &= 0 \quad \text{otherwise} . \end{aligned}$$

Let $N = (p_2-1)\,p_1 + (p_1-1)\,p_3 + (p_3-1)\,p_2 + (p_1-1)\,p_4$; $N_1 = (p_2-1)\,p_1 + (p_1-1)\,p_3$; $N_2 = (p_3-1)\,p_2 + (p_1-1)\,p_4$. Write

$$\left(\sum_{n=0}^{N_1} b_n x^n\right)\left(\sum_{n=0}^{N_2} d_n x^n\right) = \sum_{n=0}^{N} e_n x^n \quad .$$

Then we have

$$e_n = b_n d_0 + b_{n-1} d_1 + \ldots . \; b_0 d_n \qquad \text{if} \;\; 0 \leq n < N_1$$

$$e_n = b_{N_1} d_{n-N_1} + b_{N_1-1} d_{n-N_1+1} + \ldots + b_0 d_0 \quad \text{if} \;\; N_1 \leq n < N_2$$

$$e_n = b_{N_1} d_{n-N_1} + \ldots + b_{n-N_2} d_{N_2} \qquad \text{if} \;\; N_2 \leq n \leq N \quad .$$

Let

$$\left(\sum a_n x^n\right)\left(\sum_{n=0}^{N} e_n x^n\right) = \sum f_n x^n \quad .$$

Then we have

$$f_n = e_n a_0 + e_n a_1 + \ldots + e_0 a_n \qquad \text{if} \;\; 0 \leq n < N$$

$$f_n = e_N a_{n-N} + e_{N-1} a_{n-N+1} + \ldots + e_0 a_n \;\; \text{if} \;\; N \leq n \leq \frac{1}{2}\phi(p_1 p_2 p_3 p_4) \quad .$$

Hence we obtain

$$\sum_{n=0}^{\phi(p_1 p_2 p_3 p_4)} c_n x^n = F_{p_1 p_2 p_3 p_4}(x)$$

$$= \left(\sum f_n x^n\right)\left(1 - x - x^{p_2 p_4} + x^{p_2 p_4 + 1} - x^{p_3 p_4} + x^{p_3 p_4 + 1} + x^{p_2 p_4 + p_3 p_4} - x^{p_2 p_4 + p_3 p_4 + 1}\right) \qquad (38)$$

Equating coefficients of like powers we find

$$c_0 = f_0 = 1$$

$$c_n = f_n - f_{n-1} \qquad \text{if} \quad 1 \leq n \leq p_2 p_4 - 1$$

$$c_n = f_n - f_{n-1} - f_0 \qquad \text{if} \quad n = p_2p_4$$

$$c_n = f_n - f_{n-1} + f_{n-(p_2p_4+1)} - f_{n-p_2p_4} \qquad \text{if} \quad p_2p_4 + 1 \le n \le p_3p_4 - 1$$

$$c_n = f_n - f_{n-1} + f_{n-(p_2p_4+1)} - f_{n-p_2p_4} - f_0 \qquad \text{if} \quad n = p_3p_4$$

$$c_n = f_n - f_{n-1} + f_{n-(p_2p_4+1)} - f_{n-p_2p_4} + f_{n-(p_3p_4+1)} - f_{n-p_3p_4}$$

$$\text{if} \quad p_3p_4 + 1 \le n \le p_2p_4 + p_3p_4 - 1$$

$$c_n = f_n - f_{n-1} + f_{n-(p_2p_4+1)} - f_{n-1_21_4} + f_{n-(p_3p_4+1)} - f_{n-p_3p_4} + f_0$$

$$\text{if} \quad n = p_2p_4 + p_3p_4$$

$$c_n = f_n - f_{n-1} + f_{n-(p_2p_4+1)} - f_{n-p_2p_4} + f_{n-(p_3p_4+1)} f_{n-p_3p_4}$$

$$+ f_{n-(p_2p_4+p_3p_4)} - f_{n-(p_2p_4+p_3p_4+1)}$$

$$\text{if} \quad p_2p_4 + p_3p_4 + 1 \le n \le \frac{1}{2}\phi(p_1p_2p_3p_4)$$

Hence we have the following theorem:

