Summer Research Fellowship Programme, (year)

Project Title

your name, reg. no.,
your institution

Guide: (Guide's name)
Guide's Institution

Abstract

Acknowledgements

Contents

Chapter 1

Introduction

Cyclotomic polynomials play an important role in several areas of mathematics and their study has a very long history, goes back at least to Gauss. Cyclotomic polynomials appear in the solution of the problem of which regular n-gons are constructible with straightedge and compass (Gauss–Wantzel theorem); elementary proofs of the existence of infinitely many prime numbers equal to 1, respectively -1, modulo n, special case of Dirichlet's theorem on primes in arithmetic progressions; Witt's proof of Wedderburn's little theorem that every finite domain is a field; the "cyclotomic criterion" in the study of primitive divisors of Lucas and Lehmer sequences; lattice-based cryptography etc.

In particular, the coefficients of cyclotomic polynomials have been intensively studied by several authors, in the last 10 years there has been a burst of activity in this field of research. Several authors has classified different types of cyclotomic polynomial in terms of their coefficient, degree etc. Some authors are also working on the relation between these polynomials and prime numbers. This particular area of Mathematics is not explored enough and there's lot of interesting stuff to do with these polynomials. In fact it's not an easy task to compute these polynomials for large values of n. But recently Arnold and Monagan have [1] developed a method to compute these polynomials relatively faster.

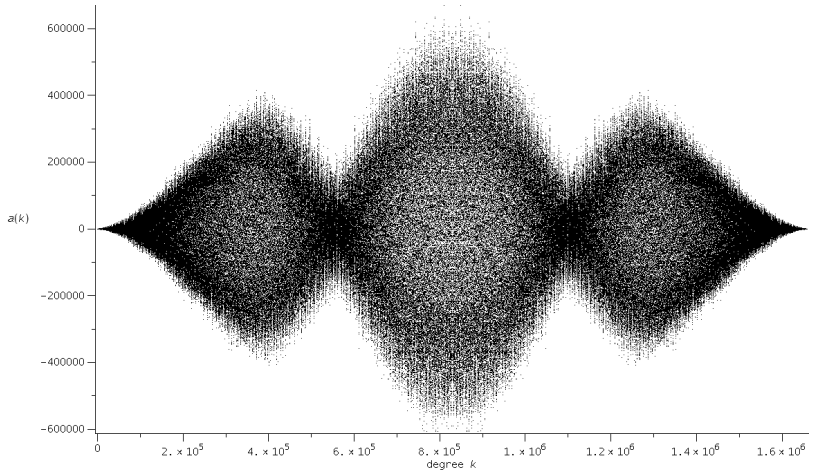

Figure 1.1: Coefficients of $\Phi_n(z) = \sum a_K z^k$ for $n = 3.5.7.11.13.17.19$ using 552960 data points

Chapter 2

Some Basic Concepts

"Cyclotomic" term is originated from the word "Cyclotomy" which means cutting a circle into equal parts. In general, $e^{i\theta}$ makes spiral curve. But, if we restrict $\theta = 2\pi$, it produces a unit circle. Using Euler's identity , we can conclude that,

$$e^{2i\pi} = 1 \implies \left(e^{i\frac{2\pi}{n}}\right)^n = 1$$

If we denote $\zeta_n := e^{i\frac{2\pi}{n}}$, then the above equation becomes ${\zeta_n}^n = 1$. ζ_n is called nth *root of unity.* Look closely that we have actually divided the circle into n equal parts just by diving the angle 2π.

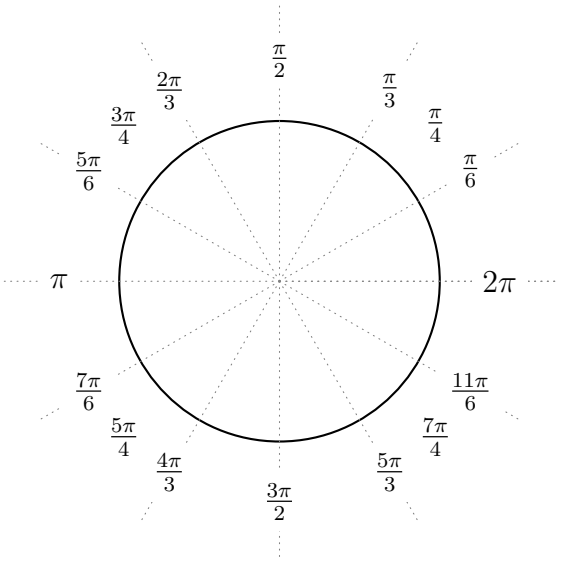

Fig : Cutting a circle into 12 equal parts.

We can write

$$\left({\zeta_n}^k\right)^n = 1, \forall k \in \mathbb{N}$$

The collection $\{{\zeta_n}^k : \left({\zeta_n}^k\right)^n = 1\}$ forms a group under complex multiplication and the elements are roots of the polynomial $z^n - 1$ for for each different n. We denote this group as μ_n, *group of* n^{th} *roots of unity*.

If d is a divisor of n and ζ is a d^{th} root of unity, then ζ is also a n^{th} of unity, since

$$\zeta^n = (\zeta^d)^{\frac{n}{d}} = 1$$

Hence, we can conclude that $\mu_d \subseteq \mu_n$ for all $d|n$.

Examples:

(1) Let's divide a circle into 2 equal parts i.e. $n = 2$. k takes values 1,2. Then

$$\zeta_2 = e^{\pi i} = -1 \quad \text{and} \quad {\zeta_2}^2 = e^{2\pi i} = 1$$

So, The associated group $\mu_2 = \{1, -1\}$.

(2) Let's divide a circle into 6 equal parts i.e. $n = 3$. k takes values 1,2,3. Then

$$\zeta_3 = e^{\frac{2}{3}\pi i} = \frac{-1+\sqrt{3}i}{2} \quad \text{and} \quad {\zeta_3}^2 = e^{\frac{4}{3}\pi i} = \frac{-1-\sqrt{3}i}{2} \quad \text{and} \quad {\zeta_3}^3 = e^{\frac{6}{3}\pi i} = 1$$

So, The associated group $\mu_3 = \{1, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\}$.

We are interested in the n^{th} roots of unity as a group is because of the following result; which allows us to derive properties of the n^{th} roots of unity by looking at more familiar group.

Lemma 1. *The mapping $\psi : \mathbb{Z}_n \to \mu_n$, given by $\psi(k) = {\zeta_n}^k$ is a group isomorphism.*

Proof. ψ is one-one and onto. Also, for $j, k \in \mathbb{Z}_n$, say that, $j + k \equiv r \pmod{n}$ i.e. $j + k = nq + r$, for some $q \in Z$.

$$\psi(j+k) = \psi(r) = {\zeta_n}^r = {\zeta_n}^{j+k-nq} = {\zeta_n}^j {\zeta_n}^k = \psi(j)\psi(k)$$

ψ is operation preserving, Hence ψ is an isomorphism. □

Definition 1. (Primitive n^{th} roots of unity). *A primitive n^{th} root of unity is an n^{th} root of unity whose order is n.*

So, in our above discussion the generators of the group μ_n are primitive n^{th} roots i.e. if ζ_n is a generator of μ_n then it follows that $< \zeta_n >= \mu_n$.

