

CYCLOTOMIC POLYNOMIALS

JORDAN BELL

CONTENTS

1. Introduction	1
2. Preliminaries	1
3. Definition and basic properties of cyclotomic polynomials	3
4. Special values	6
5. Primes in arithmetic progressions	10
6. Zsigmondy's theorem	11
7. Newton's identities and Ramanujan sums	11
8. Algebraic theorems about coefficients of cyclotomic polynomials	15
9. Analytic theorems about coefficients of cyclotomic polynomials	21
10. Fourier analysis	23
11. Algebraic topology	24
References	25

1. INTRODUCTION

2. PRELIMINARIES

By an arithmetical function we mean a function whose domain contains the positive integers. We say that an arithmetical function f is **multiplicative** when $\gcd(n, m) = 1$ implies $f(nm) = f(n)f(m)$, and that it is **completely multiplicative** when $f(nm) = f(n)f(m)$ for all $n, m \geq 1$.

Write

$$U_n = \{e^{2\pi ik/n} : 1 \leq k \leq n\} = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\},$$

the n th roots of unity. For $n > 1$, there is an element ζ of U_n with $\zeta \neq 1$. Because $\xi \mapsto \zeta\xi$ is a bijection $U_n \rightarrow U_n$ we have $\zeta \sum_{\xi \in U_n} \xi = \sum_{\xi \in U_n} \xi$, hence $(1 - \zeta) \sum_{\xi \in U_n} \xi = 0$. But $\zeta \neq 1$, which means that

$$\sum_{k=0}^{n-1} e^{2\pi ik/n} = \sum_{\xi \in U_n} \xi = 0, \quad n > 1.$$

Write

$$\Delta_n = \{e^{2\pi ik/n} : 1 \leq k \leq n, \gcd(k, n) = 1\},$$

the primitive n th roots of unity. Let ϕ be the **Euler phi function**:

$$\phi(n) = |\{k : 1 \leq k \leq n, \gcd(k, n) = 1\}| = |\Delta_n|.$$

ϕ is multiplicative, and for prime p and for $r \geq 1$, $\phi(p^r) = p^{r-1}(p-1)$.

Date: April 12, 2017.

Let μ be the **Möbius function**:

$$\mu(n) = \sum_{1 \leq k \leq n, \gcd(k, n) = 1} e^{2\pi i k/n} = \sum_{\xi \in \Delta_n} \xi.$$

For p prime, as $\Delta_p = U_p \setminus \{1\}$,

$$\mu(p) = -1 + \sum_{\xi \in U_p} \xi = 0 - 1 = -1.$$

For $r \geq 2$, as $\Delta_{p^r} = U_{p^r} \setminus U_{p^{r-1}}$,

$$\mu(p^r) = - \sum_{\xi \in U_{p^{r-1}}} \xi + \sum_{\xi \in U_{p^r}} \xi = -0 + 0 = 0.$$

Furthermore, one proves that μ is multiplicative. Thus

$$\mu(n) = \begin{cases} 1 & n \text{ is a square-free integer with an even number of prime factors} \\ -1 & n \text{ is a square-free integer with an odd number of prime factors} \\ 0 & \text{otherwise.} \end{cases}$$

The **Möbius inversion formula** states that if f and g are arithmetic functions satisfying

$$g(n) = \sum_{d|n} f(d), \quad n \geq 1,$$

then

$$f(n) = \sum_{d|n} \mu(n/d)g(d), \quad n \geq 1.$$

We can write

$$U_n = \bigcup_{d|n} \Delta_d,$$

and $\Delta_d \cap \Delta_e = \emptyset$ for $d \neq e$. So

$$n = \sum_{d|n} \phi(d).$$

Therefore by the Möbius inversion formula,

$$\phi(n) = \sum_{d|n} d \cdot \mu(n/d).$$

Also, for $n > 1$,

$$(1) \quad \sum_{d|n} \mu(d) = \sum_{d|n} \sum_{\xi \in \Delta_d} \xi = \sum_{\xi \in U_n} \xi = 0.$$

Let

$$d(n) = \sum_{d|n} 1,$$

the number of divisors of n , for example, $d(6) = 4$. Let

$$\omega(n) = \sum_{p|n} 1,$$

the number of prime divisors of n : for $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_1, \dots, \alpha_r \geq 1$, we have $\omega(n) = r$, for example $\omega(12) = \omega(2^2 \cdot 3) = 2$.

3. DEFINITION AND BASIC PROPERTIES OF CYCLOTOMIC POLYNOMIALS

For $n \geq 1$, let

$$\Phi_n(x) = \prod_{1 \leq k \leq n, \gcd(k, n) = 1} (x - e^{2\pi i k/n}) = \prod_{\xi \in \Delta_n} (x - \xi),$$

the n th cyclotomic polynomial. The first of the following two identities was found by Euler [45, pp. 199–200, Chap. III, §VI].