<u>Theorem 5</u>: Let $F_{p_1p_2p_3p_4}(x) = \sum c_n x^n$ be the cyclotomic polynomial. Let:

$$b_n = \begin{cases} 1 & \text{if } n \equiv kp_1 \pmod{p_3} \text{ and } kp_1 \le n \le kp_1 + (p_1-1)p_3 \\ & \quad \text{where } 0 \le k \le p_2 - 1 \ ; \\ 0 & \text{otherwise} \ . \end{cases}$$

$$d_n = \begin{cases} 1 & \text{if } n \equiv kp_2 \pmod{p_4} \text{ and } kp_2 \le n \le kp_2 + (p_1-1)p_4 \\ & \quad \text{where } 0 \le k \le p_2 - 1 \ ; \\ 0 & \text{otherwise} \ . \end{cases}$$

$$a_n = \begin{cases} 1 & \text{if } n = i_1p_2p_3p_4 + i_2p_1p_2p_3 + i_3p_1p_2p_4 + i_4p_1p_2p_3 \\ & \quad \text{has a positive integral solution ;} \\ 0 & \text{otherwise .} \end{cases}$$

$$N = (p_2-1)\, p_1 + (p_1-1)\, p_3 + (p_3-1)\, p_2 + (p_1-1)\, p_4$$

$$N_1 = (p_2-1)\, p_1 + (p_1-1)\, p_3$$

$$N_2 = (p_3-1)\, p_2 + (p_1-1)\, p_4$$

$$e_n = \begin{cases} b_nd_0 + \ldots + b_0d_n & \text{if } 0 \le n < N_1 \\ b_{N_1}d_{n-N_1} + \ldots + b_0d_n & \text{if } N_1 \le n < N_2 \\ b_{N_1}d_{n-N_1} + \ldots + b_{n-N_2}d_{N_2} & \text{if } N_2 \le n \le N \ . \end{cases}$$

$$f_n = \begin{cases} e_na_0 + \ldots + e_0a_n & \text{if } 0 \le n < N \\ e_Na_{n-N} + \ldots + e_0a_n & \text{if } N \le n \le \frac{1}{2}\,\phi(p_1p_2p_3p_4) \ . \end{cases}$$

Then

$$c_n = f_n - f_{n-1} + f_{n-(p_2p_4+1)} - f_{n-p_2p_4} + f_{n-(p_3p_4+1)}$$
$$- f_{n-p_3p_4} + f_{n-(p_2p_4+p_3p_4)} - f_{n-(p_2p_4+p_3p_4+1)} \ ,$$
$$\text{where} \quad f_i = 0 \ \text{ if } \ i < 0 \ .$$

4.2 Upper Bounds for the Coefficients

Theorem 6: Adopt the same notations as in Theorem 5. Let α be the maximum number of nonzero a_n's for n in the range $k \le n \le k + N \le \frac{1}{2}\,\phi(p_1p_2p_3p_4)$ for any integer $k \ge 0$; let

$\beta = \max_{0 \leq n \leq N} |e_n - e_{n-1}|$. Then

$$|c_n| \leq 4\,\alpha\beta \quad .$$

Proof: From Theorem 5 we have

$$\begin{aligned} |c_n| &\leq 4 \max |f_n - f_{n-1}| \\ &\leq 4 \max (a_{n-N} + \dots + a_n) \max |e_n - e_{n-1}| \\ &= 4\,\alpha\,\beta \quad . \end{aligned}$$

FromTheorem 6 we see that the differences between successive f_n's keep the values of c_n's small. If we consider only the positive part, we obtain an upper bound for $|c_n|$.