Remark 1. *If n is a positive integer, then the primitive n^{th} roots are*

$$\{{\zeta_n}^k : 1 \leq k \leq n, gcd(k, n) = 1\}$$

Definition 2. (n^{th} Cyclotomic Polynomial). *For any positive integer n the n^{th} cyclotomic polynomial, $\Phi_n(x)$, is given by*

$$\Phi_n(x) = (x - \zeta_1)(x - \zeta_2)...(x - \zeta_s)$$

where, $\zeta_1, \zeta_2, ..., \zeta_s$ are primitive n^{th} roots of unity.

Using the above remark we can also write n^{th} cyclotomic polynomials as follows,

$$\Phi_n(x) := \prod_{\substack{1 \leq k \leq n \\ gcd(n,k)=1}} (x - {\zeta_n}^k)$$

Now, We have a formal definition for the cyclotomic polynomials and some related things. Let's explore some of their simpler properties.

Theorem 1. *If n is a positive integer, then $\Phi_n(x)$ is monic and its degree is $\phi(n)$, where ϕ is the Euler phi function.*

Proof. According to Definition 2,

$$\Phi_n(x) := \prod_{\substack{1\leq k\leq n \\ gcd(n,k)=1}} (x - {\zeta_n}^k)$$

So, it is written as product of linear factors. Number of linear factors depend on the number of different primitive n^{th} roots of unity which is precisely $\phi(n)$. In each linear factor, x has highest degree 1 and coefficient 1. So, the product of $\phi(n)$ linear factors will contain x with highest degree $\phi(n)$ and coefficient 1. Hence, $\Phi_n(x)$ is monic and its degree is $\phi(n)$. □

Theorem 2. *Let n be a positive integer, then*

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

Proof. We already know that μ_n contains all n^{th} roots of unity. So, we can write

$$x^n - 1 = \prod_{\zeta\in\mu_n} (x - \zeta)$$

Each, ζ is not a primitive. Now, we group together those factors $(x - \zeta)$ where ζ is an element of order d in μ_n and $\zeta \in \mu_d$ where $d|n$. This means ζ is a primitive of μ_d. Then we obtain,

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta\in\mu_d \\ \zeta\ primitive}} (x - \zeta) = \prod_{d|n} \Phi_d(x)$$

□

Remark 2. Incidentally, comparing the degrees of both side of the above equation, we get the identity, $n = \sum_{d|n} \varphi(d)$

There is a beautiful connection between cyclotomic polynomials and Möbius inversion formula. Many famous results are proved in terms of this function. Before giving the proof of the famous identity we should first define the Möbius function and a short proof regarding the Möbius inversion formula.

Definition 3. (Möbius function) *Suppose n is a positive integer. Then the function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ given by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \text{ for all } k \\ (-1)^k & \text{if } n = p_1p_2...p_k \text{ for distinct primes } p_i \\ 0 & \text{if } otherwise. \end{cases}$$

is called the Möbius function

Theorem 3. *Suppose that $f, g : \mathbb{Z}^+ \to \mathbb{Z}^+$ functions such that*

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

Then,

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

Proof. We have,

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

Since,

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

□

Theorem 4. *If $\mu(n)$ denotes the Möbius function, then*

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

Proof. In theorem 3, put $f(n) = x^n - 1$ and $g(d) = \Phi_d(x)$. □

Theorem 5. *Let $n = \prod_{k=1}^{r} {p_k}^{a_k}$ and $m = \prod_{k=1}^{r} {p_k}^{b_k}$ be a positive integers such that $1 \leq b_k \leq a_k$, then $\Phi_n(x) = \Phi_m(x^{(n/m)})$*

Proof. **Case 1:** $d|n$ **but** $d \nmid m$

d is not square free, so $\mu(d) = 0$ means that $(x^{n/d} - 1)^0 = 1$.

Case 2: $d \mid n$ **and** $d \mid m$

Therefore,

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

□

Corollary 1. *Let p be a prime and m a positive integer. If $p \mid m$, then $\Phi_{pm}(x) = \Phi_m(x^p)$.*

Theorem 6. *Let p be a prime and m be a positive integer. If $p \nmid m$, then $\Phi_{pm}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)}$*

Proof. Given that, $p \nmid m$. If we can write,

$$\begin{aligned}
\Phi_{pm}(x) &= \prod_{d|pm} \left(x^d - 1\right)^{\mu(pm/d)} \\
&= \prod_{\substack{d|pm \\ p|d}} \left(x^d - 1\right)^{\mu(pm/d)} \prod_{\substack{d|pm \\ p\nmid d}} \left(x^d - 1\right)^{\mu(pm/d)} \\
&= \prod_{n|m} (x^{pn} - 1)^{\mu(pm/pn)} \prod_{d|m} \left(x^d - 1\right)^{\mu(pm/d)} \text{ [Since, } p \mid d \text{, hence } \exists \text{ some } n \text{ such that } d = pn] \\
&= \Phi_m(x^p) \prod_{d|m} \left(x^d - 1\right)^{-\mu(m/d)} \\
&= \frac{\Phi_m(x^p)}{\Phi_m(x)}
\end{aligned}$$

□

Theorem 7. *If n is an odd integer greater than 1, then $\Phi_{2n}(x) = \Phi_n(-x)$*

Proof. Consider,

$$\begin{aligned}
\Phi_{2n}(x) &= \prod_{d|2n} \left(x^d - 1\right)^{\mu(2n/d)} \\
&= \prod_{\substack{d|2n \\ 2|d}} \left(x^d - 1\right)^{\mu(2n/d)} \prod_{\substack{d|2n \\ 2\nmid d}} \left(x^d - 1\right)^{\mu(2n/d)} \\
&= \prod_{\substack{k|n \\ 2|d}} \left(x^{2k} - 1\right)^{\mu(2n/2k)} \prod_{d|n} \left(x^d - 1\right)^{\mu(2n/d)} \text{ [Since, } 2 \mid d \text{, hence } \exists \text{ some } k \text{ such that } d = 2k] \\
&= \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)} \left(x^d + 1\right)^{\mu(n/d)} \prod_{d|n} \left(x^d - 1\right)^{-\mu(n/d)} \text{ [As, } \mu(2m) = -\mu(m) \text{ for odd } m] \\
&= \prod_{d|n} \left(x^d + 1\right)^{\mu(n/d)} \\
&= \prod_{d|n} \left(-x^d - 1\right)^{\mu(n/d)} = \Phi_n(-x)
\end{aligned}$$

□

Theorem 8. *For all positive integers $n > 1$, we have $x^{\Phi(n)}\Phi_n(1/x) = \Phi_n(x)$*

Proof. Now consider,

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

Therefore, we get,

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

□

So, we have explored some beautiful properties of cyclotomic polynomials that are necessary for our further studies of the subject. These polynomials are so special because of it's irreducibility over $\mathbb{Q}$. We now extend our study to prove the irreducibility of these polynomials over $\mathbb{Q}$.