Lemma 1. For $n \geq 1$,

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

and for $x \notin U_n$,

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

Proof. For $F_n(x) = x^n - 1$, each of $e^{2\pi i k/n}$, $1 \leq k \leq n$, is a distinct root of $F_n(x)$, so

$$\begin{aligned} x^n - 1 &= \prod_{1 \leq k \leq n} (x - e^{2\pi i k/n}) \\ &= \prod_{d|n} \prod_{1 \leq k \leq n, \gcd(k, n) = d} (x - e^{2\pi i k/n}) \\ &= \prod_{d|n} \prod_{1 \leq j \leq n/d, \gcd(j, n/d) = 1} (x - e^{2\pi i j d/n}) \\ &= \prod_{d|n} \Phi_{n/d}(x) \\ &= \prod_{d|n} \Phi_d(x). \end{aligned}$$

That is, $\log F_n = \sum_{d|n} \log \Phi_d$. Therefore applying the Möbius inversion formula yields $\log \Phi_n = \sum_{d|n} \mu(n/d) \log F_d$ and so $\Phi_n = \prod_{d|n} F_d^{\mu(n/d)}$. \square

Lemma 2. When p is a prime,

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

When p is an odd prime,

$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1.$$

Proof. When p is a prime, $x^p - 1 = \Phi_1(x) \cdot \Phi_p(x)$, i.e.

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

When p is an odd prime,

$$\Phi_{2p}(x) = \frac{x^{2p} - 1}{\Phi_1(x)\Phi_2(x)\Phi_p(x)} = \frac{x^{2p} - 1}{(x^p - 1)\Phi_2(x)} = \frac{(x^p - 1)(x^p + 1)}{(x^p - 1)(x + 1)} = \frac{x^p + 1}{x + 1},$$

and because $(x + 1)(x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1) = x^p + 1$,

$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1. \quad \square$$

Lemma 3. *If p is a prime and $m \geq 1$,*

$$\Phi_{pm}(x) = \begin{cases} \Phi_m(x^p) & p|m \\ \Phi_m(x^p)/\Phi_m(x) & p \nmid m. \end{cases}$$

For $k \geq 1$,

$$\Phi_{p^k m}(x) = \begin{cases} \Phi_m(x^{p^k}) & p|m \\ \Phi_m(x^{p^k})/\Phi_m(x^{p^{k-1}}) & p \nmid m, \end{cases}$$

Proof. Using Lemma 1,

$$\begin{aligned} \Phi_{pm}(x) &= \prod_{d|(pm)} (x^d - 1)^{\mu(pm/d)} \\ &= \prod_{d|(pm), p|d} (x^d - 1)^{\mu(pm/d)} \cdot \prod_{d|(pm), p \nmid d} (x^d - 1)^{\mu(pm/d)} \\ &= \prod_{e|m} (x^{pe} - 1)^{\mu(m/e)} \cdot \prod_{d|(pm), p \nmid d} (x^d - 1)^{\mu(pm/d)} \\ &= \Phi_m(x^p) \cdot \prod_{d|(pm), p \nmid d} (x^d - 1)^{\mu(pm/d)}. \end{aligned}$$

If $m = ap$ and $d|(pm)$ and $p \nmid d$, then $\mu(pm/d) = \mu(ap^2/d) = 0$ and

$$\Phi_{pm}(x) = \Phi_m(x^p) \cdot \prod_{d|a} (x^d - 1)^{\mu(ap^2/d)} = \Phi_m(x^p).$$

If $p \nmid m$ and $d|(pm)$ and $p \nmid d$, then $\mu(pm/d) = \mu(p)\mu(m/d) = -\mu(m/d)$ and

$$\Phi_{pm}(x) = \Phi_m(x^p) \cdot \prod_{d|(pm), p \nmid d} (x^d - 1)^{\mu(pm/d)} = \Phi_m(x^p) \cdot \prod_{d|m} (x^d - 1)^{-\mu(m/d)}.$$

For $k \geq 2$,

$$\Phi_{p^k m}(x) = \Phi_{p \cdot p^{k-1} m}(x) = \Phi_{p^{k-1} m}(x^p) = \cdots = \Phi_{pm}(x^{p^{k-1}}),$$

and using the expression we obtained for $\Phi_{pm}(x)$ we get the expression stated for $\Phi_{p^k m}(x)$. \square

Lemma 4. *For $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where p_i are prime and $\alpha_i \geq 1$, and $N = p_1 \cdots p_r$,*

$$\Phi_n(x) = \Phi_N(x^{n/N}).$$

Proof. If $d|n$ and $d \nmid N$ then $\mu(d) = 0$, hence

$$\begin{aligned} \Phi_n(x) &= \prod_{d|n} (x^{n/d} - 1)^{\mu(d)} \\ &= \prod_{d|N} (x^{n/d} - 1)^{\mu(d)} \\ &= \prod_{d|N} ((x^{n/N})^{N/d} - 1)^{\mu(d)} \\ &= \Phi_N(x^{n/N}). \end{aligned}$$

\square

Lemma 5. *If $n > 1$ then*

$$\Phi_n(x^{-1}) = x^{-\phi(n)} \Phi_n(x).$$

Proof.