Theorem 7: Let $F_{p_1p_2p_3p_4}(x) = \sum c_n x^n$ be the cyclotomic polynomial, where $p_1 < p_2 < p_3 < p_4$ are distinct odd primes. Then

$$|c_n| \leq p_1^{\,2}\,(p_2 - 1)(p_3 - 1) \quad .$$

Proof: In equation (38) we proved the formula

$$\begin{aligned} F_{p_1p_2p_3p_4}(x) = &\left(\sum f_n x^n\right) \\ &\left(1 - x - x^{p_2p_4} + x^{p_2p_4+1} - x^{p_3p_4} + x^{p_3p_4+1}\right. \\ &\left. + x^{p_2p_4+p_3p_4} - x^{p_2p_4+p_3p_4+1}\right) \end{aligned} \tag{39}$$

where

$$\sum f_n x^n = \sum x^{i_1p_2p_3p_4+i_2p_1p_3p_4+i_3p_1p_2p_4+i_4p_1p_2p_3+j_1p_1+j_2p_2+j_3p_3+j_4p_4} \; .$$

We need only consider those n in the interval $0 \leq n \leq \frac{1}{2} \phi(p_1p_2p_3p_4)$. For these n, f_n is the number of solutions of

$$n = i_1p_2p_3p_4 + i_2p_1p_3p_4 + i_3p_1p_2p_4 + i_4p_1p_2p_3 + j_1p_1 + j_2p_2 + j_3p_3 + j_4p_4 , \quad (40)$$

with

$$0 \leq i_1 < \frac{p_1-1}{2}; \; 0 \leq i_2 < \frac{p_2-1}{2}; \; 0 \leq i_3 < \frac{p_3-1}{2};$$

$$0 \leq i_4 < \frac{p_4-1}{2}; \; 0 \leq j_1 \leq p_2-1; \; 0 \leq j_3 \leq p_3-1; \; 0 \leq j_4 \leq p_1-1 .$$

To show that $|f_n| \leq \frac{1}{4} p_1^2 (p_2-1)(p_3-1)$ it suffices to prove that for fixed (i_2, i_3, j_3, j_4) the diophantine equation (40) has at most one solution (i_1, i_4, j_1, j_2), because the number of possible choices for (i_2, i_3, j_3, j_4) is $\frac{1}{4} p_1^2 (p_2-1)(p_3-1)$.

Suppose (40) has more than one solution, say

$$\begin{aligned} n &= i_1p_2p_3p_4 + i_2p_1p_3p_4 + i_3p_1p_2p_4 + i_4p_1p_2p_3 \\ &\qquad + j_1p_1 + j_2p_2 + j_3p_3 + j_4p_4 \\ &= i_1'p_2p_3p_4 + i_2p_1p_3p_4 + i_3p_1p_2p_4 + i_4'p_1p_2p_3 \\ &\qquad + j_1'p_1 + j_2'p_2 + j_3p_3 + j_4p_4 \end{aligned}$$

where $\quad (i_1, i_4, j_1, j_2) \neq (i_1', i_4', j_1', j_2') \quad .$

Then we obtain

$$(i_1-i_1') \, p_2p_3p_4 + (i_4-i_4') \, p_1p_2p_3 + (j_1-j_1') \, p_1 + (j_2-j_2') \, p_2 = 0 . \quad (41)$$

Reducing this modulo p_2p_3, we obtain

$$(j_1-j_1')\,p_1 + (j_2-j_2')\,p_2 = 0 \pmod{p_2p_3} \quad . \tag{42}$$

But (42) is equivalent to the system

$$\left.\begin{aligned} (j_1-j_1')\,p_1 &\equiv 0 \pmod{p_2} \\ (j_1-j_1')\,p_1 + (j_2-j_2')\,p_2 &\equiv 0 \pmod{p_3} \end{aligned}\right\} \tag{43}$$