2.1 Irreducibility of Cyclotomic Polynomial

It is very basic result in number theory that $\Phi_n(x)$ is irreducible for every positive integer n. Our main objective here is to present a classical proof of this theorem. Before going to the main result, we first give some well known results to have it available when we present the main result. The first result that we need about polynomials is Gauss's lemma, which we state in the form in which we will use it.

Lemma 2. *If a monic polynomial in $\mathbb{Q}[x]$ divides a monic polynomial with integral coefficients, then its coefficients are all integral.*

Proof. Let, $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Q}[x]$ be a monic polynomial which divides a monic polynomial $P(x) \in \mathbb{Z}[x]$, and let $g(x) \in \mathbb{Q}[x]$ be the quotient,

$$f(x)g(x) = P(x) \in \mathbb{Z}[x]$$

In the above equation, $P(x)$ and $f(x)$ are monic, so $g(x)$ is monic too. Let

$$g(x) = x^m + b_{m-1}x^{m-1} + ... + b_0 \in \mathbb{Q}[x]$$

Claim: The coefficients $a_0, a_1, ..., a_{n-1}$ are all integers.
Assume that, the above claim is not true. Let, d be the least common multiple of the denominators of $a_0, a_1, ..., a_{n-1}$; Then,

$$f = \frac{1}{d}\left(dx^n + a'_{n-1}x^{n-1} + ... + a'_0\right)$$

Where, $a'_0, a'_1, ..., a'_{n-1}, d$ are relatively prime integers. Similary, let

$$d = \frac{1}{e}\left(ex^m + b'_{m-1}x^{m-1} + ... + b'_0\right)$$

Where, $b'_0, b'_1, ..., b'_{n-1}, e$ are relatively prime integers. Let p be a prime number which divides d. Since $a'_0, a'_1, ..., a'_{n-1}, d$ are relatively prime, there is a largest index k such that p does not divide a'_k. Let also there is a largest index l such that p does not divide b'_l (if p does not divide e, let $l = m$ and $b'_l = e$). Since $f(x)g(x) = P(x) \in \mathbb{Z}[x]$, it follows that,

$$\left(dx^n + a'_{n-1}x^{n-1} + ... + a'_0\right)\left(ex^m + b'_{m-1}x^{m-1} + ... + b'_0\right) \in de\mathbb{Z}[x].$$

In particular the coefficientof x^{k+l} in the product is divisible by p since p divides d, i.e.

$$\sum_{i+j=k+l} a'_i b'_j = ... + a'_{k-1}b'_{l+1} + a'_k b'_l + a'_{k+1}b'_{l-1} + ... \equiv 0 \mod p$$

Since, $a'_i \equiv 0 \mod p$ for $i > k$ and $b'_j \equiv 0 \mod p$ for $j > l$, we have $\sum_{i+j=k+l} a'_i b'_j \equiv 0 \mod p$. Therefore from previous equation,

$$a'_k b'_l \equiv 0 \mod p$$

It's a contradiction! since p does not divide a'_k nor b'_l. Hence, our assumption is wrong and coefficients $a_0, a_1, ..., a_{n-1}$ are all integers.

□

Lemma 3. *Let $p(x)$ and $q(x)$ be polynomials with coefficients in some field F, and assume $p(x)$ is irreducible in $F[x]$. If $p(x)$ and $q(x)$ have a common root in some field K containing F, then $p(x)$ divides $q(x)$.*

Proof. If, $p(x)$ does not divide $q(x)$, then $p(x)$ and $q(x)$ are relatively prime, because $p(x)$ is irreducible. Then there exists polynomials $u(x)$ and $v(x)$ in $F[x]$ such that

$$p(x)u(x) + q(x)v(x) = 1$$

Substituting in this equation the common root s of $p(x)$ and $q(x)$ for the indeterminate x, we obtain

$$p(s)u(s) + q(s)v(s) = 1 \quad in \ K$$

Since, $p(s) = q(s) = 0$, the above equation yields $0 = 1$ in K, a contradiction! Therefore, $p(x)$ divides $q(x)$.

□

Lemma 4. *Let $f(x)$ be a monic irreducible factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$ and let p be a prime number that does not divide n. If $\omega \in \mathbb{C}$ is a root of $f(x)$, then ω^p is also a root of $f(x)$, so*

$$f(\omega) = 0 \implies f(\omega^p) = 0$$

Proof. Assume that, $f(\omega) = 0$ but $f(\omega^p) \neq 0$ and our goal is to get a contradiction. Since, $\Phi_n(x)$ divides $(x^n - 1)$, we have

$$x^n - 1 = f(x)g(x)$$

for some monic polynomial $g(x) \in \mathbb{Q}[x]$. Since $f(\omega) = 0$, it follows that $\omega^n = 1$, hence also, raising each side to the p^{th} power, $(\omega^p)^n = 1$. In other words, ω^p is a root of $x^n - 1$. Since on the other hand it was assumed that $f(\omega^p) \neq 0$, we conclude $g(\omega^p) = 0$. This shows that ω is a root of $g(x^p)$. Therefore by lemma 2, $f(x)$ divides $g(x^p)$. Let, $h(x) \in \mathbb{Q}[x]$ be a monic polynomial such that

$$g(x^p) = f(x)h(x)$$

Using Gauss's lemma, we can conclude from the above equations that $f(x)$, $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$. Therefore, we may consider the polynomials $\bar{f}(x)$, $\bar{g}(x)$ and $\bar{h}(x)$ whose coefficients are the congruence classes modulo p of the coefficients $f(x)$, $g(x)$ and $h(x)$ respectively. By reduction modulo p, we get from the above equations,

$$x^n - 1 = \bar{f}(x)\bar{g}(x) \quad in\ \mathbb{F}_p[x]$$

and,

$$\bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \quad in\ \mathbb{F}_p[x]$$

Now, Fermat's theorem shows that $a^p = a$ for all $a \in \mathbb{F}_p$. Therefore, if

$$\bar{g}(x) = a_0 + a_1 x + ... + a_{r-1}x^{r-1} + x^r$$

we also have,

$$\bar{g}(x) = {a_0}^p + a_1 x^p + ... + {a_{r-1}}^p x^{r-1} + x^{pr}$$

Since, $(u+v)^p = u^p + v^p$ in $\mathbb{F}_p$, it follows that

$$\bar{g}(x^p) = \left(a_0 + a_1 x + ... + a_{r-1}x^{r-1} + x^r\right)^p = [\bar{g}(x)]^p \quad in\ \mathbb{F}_p$$

Hence, we get from above,

$$[\bar{g}(x)]^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \quad in\ \mathbb{F}_p[x]$$

and this shows that $\bar{f}(x)$ and $\bar{g}(x)$ are not relatively prime. Let, $\varphi(x) \in \mathbb{F}_p[x]$ be a non-constant common factor of $\bar{f}(x)$ and $\bar{g}(x)$. So, we can conclude that $\varphi(x)$ divides $x^n - 1$. Let

$$x^n - 1 = [\varphi(x)]^2\psi(x) \quad in\ \mathbb{F}_p[x]$$

Comparing the derivatives of both sides, we obtain

$$nx^{n-1} = \varphi(x)\left(2\partial\varphi(x)\psi(x) + \varphi(x)\partial\psi(x)\right)$$

Hence, $\varphi(x)$ divides both nx^{n-1} and x^n. But, according to the hypothesis $p \nmid n$, so nx^{n-1} and x^n are relatively prime in $\mathbb{F}_p[x]$ and they do not have any common factor. So we come to a contradiction. So our assumption that $f(\omega^p) \neq 0$ was absurd.