Since $|j_1-j_1'| \leq p_2-1$, the first congruence relation in (43) is an equality, i.e., $(j_1-j_1')\,p_1 = 0$. Hence the second congruence in (43) becomes

$$(j_2-j_2')\,p_2 \equiv 0 \pmod{p_3} \quad .$$

Since $|j_2-j_2'| \leq p_3-1$, the above congruence is an equality. Hence we conclude that $j_2 = j_2'$, and (41) becomes

$$(i_1-i_1')\,p_2p_3p_4 + (i_4-i_4')\,p_1p_2p_3 = 0 \quad .$$

Hence $p_1 | (i_1-i_1')$. But $|i_1-i_1'| \leq \frac{p_1-1}{2}$, so we have $i_1 = i_1'$. Hence we also have $i_4 = i_4'$. Thus, for fixed (i_2, i_3, j_3, j_4), (40) has at most one solution. Therefore we obtain the inequality

$$|f_n| \leq \frac{1}{4}\,p_1^2\,(p_2-1)(p_3-1) \quad .$$

Since $|c_n| \leq 4 \max |f_n|$, this gives us the upper bound

$$|c_n| \leq p_1^2\,(p_2-1)(p_3-1) \quad .$$

CHAPTER V

THE CYCLOTOMIC POLYNOMIAL $F_m(x)$ WHERE m IS A PRODUCT OF AN ARBITRARY NUMBER OF DISTINCT ODD PRIMES

If m is a product of more than four distinct odd primes, the formula for $F_m(x)$ in Lemma 2 and the method depending on this lemma are no longer applicable. This chapter contains results of a different type for $F_m(x)$, where m is a product of an arbitrary number of odd primes.

5.1 A Partition Function and Its Generating Function

Let S_m denote the reduced residue system modulo m. Let $s_1 \le s_2 \le s_3 \le \dots \le s_{\phi(m)}$ be its elements, chosen to lie in the interval $1 \le s_i \le m$.

We define $p(k,m,n)$ to be the number of ways that an integer k can be partitioned into sum of n distinct members of S_m.

A generating function for $p(k,m,n)$ is given in the following theorem.

<u>Theorem 8:</u>
$$\sum_{S_m} \prod_{\substack{\ell=1 \\ k_\ell \epsilon S_m \\ k_i \neq k_j \text{ for } i \neq j}}^{n} x^{k_\ell} = \sum p(k,m,n)x^k . \tag{44}$$

<u>Proof:</u> Consider the coefficient of x^k. From the left-hand side of (44) we see that the coefficient of x^k is equal to the number of

ways that k can be partitioned into sum of n distinct members of S_m, which is exactly $p(k, m, n)$. Hence (44) is an identity.

5.2 Connection Between p(k, m, n) and the Cyclotomic Coefficients

Theorem 9: Consider the cyclotomic polynomial

$$F_m(x) = \sum_{n=0}^{\phi(m)} (-1)^n c_n x^{\phi(m)-n} ,$$

where m is a product of t distinct odd primes. For any $n \leq \phi(m)$ let

$$K_n = s_{\phi(m)} + s_{\phi(m)-1} + \ldots + s_{\phi(m)-(n-1)}$$

where $s_{\phi(m)}, s_{\phi(m)-1}, \ldots, s_{\phi(m)-(n-1)}$ are the largest n elements of the reduced residue system modulo m. Then we have

$$c_n = \sum_{d|m} \left[\left(\sum_{\substack{\ell \equiv d \pmod m \\ \ell \leq K_n}} p(d, m, n) \right) \mu\left(\frac{m}{d}\right) \right] .$$

Proof: We shall use the following well-known formula:

$$\sum_{\substack{k \bmod m \\ (m,k)=1}} \exp\left(\frac{2\pi i k}{m}\right) = \mu(m) .$$

From the definition of the cyclotomic polynomial we have

$$F_m(x) = \prod_{\substack{(\ell, m)=1 \\ \ell \bmod m}} \left(x - \exp\left(\frac{2\pi i \ell}{m}\right)\right) .$$

From the hypothesis of the theorem, this is equal to

$$\sum_{n=0}^{\phi(m)} (-1)^n c_n x^{\phi(m)-n} .$$

Hence we have

$$c_n = \sum_{\substack{\nu_1+\nu_2+\ldots+\nu_{\phi(m)}=n \\ \nu_i=0,\ \text{or}\ 1}} \exp\left(\frac{2\pi i}{m}\left(\nu_1 s_1 + \nu_2 s_2 + \ldots + \nu_{\phi(m)} s_{\phi(m)}\right)\right) \qquad (45)$$

where the s_i are the elements of S_m. Since $e^{2\pi i \ell/m}$ is periodic with period m, we can write

$$c_n = \sum_{k=0}^{m-1} a(k)\, e^{\frac{2\pi i k}{m}} \quad . \qquad (46)$$

Collecting the terms $e^{2\pi i \ell/m}$ with $\ell \equiv k \pmod m$ and $\ell \leq K_n$ we see that the coefficient of $e^{2\pi i \ell/m}$ is $p(\ell, m, n)$, so we have

$$a(k) = \sum_{\substack{\ell \equiv k \pmod m \\ \ell \leq K_n}} p(\ell, m, n) \quad . \qquad (47)$$

From (46) we see that

$$c_n = \sum_{d|m} \left(\sum_{\substack{k' \bmod m/d \\ (k', m/d)=1}} b(d, m, n, k')\, e^{\frac{2\pi i k'}{m/d}} \right) \qquad (48)$$

where $b(d, m, n, k') = a(k'd)$.

We will prove that $b(d, m, n, k')$ is independent of k'.

It can be seen that if we replace $e^{2\pi i/m}$ by $e^{2\pi i k/m}$ with $(k, m) = 1$ we get the same set of primitive mth roots of unity S_m. Since c_n is a symmetric function of the elements of S_m from (45), there is no change in c_n if we replace $e^{2\pi i/m}$ by $e^{2\pi i k/m}$ with $(k, m) = 1$. We can also prove that the set

$$\left\{ e^{\frac{2\pi i k'}{m/d}} \; ; \quad (k', \tfrac{m}{d}) = 1 \; , \quad k' \bmod \tfrac{m}{d} \right\}$$

is invariant under the replacement of $e^{2\pi i/m}$ by $e^{2\pi ik/m}$ with $(k, m) = 1$.

For $d = 1$; if we replace $e^{2\pi i/m}$ by $e^{2\pi ik/m}$, then $b(1, m, n, 1)$ plays the role of $b(1, m, n, k)$. Hence we have

$$b(1, m, n, 1) = b(1, m, n, k) \quad .$$

If we let k go from 2 to m with $(m, k) = 1$, then we obtain

$$b(1, m, n, 1) = \ldots = b(1, m, n, k) \quad ,$$

where $(k, m) = 1$, $k \bmod m$. Let us write $b(1, m, n, 1) = b(1, m, n)$. Then we have

$$\sum_{\substack{k' \bmod m \\ (k', m) = 1}} b(1, m, n, k')\, e^{\frac{2\pi i k'}{m}} = b(1, m, n) \sum_{\substack{k' \bmod m \\ (k', m) = 1}} e^{\frac{2\pi i k'}{m}} \quad .$$

For $d > 1$; if we replace $e^{2\pi i/m}$ by $e^{2\pi ik/m}$ with $(m, k) = 1$, then $b(d, m, n, 1)$ plays the role of $b(d, m, n, k)$. Hence we have

$$b(d, m, n, 1) = b(d, m, n, k) \quad .$$

If we let k go from 2 to m/d with $(k, m/d) = 1$, then we obtain

$$b(d, m, n, 1) = \ldots = b(d, m, n, k)$$

where $(k, m/d) = 1$, $k \bmod m/d$. Write $b(d, m, n, 1) = b(d, m, n)$. Then we have

$$\sum_{\substack{k' \bmod m/d \\ (k', m/d)=1}} b(d,m,n,k')\, e^{\frac{2\pi ik'}{m/d}} = b(d,m,n) \sum_{\substack{k' \bmod m/d \\ (k', m/d)=1}} e^{\frac{2\pi ik'}{m/d}} \; .$$