□

Now, we are ready to going through of our first classical proof inspired by some ideas of Dedekind. Though Dedekind gave a stronger result, we use his idea to prove the weaker one first. Then we will also describe the stronger result. Let's give a proposition first that is necessary for our proof.

Proposition 1. *If a polynomial is divisible by pairwise relatively prime polynomials then it is divisible by their product.*

Proof. Let, $P_1(x)P_2(x)...P_r(x)$ be pairwie relatively prime polynomials which divide a polynomial $f(x)$. We argue by induction on r, the case $r = 1$ being trivial. By induction hypothesis,

$$f(x) = P_1(x)P_2(x)...Q(x)$$

for some polynomial $Q[x]$. Since, $P_r(x)$ divides $P(x)$ so $P_r(x)$ divides $Q(x)$. Hence $P_1(x)P_2(x)...P_r(x)$ divides $P(x)$. □

Theorem 9. *For every integer $n \geq 1$, the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Let $f(x)$ be a monic irreducible factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$. Let ζ be a root of $f(x)$. Then ζ is a root of $\Phi_n(x)$. Since $\Phi_n(x)$ divides $x^n - 1$, so ζ is also a root of $x^n - 1$ i.e. ζ is a primitive n^{th} root of unity. We know that any other primitive n^{th} root of unity has the form ζ^k where k is an integer relatively prime to n between 0 and n. Factoring k into prime factors (not necessarily distinct)

$$k = p_1 ... p_s$$

we find that,

$$f(\zeta) = 0 \implies f(\zeta^{p_1}) = 0 \implies f(\zeta^{p_1 p_2}) \implies ... \implies f(\zeta^{p_1 ... p_{s-1}}) = 0 \implies f(\zeta^k) = 0$$

Thus, $f(x)$ has as root every primitive n^{th} root of unity i.e. every root of $\Phi_n(x)$. Using the above proposition we can conclude that, $\Phi_n(x)$ divides $f(x)$. Also we have assumed that $f(x)$ is a factor of $\Phi_n(x)$ and both are monic. Hence, $\Phi_n(x) = f(x)$. So, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. □

In number theory, a cyclotomic field is a number field obtained by adjoining a complex root of unity to $\mathbb{Q}$, the field of rational numbers. For $m \geq 1$, Let $\mu_m = e^{\frac{2\pi i}{m}} \in \mathbb{C}$. This is a primitive m^{th} root of unity. The m^{th} cyclotomic field is the extension $\mathbb{Q}(\mu_m)$ of $\mathbb{Q}$, generated by μ_m. We now give a powerful result of irreducibility of cyclotomic polynomials over $\mathbb{Q}(\mu_m)$ due to Dedekind which can be state as follows,

Theorem 10. *If m and n are relatively prime integers, then $\Phi_n(x)$ is irreducible over $\mathbb{Q}(\mu_m)$.*

Proof. Assume that, $\Phi_n(x)$ is reducible over $\mathbb{Q}(\mu_m)$ and $f(x)$ be a monic irreducible factor of $\Phi_n(x)$ in $\mathbb{Q}(\mu_m)[x]$. let $\zeta \in \mathbb{C}$ be a root of $f(x)$. It suffices to prove

$$f(\zeta^k) = 0$$

for every integer k relatively prime to n between 0 and n.

Let η be a primitive m^{th} root of unity. Every element in $\mathbb{Q}(\mu_m)$ can be expressed uniquely as a linear combination with rational coefficients of the m^{th} roots of unity other than 1. Hence, $\mathbb{Q}(\mu_m) = \mathbb{Q}(\eta)$ and $f(x) \in \mathbb{Q}(\eta)$. Clearly, every coefficient of $f(x)$ is a polynomial expression of η with rational coefficients. Basically, we want see $f(x)$ over $\mathbb{Q}$ and it's nature over $\mathbb{Q}$ is proved earlier which may be helpful in this strong case. Therefore,

$$f(x) = \varphi(\eta, x)$$

for some polynomial $\varphi(y, x) \in \mathbb{Q}[y, x]$

Let now $\rho = \zeta\eta$ and we see that ρ is mn^{th} root of unity as m and n are relatively prime. Also, there exists integers r and s such that

$$mr + ns = 1$$

As $\zeta^n = 1$ and $\eta^m = 1$, this equation implies that,

$$\zeta = \zeta^{mr} = \rho^{mr}$$

and

$$\eta = \eta^{ns} = \rho^{ns}$$

Since $f(\zeta) = 0$, we have $\varphi(\eta, \zeta) = 0$, or

$$\varphi(\rho^{ns}, \rho^{mr}) = 0$$

It is easy to see that, $\Phi_{mn}(x)$ and $\varphi(x^{ns}, x^{mr})$ have same roots. $\Phi_{mn}(x)$ and $\varphi(x^{ns}, x^{mr})$ both have coefficients from $\mathbb{Q}$ and using above theorem, we can conclude that $\Phi_{mn}(x)$ is irreducible over $\mathbb{Q}$. So, from Lemma 2, it can be easily verified that $\Phi_{mn}(x)$ divides $\varphi(x^{ns}, x^{mr})$. It follows that,

$$\varphi(\omega^{ns}, \omega^{mr}) = 0$$

for every primitive mn^{th} root of unity ω.

For any integer k relatively prime to n between 0 and n, let

$$l = kmr + ns$$

Since, $mr + ns = 1$, we have $mr \equiv 1 \mod n$ and $ns \equiv 1 \mod m$, hence

$$l \equiv k \mod n$$

and

$$l \equiv 1 \mod m$$

It follows that, $\zeta^l = \zeta^k$ and $\eta^l = \eta$, and since we already observed that $\zeta = \rho^{mr}$ and $\eta = \rho^{ns}$, we have

$$\zeta^k = \rho^{lmr}$$

and

$$\eta = \rho^{lns}$$

From the above congruence relations it is clear that, l is also relatively prime to mn. Therefore, ρ^l is a primitive mn^{th} root of unity and we can write,

$$\varphi(\rho^{lns}, \rho^{lmr}) = 0 \implies \varphi(\eta, \zeta^k) = f(\zeta^k) = 0$$

Hence, our assumption is wrong and $\Phi_n(x)$ is irreducible over $\mathbb{Q}(\mu_m)$.

□

[2]

Chapter 3

Coefficients of Cyclotomic Polynomial

We have already defined cyclotomic polynomials and some of it's fundamental properties. For every positive integer n, let us write,

$$\Phi_n(x) = \sum_{i=0}^{\phi(n)} a_n(i)x^i$$

It is well known that the coefficients, $a_n(i) \in \mathbf{Z}$. These coefficients are of particular interest and have been intensively studied by several authors. We denote the set of all coefficients of $\Phi_n(x)$ by $\mathcal{A}(n) := \{a_n(i) : 0 \leq i \leq \phi(n)\}$. Moreover we let $\theta(n) := \#\{0 \leq i \leq \phi(n) : a_i(n) \neq 0\}$ be the number of nonzero coefficients. It satisfies the trivial inequality $2 \leq \theta(n) \leq \phi(n) + 1$, which are optimal when one considers the cases $m = 1$ or $m = p$, a prime number. Before going to further discussion we have to define some definitions and terminologies. These are given as follows.

Definition 4. *(Height of Cyclotomic polynomials)* The height of a cyclotomic polynomial $\Phi_n(x)$, is the highest absolute value of the coefficients, denoted by $A(n)$, $n \in \mathbb{N}$. is the degree of the polynomial.

Definition 5. *(Flat cyclotomic polynomials)* A cyclotomic polynomial $\Phi_n(x)$ is said to be flat if the highest absolute value of the coefficients never exceeds 1.

Definition 6. *(Middle term of cyclotomic polynomial)* Let $\Phi_n(x)$ be a cyclotomic polynomial, the coefficient of $x^{\frac{\varphi(n)}{2}}$, denoted by $M(\Phi_n(x))$, is called the middle term coefficient of $\Phi_n(x)$

To have a brief idea of the above terms, we give an example here.

Example 1. For $n = 6$, we have the cyclotomic polynomial, $\Phi_6(x) := x^2 - x + 1$.

Here,

- $A(6) = 1$
- $M(\Phi_6(x)) = 1$

$\Phi_6(x)$ is a flat cyclotomic polynomial.

So, we have some basic definitions of different terminologies and their notations. It can be seen that the coefficients are only $\{-1, 0, +1\}$ up to $n = 104$ i.e. $A(n) = 1, \ \forall n < 105$. For $n = 105$, there is different coefficient other than the above set. So, $n = 105$ is the smallest value of n for which $A(n) > 1$. There are infinitely many cyclotomic polynomials, if we increase the value of n, we will get cyclotomic polynomials of different heights and with different properties.

3.1 Structure of cyclotomic polynomials

Generally, there is no explicit non-recursive formula for computing the coefficients of $\Phi_n(x)$. In this section we summarize some of the well known formulas/ descriptions for determining the structure of the polynomial $\Phi_n(x)$. We first give some lemmas that can be easily proved from the early theorems of this paper.

Lemma 5. *$a_n(i) \in \mathbb{Z}$ for all i, $0 \leq i \leq \phi(n)$, $n \in \mathbb{N}$.*

Lemma 6. *$a_n(i) = a_n(\phi(n) - i)$ for all i, $0 \leq i \leq \phi(n)$, $n(> 1) \in \mathbb{N}$. That is, the coefficients of cyclotomic polynomials has palindromic property.*

Definition 7. *(Order of cyclotomic polynomial)* Let $n = p_1.p_2...p_k$ be a product of k distinct prime numbers. Then $\Phi_n(x)$ is called a cyclotomic polynomial of order k.

Remark 3. $\Phi_{p_1p_2}(x)$ and $\Phi_{p_1p_2p_3}(x)$ are called **binary** $(k = 2)$ and **ternary** $(k = 3)$ cyclotomic polynomial respectively, the binary and ternary are the first non trivial cases that has been studied by several authors. In any investigation about the coefficients of cyclotomic polynomials we can reduce our enquiry to the case when n is odd, square-free and composite. Hence we can state the following observations,

(i) Form earlier proven lemmas we have

$$a_n(i) = \begin{cases} a_n(i\frac{N}{n}) & \text{if } \frac{n}{N} \mid i \\ 0 & \text{Otherwise.} \end{cases}$$

(ii) For odd $n > 1$, we have $a_{2n}(i) = (-1)^i a_n(i)$

(iii) When, $n = p$, a prime number we have $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + 1$. Hence, $a_p(i) = 1$ for all prime $i = 0, 1, 2, ..., p - 1$.

Now we give an explicit formula for binary cyclotomic polynomial due to Lam and Leung [3].

Theorem 11. *Let s, r be non negative integers such that $(p-1)(q-1) = rp + sq$. Then,*

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

Moreover for any $0 \leq k \leq (p-1)(q-1)$ we have,

(i) $a_{pq}(k) = 1$ if and only if $k = ip + jq$ for some $i \in [0, r]$, $j \in [0, s]$.

(ii) $a_{pq}(k) = -1$ if and only if $k + pq = ip + jq$ for some $i \in [r + 1, q - 1]$, $j \in [s + 1, p - 1]$.

(iii) $a_{pq}(k) = 0$ is zero otherwise.

Proof. Let, $\zeta = e^{\frac{2i\pi}{pq}}$ be a primitive pq^{th} root of unity. Hence we can say that $\zeta^p = e^{\frac{2i\pi}{q}}$ and $\zeta^q = e^{\frac{2i\pi}{p}}$ i.e. ζ^p is a q^{th} root of unity and ζ^q is a p^th root of unity.

Now, consider two polynomials $\Phi_p(x)$ and $\Phi_q(x)$ for some primes p, q. These polynomials are of degrees $(p-1)$ and $(q-1)$ respectively. So, we can write,

$$\Phi_p(\zeta^q) = 0 \implies \sum_{i=0}^{q-1} (\zeta^p)^i = 0 \implies \sum_{i=0}^{r} (\zeta^p)^i = -\sum_{i=r+1}^{q-1} (\zeta^p)^i$$

and,

$$\Phi_q(\zeta^p) = 0 \implies \sum_{j=0}^{p-1} (\zeta^q)^j = 0 \implies \sum_{j=0}^{s} (\zeta^q)^j = -\sum_{j=s+1}^{p-1} (\zeta^q)^j$$

Now, multiplying the above two equations,

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

Now, we can check that, ζ is the root of the following polynomial,

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

Clearly, the first product of the above equation has highest degree $pr + sq$ and we know that $pr + sq = (p-1)(q-1)$. The second product of the above equation has highest degree $(q-1)p + (p-1)q - pq = (p-1)(q-1)-1$ and lowest degree $(r+1)p+(s+1)q-pq = rp+sq+p+q+pq = (p-1)(q-1)+p+q-pq = pq - p - q + 1 + p + q - pq = 1$. Hence, both products of the above are monic polynomials and thus $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $(p-1)(q-1) = \phi(pq)$.