Hence (48) becomes

$$c_n = \sum_{d|m} \left(b(d,m,n) \left(\sum_{\substack{k' \bmod m/d \\ (k', m/d)=1}} e^{\frac{2\pi ik'}{m/d}} \right) \right) .$$

By the formula

$$\sum_{\substack{k' \bmod m/d \\ (k', m/d)=1}} e^{\frac{2\pi ik'}{m/d}} = \mu\left(\frac{m}{d}\right)$$

we obtain

$$c_n = \sum_{d|m} b(d,m,n)\, \mu\left(\frac{m}{d}\right) .$$

But $b(d,m,n) = a(d)$ by (48), so we have

$$c_n = \sum_{d|m} a(d)\, \mu\left(\frac{m}{d}\right) .$$

By (46) we have

$$c_n = \sum_{d|m} \left[\left(\sum_{\substack{\ell \equiv d \pmod m \\ \ell \leq K_n}} p(d,m,n) \right) \mu\left(\frac{m}{d}\right) \right] .$$

5.3 An Upper Bound for the Coefficients

<u>Theorem 10</u>: Consider the cyclotomic polynomial

$$F_m(x) = \sum_{n=0}^{\phi(m)} c_n x^n \quad ,$$

where m is a product of t distinct odd primes. Then we have

$$|c_n| \leq 2^{\phi(m)} \left(\cos^2 \frac{2\pi}{m}\right)\left(\cos^2 \frac{4\pi}{m}\right) \cdots \left(\cos^2\left(\frac{\phi(m)}{2} - 1\right) \frac{2\pi}{m}\right) \quad .$$

Proof: Since $F_m(x)$ is analytic, we have

$$F_m^{(n)}(0) = \frac{n!}{2\pi i} \int_{|z|=1} \frac{F_m(z)}{z^{n+1}}\, dz \quad .$$

Therefore we obtain

$$n!\, c_n = \frac{n!}{2\pi i} \int_{|z|=1} \frac{F_m(z)}{z^{n+1}}\, dz \quad .$$

Hence we have

$$\begin{aligned} |c_n| &\leq \frac{1}{2\pi} \left| \int_{|z|=1} \frac{F_m(z)}{z^{n+1}}\, dz \right| \\ &\leq \frac{1}{2\pi} \max_{|z|=1} \left| F_m(z) \right| \; 2\pi \\ &= \max_{|z|=1} \left| F_m(z) \right| \quad . \end{aligned} \tag{49}$$

To complete the proof we will show that

$$\max_{|z|=1} |F_m(z)| \leq 2^{\phi(m)} \left(\cos^2 \frac{2\pi}{m}\right)\left(\cos^2 \frac{4\pi}{m}\right) \cdots$$

$$\cdots \left(\cos^2 \left(\frac{\phi(m)}{2} - 1\right)\frac{2\pi}{m}\right) \quad . \qquad (50)$$

From the definition of $F_m(x)$ we see that

$$F_m(x) = \prod_{(k,m)=1} \left(x - e^{\frac{2\pi ki}{m}}\right) .$$

Therefore we obtain

$$|F_m(z)| = \prod_{(k,m)=1} \left|z - e^{\frac{2\pi ki}{m}}\right| .$$

Hence we have

$$\max_{|z|=1} |F_m(z)| = \max_{|z|=1} \prod_{(k,m)=1} \left|z - e^{\frac{2\pi ki}{m}}\right| . \qquad (51)$$

We therefore see that $\max_{|z|=1} |F_m(z)|$ is equal to the maximum of the product of the lengths of the segments between z on the unit circle and $e^{2\pi ki/m}$ with $(k, m) = 1$. We consider a half unit circle

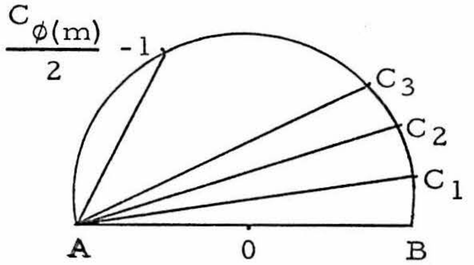

Figure 1

Write C_k as the point $e^{2\pi ik/m}$ for $k = 1, 2, \ldots, \frac{\phi(m)}{2} - 1$.