Moreover, we know that $f(\zeta) = 0$. If ζ' be another root of unity, then also we have $f(\zeta') = 0$. Since, $f(x)$ is monic polynomial of degree $\phi(pq)$ with $f(e^{2i\pi m/pq}) = 0$ for all integers m such that $g.c.d(m, pq) = 1$. So, we must have $f(x) = \Phi_{pq}(x)$.

Now note that, if $i, i' \in [0, q-1]$ and $j, j' \in [0, p-1]$ such that $ip+jq = i'p+j'q$ or $ip+jq = i'p+j'q-pq$, then

$$q \mid (i - i') \quad \text{and} \quad p \mid (j - j') \implies i = i' \quad \text{and} \quad j = j'$$

.

If we expand the products of the above polynomial equation, then the rest of the assertions follows easily. □

Remark 4. The above theorem together with the properties that we have proved earlier, proves that the coefficients of the first 104 polynomials are $\{-1, 0, +1\}$.

Higher degree cyclotomic polynomials are quite tough to follow general formulas for coefficients and there is no significant development in this topic till now. But, middle terms of cyclotomic polynomials plays a crucial role. Instead of looking over all the coefficients, we can just focus the middle term of a polynomial to get some useful informations. So, middle terms are interesting and studied by several authors. We now present a short proof of the middle terms of binary cyclotomic polynomials that follows directly from the above theorem.

Corollary 2. *Assume that $q > p$ and let $l = \frac{(p-1)(q-1)}{2}$. Then the middle coefficient $a_{pq}(l)$ of $\Phi_{pq}(x)$ is $(-1)^r$*

Proof. See p.315 of [4]

□

Theorem 12. $\mathbb{Z} = \{a_n(k) \mid k, n \in \mathbb{N}\}$

Proof. Let's prove that if t is any integer greater than 2, then there exist t distinct primes $p_1 < p_2 < ... < p_t$ such that $p_1 + p_2 > p_t$.

Assume the contrary, that is, there exists an integer $t > 2$ for which our claim is false. For this t, given any t distinct primes $p_1 < p_2 < ... < p_t$ we have $p_1 + p_2 \leq p_t$. This implies $2p_1 < p_t$. Therefore, for any given integer k, the number of primes between 2^{k-1} and 2^k is always less than t. This is because if we have t distinct primes between 2^{k-1} and 2^k, then we have $p_1 > 2^{k-1} \implies 2p_1 > 2^k > p_t$ which is not true by our assumption. Hence the number of primes less than 2^k is $\pi(2^k) < kt$ which is false by prime number theorem, since $\pi(x) > \frac{x}{\log x}$ for all $x \geq 17$. Thus the claim is true.

Now we shall prove the theorem. Let t be any odd positive integer greater than 2. From the above claim, we can find t distinct primes $p_1 < p_2 < ... < p_t$ such that $p_1 + p_2 > p_t$. Let $p = p_t$ and $n = p_1.p_2...p_t$. Now consider $\Phi_n(x)$. We have $\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}$. We go modulo x^{p+1} and since n is square-free integer, because of the conditions on these set of primes, whenever $d \neq p_i, 1$ for all $i = 1, 2, ..., t$ we have

$$\begin{aligned}
\Phi_n(x) &= \prod_{d|n} \left(x^d - 1\right)^{\mu(\frac{n}{d})} \\
&\equiv \prod_{i=1}^{t} \frac{x^{p_i} - 1}{x - 1} \pmod{x^{p+1}} \\
&\equiv \frac{1 - x^p}{1 - x}(1 - x^{p_1})...(1 - x^{p_{t-1}}) \pmod{x^{p+1}} \\
&\equiv (1 + x + ... + x^{p-1})(1 - x - ... - x^{p_t - 1}) \pmod{x^{p+1}}
\end{aligned}$$

This yields that, $a_n(p) = -t + 1$ and $a_n(p - 2) = -t + 2$. Hence, if we let

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

then S contains $\{l \in \mathbb{Z} \mid l \leq -1\}$ as t varies over all the odd integer greater than or equal to 3. By the above theorem, already we know $\{-1, 0, +1\} \subset S$. In order to prove that S contains all positive integers greater than or equal to 2, consider $\Phi_{2n}(x)$ where $n = p_1.p_2...p_t$. From the observations stated earlier, we have $a_{2n}(p) = (-1)^p a_n(p) = t - 1$ and $a_{2n}(p - 2) = (-1)^{p-2} a_n(p - 2) = t - 2$. Hence by varying t over all the odd integers ≥ 3, we see that S contains all the positive integers greater than or equal to 1.

□

If n is a product of more than two distinct primes, then the explicit values of the coefficients are not known in general. Ternary cyclotomic polynomials are the simplest one for which the behaviour of the coefficients is not fully understood but some good amount of progress has been made in the last two decades. We now give a following significant lemma due to kaplan [5] which has been used to prove several results on ternary cyclotomic polynomials.

Lemma 7. *Let $f(m)$ be the unique value $0 \leq f(m) < pq$ such that,*

$$f(m) \equiv r^{-1}(n-m) \pmod{pq}$$

We have,

$$C_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{a+p-1} a'_{f(m)}$$

Proof. We first use the result stated earlier, in Theorem 6, to factor

$$\Phi_{pqr}(x) = \frac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)} = \frac{\Phi_{pq}(x^r)\Phi_1(x)\Phi_p(x)\Phi_q(x)}{x^{pq}-1}$$

We can write $\frac{1}{x^{pq}-1}$ in terms of it's power series expansion.

$$\frac{1}{x^{pq}-1} = -(1 + x^{pq} + x^{2pq} + ...)$$

Therefore,

$$\Phi_{pqr}(x) = (1 + x^{pq} + ...)(1 + x + ... + x^{p-1} - x^q - x^{q+1} - ... - x^{q+p-1})\Phi_{pq}(x^r)$$

Let,

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

We will determine the terms of $g(x)$ that have exponent congruent to $n \pmod{pq}$. Now, let

$$\chi_m = \begin{cases} 1 & \text{if } m \in [0, p-1] \\ -1 & \text{if } m \in [q, q+p-1] \\ 0 & \text{Otherwise.} \end{cases}$$

We call that, $f(m) \equiv r^{-1}(n-m) \pmod{pq}$. Therefore, $\chi_m x^m a_{f(m)} x^{rf(m)}$ is a term of $g(x)$ with exponent congruent to $n \pmod{pq}$. We note that the degree of $\Phi_{pq} = (p-1)(q-1)$. As we range m over $[0, pq-1]$, we find all the terms of $g(x)$ with exponent congruent to $n \pmod{pq}$.

We can now write the expression for the coefficients of $\Phi_{pqr}(x)$. To compute c_n we only want to sum terms with exponents at most n. Since, $m < pq$ and $rf(m) \equiv n - m \pmod{pq}$, we have $rf(m) \leq n$ if and only if $m + rf(m) \leq n$. Therefore,

$$C_n = \sum_{m \geq 0} \chi_m a'_{f(m)} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{a+p-1} a'_{f(m)}$$

□

The above lemma is sometimes referred as **kaplan's lemma** and it is very useful in the study of ternary cyclotomic polynomials. It basically reduces the the computation of $a_{pqr}(j)$ to that of $a_{pq}(j)$ and the coefficients of binary cyclotomic polynomials is quite easy to understand. We will use this lemma to study flat ternary cyclotomic polyomials in later sections. We can extend the study of cyclotomic polyomials for higher degree too. But there are very few works has been done on cyclotomic polynomials of order greater than 3. It is hard to give a general formula. Several authors has done some specific works on higher order using so much restrictions. One can follow these [6][7] to have an idea of some recent developments of the subject. We now explore some more properties of these polynomials.

3.2 Height

In general, the highest absolute value of the coefficients of a polynomial is called the **height** of that polynomial and is denoted by $A(n)$, $n \in \mathbb{N}$ is the degree of the polynomial. Several authors have studied the height of cyclotomic poynomials. Schur was the first to prove that the coefficients of cyclotomic polynomials can be arbitrarily large i.e. $\sup_{n\geq 1} A(n) = +\infty$. There's a significant generalization by Erdös which is as follows:

$$A(n) > \exp\left(C(\log n)^{\frac{4}{3}}\right)$$

For infinitely many positive integers n and for some constant $C > 0$. His proof rests on a lower bound for the maximum of $\mid \Phi_n(x) \mid$ on the unit circle, and the simple consideration that $\mid \Phi_n(x) \mid \leq nA(n)$ for every $z \in \mathbb{C}$ with $\mid z \mid \leq 1$. This is essentially the main technique that has been used to prove the lower bounds for $A(n)$ by several authors.

There are several interesting open questions concerning cyclotomic polynomials of order three. We assume that $p < q < r$. Bang proved the bound

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

This was improved by Beither, who proved that

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

and made the following conjecture,

Conjecture 1. *(Beiter, 1968)*

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

Leher found a counter example to *Beiter's Conjecture*, that is, $A(17.29.41) = 10 > \frac{(17+1)}{2}$. Let, $M(p) := \max_{p<q<r} A(p)$ for every odd prime p. Gallot & Moore defined an effectively computable set of natural numbers for which *Beiter's Conjecture* is false. So, they formulated the following,

Conjecture 2. *(Corrected Beiter's, 2008)*

$$M(p) \leq \frac{2}{3}p \quad \text{for every prime } p$$

More recently Kosyak, Moore, Sofos & Zhang conjectured that every positive integer is of the form $A(n)$, for some ternary integer n. They proved this conjecture under a stronger form of *Andrica's Conjecture* on prime gaps, that is, assuming that,

$$p_{n+1} - p_n < \sqrt{p_n} + 1$$

holds for every $n \geq 31$, where p_n denotes the n^{th} prime number. A nice survey regarding these connections between cyclotomic polynomials & prime gaps is given by Moore.

3.3 Flatness

Instead of studying upper bounds of $A(n)$ for different n, we can give conditions on the prime factorization of n. In that case $A(n)$ is small and relatively easy to study. Recall the definition of flat cyclotomic polynomials given earlier, basically the polynomials with $A(n) = 1$ are called flat. Several families of flat cyclotomic polynomials have been constructed for binary and ternary cyclotomic polynomials but a complete classification of ternary cases is not known till now. Even there are not enough works have been done for higher order cyclotomic polynomials. These polynomials are very uncertain and there is no general formula to study their nature. All works has been done after implementing so many restrictions. Here, We now talk about flat ternary cyclotomic polynomials. Bachman [8] proved that for any prime $p \geq 5$, there are infinitely many pairs of primes (q, r) such that $A(pqr) = 1$. Bachman's theorem's requires that $q \equiv -1 \ (mod\ p)$. But Kaplan [5] proved that for any pair of primes (p, q) there exists infinitely many primes r such that $\Phi_{pqr}(x)$ is flat using his own lemma. This theorem is very useful for study the behaviour of flat ternary cyclotomicc polynomials and has been used by several authors in further development of the subject. We present this significant proof. Before that we state a proposition which can be easily derived from the Theorem 11.

Proposition 2. *The nonzero coefficients of $\Phi_{pq}(x)$ alternate between $+1$ and -1.*

Theorem 13. *Let $p < q$ be primes. Let $r \equiv 1(\mod pq)$ be prime. Then $\Phi_{pqr}(x)$ is flat.*

Proof. Assume, $r \equiv 1(\mod pq)$. So, $r^{-1} \equiv 1(\mod pq)$. We have to show that any coefficient c_n of $\Phi_{pqr}(x)$ has absolute value at most 1. Given n, let $f(i)$ be the unique value $0 \leq f(i) \leq pq$ such that $f(i) \equiv n - i(\mod pq)$. So, we conclude from *Kaplan's lemma* that ,

$$c_n = \sum_{i=0}^{p-1} a'_{f(i)} - \sum_{j=q}^{q+p-1} a'_{f(j)}$$

Let S be the first sum of the expression and T be the second sum of the expression. From *Kaplan's lemma* we write,

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

The degree of $g(x)$ is $r(p-1)(q-1) + q + p - 1 = (r-1)(p-1)(q-1) + pq$. For $n > \deg(\Phi_{pqr}(x)) = (p-1)(q-1)(r-1)$, we have $c_n = 0$. Since, $a_i \neq 0$ implies $i \leq (p-1)(q-1)$, for $n \geq r(p-1)(q-1)$, we have $a_{f(i)} = a_{f(i)}$ for all i. These facts together imply that,

$$\sum_{i=0}^{p-1} a_{f(i)} = \sum_{j=q}^{p+q-1} a_{f(j)}$$

Though we assume that $n \geq r(p-1)(q-1)$ to establish the equality. It is clear that it holds for all n.

By above proposition, for any values α and β we have,

$$\left| \sum_{i=\alpha}^{\beta} a_i \right| \leq 1$$

We note that $f(i+k) \equiv f(i)-k(\mod pq)$ and that $pq-(p-1)(q-1) = q+p-1$. Let, $j \leq i \leq j+p-1$. The values of $f(i)$ that $a_{f(i)} \neq 0$ lie in some interval $[l, l+p-1]$. This is because if $(p-1)(q-1) < f(i) < pq$, then $a_{f(i)} = 0$. This implies that both S and T have absolute value 1.

If $T = 0$, then it is clear that $\mid c_n \mid \leq 1$. So, suppose that $T = 1$, with the case $T = -1$ following similarly.

We consider two cases. First suppose that there exists k such that $q \leq k \leq q+p-1$, $a_{f(k)} \neq 0$, and $rf(k) > n$, so that $a'_{f(k)} = 0$. We show that in this case $S = 0$ and hence $c_n = 1$
Now, observe that $f(k) \leq (p-1)(q-1)$ and that it is not possible to have both $f(k) = (p-1)(q-1)$ and $k = p+q-1$. Indeed in the latter case $f(j) \geq f(k)$ for all $q \leq j \leq q+p-1$. So that $a'_{f(j)} = 0$, contradicting the assumption $T = 1$. It follows that k also satisfies $k + f(k) < pq$. Therefore, for $0 \leq i \leq p-1$, $\quad f(i) > f(k)$, so that $a'_{f(i)} = 0$ and $S = 0$. Now, assume that for all $q \leq k \leq q+p-1$, $a'_{f(k)} = a_{f(k)}$.