Write

$$p = 2 \prod_{k=1}^{\frac{\phi(m)}{2} - 1} |\overline{AC}_k| \tag{52}$$

where $|\overline{AC}_k|$ is the length of $\overline{AC}_k$.

Since the angle $\angle BAC_k = 2\pi k/m$, we have

$$|\overline{AC}_k| = 2 \cos \frac{2\pi k}{m} .$$

Hence

$$p = 2^{\frac{\phi(m)}{2}} \left(\cos \frac{2\pi}{m}\right)\left(\cos \frac{4\pi}{m}\right) \ldots \left(\cos \left(\frac{\phi(m)}{2} - 1\right) \frac{2\pi}{m}\right) .$$

We therefore have

$$p^2 = 2^{\phi(m)} \left(\cos^2 \frac{2\pi}{m}\right)\left(\cos^2 \frac{4\pi}{m}\right) \ldots \left(\cos^2\left(\frac{\phi(m)}{2} - 1\right) \frac{2\pi}{m}\right) .$$

The problem now reduces to showing that

$$\max_{|z|=1} \prod_{(k,m)=1} \left| z - e^{\frac{2\pi ik}{m}} \right| \leq p^2 . \tag{53}$$

Consider

$$\prod_{(k,m)=1} \left| z - e^{\frac{2\pi ik}{m}} \right| .$$

It is a continuous function of z. Let Z_0 be the point such that

$$\prod_{(k,m)=1} \left| Z_0 - e^{\frac{2\pi ik}{m}} \right| = \max_{|z|=1} \prod_{(k,m)=1} \left| z - e^{\frac{2\pi ik}{m}} \right| . \tag{54}$$

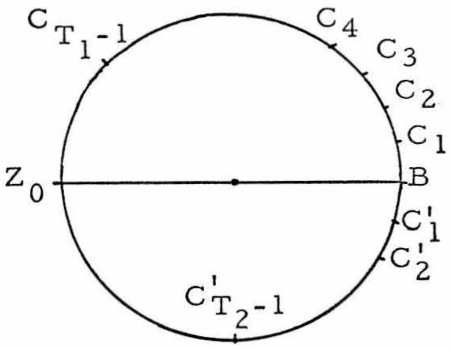

Figure 2

We draw a diameter $\overline{Z_0B}$. Let

T_1 = number of $e^{\frac{2\pi ik}{m}}$ with $(k,m)=1$ and $1 \leq k \leq m$, which are on the upper half closed circle.

T_2 = number of $e^{\frac{2\pi ik}{m}}$ with $(k,m)=1$ and $1 \leq k \leq m$, which are on the lower open half circle.

Then we have $T_1 + T_2 = \phi(m)$.

Let $B = e^{i\theta_0}$. Write

$$C_\ell = e^{\frac{2\pi i\ell}{m} + \theta_0} \quad \text{for} \quad \ell = 1,2,\ldots,\frac{m}{4} .$$

$$C_\ell' = e^{\frac{-2\pi i\ell}{m} + \theta_0} \quad \text{for} \quad \ell = 1,2,\ldots,\frac{m}{4} .$$

Then we have

$$\prod_{(k,m)=1} \left| Z_0 - e^{\frac{2\pi ik}{m}} \right| \leq 2^2 \left(\prod_{\ell=1}^{T_1-1} |\overline{Z_0C_\ell}| \right) \left(\prod_{\ell=1}^{T_2-1} |\overline{Z_0C_\ell'}| \right) . \quad (55)$$

where $|\overline{Z_0C_\ell}|$ is the length of $\overline{Z_0C_\ell}$, and $|\overline{Z_0C'_\ell}|$ is the length of $\overline{Z_0C'_\ell}$. Say $T_1 \geq T_2$, then we have $T_2 \leq \frac{T_1+T_2}{2}$. Thus we see that

$$\left|\overline{Z_0C_{\frac{T_1+T_2}{2}}}\right| \leq \left|\overline{Z_0C'_{T_2}}\right| \quad ,$$

$$\left|\overline{Z_0C_{\frac{T_1+T_2}{2}+1}}\right| \leq \left|\overline{Z_0C'_{T_2+1}}\right| \quad ,$$

$$\left|\overline{Z_0C_{T_1-1}}\right| \leq \left|\overline{Z_0C'_{\frac{T_1+T_2}{2}-1}}\right| \quad .$$