So,

$$T = \sum_{j=q}^{j=p+q-1} a_{f(j)} = 1$$

Since, $\sum_{i=0}^{p-1} a_{f(i)} = T = 1$ and the nonzero coefficients of each sum alternate between $1\ -1$, the nonzero term giving the minimum value of $f(j)$ and the nonzero term giving the maximum value of $f(j)$ must both be 1. Therefore, for each n, $S = 1$ or $S = 0$. Thus, $\mid c_n \mid \leq 1$.
For the case $r \equiv -1(\mod pq)$ we apply *kaplan's lemma* again. In this case $r^{-1} \equiv -1(\mod pq)$. So, we define $f(i)$ to be unique value $0 \leq f(i) < pq$ such that $f(i) \equiv -(n-i)(\mod pq)$. The rest of the argument is the same.

□

Remark 5. Note that this theorem does not include all flat cyclotomic polynomials $\Phi_{pqr}(x)$. For example, $A(3.7.11) = 1$

Appendix A

Cyclotomic Field

Cyclotomic polynomials are irreducible over $\mathbb{Q}$. We can extend $\mathbb{Q}$ to a field $\mathbb{Q}(\zeta_n)$ by adjoining n^{th} root of unity. The extended field is called *cyclotomic field*. Cyclotomic fields played a crucial role in the development of modern algebra and number theory because of their relation with Fermat's Last Theorem. The n^{th} cyclotomic field is the extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ generated by ζ_n. We can show that the extension $\mathbb{Q}(\zeta_n)$ is a Galios extension [9] over $\mathbb{Q}$ of order $\varphi(n)$ where $\varphi(n)$ denotes the Euler φ-function and the respective Galios group is isomorphic with the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ (see p.577 of [9]) and there's a standard result that a cyclotomic field is an Abelian extension of $\mathbb{Q}$ [9]. Galios groups are particularly fascinating because of it's connections with different branches of Mathematics. In fact it's an open problem to determine which groups arise as the Galios groups of Galios extensions of $\mathbb{Q}$. There's a stronger result on the connection between any finite Abelian group and cyclotomic fields which can be stated as follows,

Theorem 14. *Let G be a finite Abelian group. Then there is a subfield K of a cyclotomic field with $Gal(K/\mathbb{Q}) \cong G$*

Proof. See p.580-581 of [9] □

So, it can be shown that every cyclotomic field is an abelian extension of the rational number field $\mathbb{Q}$, having Galois group of the form $(\mathbb{Z}/n\mathbb{Z})^\times$. There is a partial converse statement of this result which can be stated as follows,

Theorem 15. *(Kronecker-Weber) Let K be a finite abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic extension of $\mathbb{Q}$.*

Proof. See [10] □

In other words, every algebraic integer whose Galois group is abelian can be expressed as a sum of roots of unity with rational coefficients. The proof requires the concept of class field theory.
There are generalizations of the above theorem known as local and global versions of *Kronecker-Weber theorem*.There's a more generalized analogue known as *Hilbert's twelfth problem* that addresses the situation of a more general algebraic number field K: what are the algebraic numbers necessary to construct all abelian extensions of K? It's an open problem till date and many developments have been done. A recent separate development was Stark's conjecture, which in contrast dealt directly with the question of finding interesting, particular units in number fields. This has seen a large conjectural development for L-functions, and is also capable of producing concrete, numerical results.

Appendix B

Some open problems

We give here some open questions on cyclotomic polynomials stated by by several authors in their papers.

- *(Conjectured by Kaplan [2010])*: If $A(n) > 1$ then for any prime p, show that $A(pn) > 1$.
- Are there any flat cyclotomic polynomials of order ≥ 5?
- *(Conjectured by pomerance and Rubinstein-Salzedo [2019])*:

  (i) Let,

  $$S = \{\alpha \in \mathbb{R} : \Phi_m(\alpha) = \Phi_n(\alpha) \text{ for some } m, n \in \mathbb{Z}^+ \text{ and } m \neq n\}$$

  Then, the largest limit point of S is 2.

  (ii) For any distinct positive integers m and n, if $z \in \mathbb{C}\backslash\mathbb{R}$ and $\Phi_m(z) = \Phi_n(z)$ then,

  $$\frac{1}{\sqrt{2}} \leq \ \mid z \mid \ \leq \sqrt{2}$$

  The upper bound is attained only for $\{m, n\} = \{1, 3\}, \{1, 4\}, \{1, 5\}$

- *(A special case of Bunyakovsky Conjecture)*: If n is a fixed positive integer, then $\Phi_n(m)$ is prime for an infinite number of integer inputs m.
- Is there any sufficiently large number $k \in \mathbb{N}$ for which any cyclotomic polynomial of degree $\geq k$ is not flat ?

Bibliography

[1] A. Arnold and M. Monagan. Cyclotomic Polynomials. 2010. URL: http://wayback.cecm.%20sfu.ca/~ada26/cyclotomic/.

[2] J. P. Tignol. Galois' Theory of Algebraic Equations. Singapore: World Scientific, 2001.

[3] T. Y. Lam & K. H. Leung. "On the Cyclotomic Polynomial $\Phi_{pq}(x)$". In: The Am. Math. Monthly 103.7 (1996), pp. 562–564. DOI: doi.org/10.1080/00029890.1996.12004786.

[4] R. Thangadurai. Cyclotomic fields and related topics. Pune, India: Bhaskaracharya Pratishthana, 2000.

[5] Nathan Kaplan. "Flat cyclotomic polynomials of order three". In: Journal of Number Theory 127 (2007), pp. 118–126. DOI: doi:10.1016/j.jnt.2007.01.008.

[6] J. Zhao & X. Zhang. "The family of ternary cyclotomic polynomials with one free prime". In: Journal of Number Theory 130.10 (2010), pp. 2223–2237. DOI: doi.org/10.1016/j.jnt.2010.03.012.

[7] R. Wilms Y. Gallot P. Moree. "Coefficients of ternary cyclotomic polynomials". In: Involve 4.4 (2011), pp. 317–341. DOI: doi.org/10.2140/INVOLVE.2011.4.317.

[8] G. Bachman. "Flat Cyclotomic Polynomials of Order Three". In: Bull. London Math. Soc. 38.1 (2006), pp. 53–60. DOI: doi.org/10.1112/S0024609305018096.

[9] D. S. Dummit & R. M. Foote. Abstract Algebra. Hoboken: John Wiley & Sons, 2004.

[10] M. J. Greenberg. "An Elementary Proof of the Kronecker-Weber Theorem". In: The Am. Math. Monthly 81.6 (1974), pp. 601–607. DOI: doi.org/10.2307/2319208.