Hence we have

$$2^2\left(\prod_{\ell=1}^{T_1-1} |\overline{Z_0C_\ell}|\right)\left(\prod_{\ell=1}^{T_2-1} |\overline{Z_0C'_\ell}|\right) \leq 2^2\left(\prod_{\ell=1}^{\frac{T_1+T_2}{2}-1} |\overline{Z_0C_\ell}|\right)^2$$

$$= 2^2\left(\prod_{\ell=1}^{\frac{\phi(m)}{2}-1} |\overline{Z_0C_\ell}|\right)^2 \qquad (56)$$

But by (52) we see that

$$p^2 = 2^2\left(\prod_{\ell=1}^{\frac{\phi(m)}{2}-1} |\overline{Z_0C_\ell}|\right)^2 \quad .$$

Combining this with (54), (55), and (56) we have

$$\max_{|z|=1} \prod_{(k,m)=1} \left|z - e^{\frac{2\pi ik}{m}}\right| \leq p^2 \quad .$$

This proves (53) and also completes the proof of Theorem 10.

REFERENCES

1. T. M. Apostol, Mathematical Analysis, Addison-Wesley, Reading, Mass., 1957.

2. T. M. Apostol and Herbert S. Zuckerman, On the functional equation $F(mn)\ F((m,n)) = F(m)\ F(n)\ f((m,n))$, Pacific Journal of Mathematics, vol. 14, (1964) pp. 377-384.

3. Douglas R. Anderson and T. M. Apostol, The evaluation of Ramanujan's sum and generalizations, Duke Mathematical Journal, vol. 20, (1953) pp. 141-338.

4. A. S. Bang, Om Ligningen $\phi_n(x) = 0$, Nyt Tidsskrift for Mathematik (B), vol. 6 (1895) pp. 6-12.

5. Marion Beiter, The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$, American Mathematical Monthly, vol. 71 (1964) pp. 769-70.

6. L. Carlitz, The number of terms in the cyclotomic polynomial $F_{pq}(x)$, American Mathematical Monthly, vol. 73 (1964) pp. 979-88.

7. L. E. Dickson, History of the Theory of Numbers, Carnegie Institution of Washington, Washington, 1919.

8. Paul Erdös, On the coefficients of the cyclotomic polynomial, Bulletin American Mathematical Society, vol. 52 (1946) pp. 179-84.

9. Helen Habermehl, Sharon Richardson, and Mary Ann Szwajkos, A note on coefficients of cyclotomic polynomials, Mathematics Magazine, vol, 37 (1964) pp. 183-85.

10. D. H. Lehmer, Some properties of the cyclotomic polynomial, Journal of Mathematical Analysis and Applications, vol. 15, (1966) pp. 105-17.

11. Emma Lehmer, On the magnitude of the coefficients of the cyclotomic polynomial, Bulletin American Mathematical Society, vol. 42 (1936) pp. 389-92.

12. A. Migotti, Zur Theorie der Kreistheilungsgleichung, S.-B. der Math.-Naturwiss lasse der Kaiserlichen Akademie der Wissenschaften, Wien, (2) 87 (1883) pp. 7-14.

13. I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, John Wiley and Sons, New York, 2nd ed., 1966.

14. H. Rademacher, Lectures on Elementary Number Theory, Blaisdell, Waltham, Mass., 1964.

15. I. J. Schoenberg, A note on the cyclotomic polynomial, Mathematika, vol. 11 (1964) pp. 131-36.