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

hence

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

Because $n > 1$ it holds that $\sum_{d|n} \mu(n/d) = 0$, and using this and $\sum_{d|n} d \cdot \mu(n/d) = \phi(n)$ yields

$$\Phi_n(x^{-1}) = x^{-\phi(n)} \Phi_n(x).$$

□

Lemma 6. *If $r > 1$ is odd then*

$$\Phi_{2r}(x) = \Phi_r(-x).$$

Proof. Because r is odd, if d_1, \dots, d_l are the divisors of r then

$$d_1, \dots, d_l, 2d_1, \dots, 2d_l$$

are the divisors of $2r$, so

$$\begin{aligned} \Phi_{2r}(x) &= \prod_{d|(2r)} (x^d - 1)^{\mu(2r/d)} \\ &= \prod_{d|r} (x^d - 1)^{\mu(2r/d)} \cdot \prod_{d|r} (x^{2d} - 1)^{\mu(2r/(2d))} \\ &= \prod_{d|r} (x^d - 1)^{\mu(2r/d)} (x^{2d} - 1)^{\mu(r/d)} \\ &= \prod_{d|r} (x^d - 1)^{\mu(2)\mu(r/d) + \mu(r/d)} (x^d + 1)^{\mu(r/d)} \\ &= \prod_{d|r} (x^d + 1)^{\mu(r/d)}. \end{aligned}$$

Because r is odd, any divisor d of r is odd and then $x^d + 1 = -((-x)^d - 1)$, so

$$\Phi_{2r}(x) = \prod_{d|r} (-1)^{\mu(r/d)} ((-x)^d - 1)^{\mu(r/d)} = (-1)^{\phi(r)} \cdot \prod_{d|r} ((-x)^d - 1)^{\mu(r/d)}.$$

Because r is odd and > 1 , $\phi(r)$ is even, so we have obtained the claim. □

Theorem 7. $\Phi_n \in \mathbb{Z}[x]$.

Proof. It is a fact that if R is a unital commutative ring, $f \in R[x]$ is a monic polynomial and $g \in R[x]$ is a polynomial, then there are $q, r \in R[x]$ with

$$g = qf + r,$$

$r = 0$ or $\deg r < \deg f$.

First, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. For $n > 1$, assume that $\Phi_d(x) \in \mathbb{Z}[x]$ for $1 \leq d < n$. Then let

$$f = \prod_{d|n, d < n} \Phi_d,$$

which by hypothesis belongs to $\mathbb{Z}[x]$. Since each Φ_d is monic, so is f . On the one hand, since $g(x) = x^n - 1 \in \mathbb{Z}[x]$, there are $q, r \in \mathbb{Z}[x]$ with $g = qf + r$ and $r = 0$ or $\deg r < \deg f$. On the other hand, by Lemma 1 we have $g = \Phi_n f \in \mathbb{C}[x]$. Thus $\Phi_n f = qf + r \in \mathbb{C}[x]$, so $r = f \cdot (\Phi_n - q) \in \mathbb{C}[x]$. If $\Phi_n \neq q$ then $\deg r = \deg f + \deg(\Phi_n - q) \geq \deg f$, contradicting that $r = 0$ or $\deg r < \deg f$. Therefore $\Phi_n = q \in \mathbb{C}[x]$, and because $q \in \mathbb{Z}[x]$ this means that $\Phi_n \in \mathbb{Z}[x]$. \square

In fact, it can be proved that Φ_n is irreducible in $\mathbb{Q}[x]$. Gauss states in entry 40 of his mathematical diary, dated October 9, 1796, that Φ_p is irreducible in $\mathbb{Q}[x]$ when p is prime, and he proves this in *Disquisitiones Arithmeticae*, Art. 341. Gauss further states in entry 136 of his mathematical diary, dated June 12, 1808, that for any n , Φ_n is irreducible in $\mathbb{Q}[x]$, and Kronecker proves this in his 1854 *Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$* . Gauss's work on cyclotomic polynomials is surveyed by Neumann [40]. For any $\xi \in \Delta_n$, $\Phi_n(\xi) = 0$, and since Φ_n is irreducible in $\mathbb{Q}[x]$ and is monic, Φ is the minimal polynomial of ξ over \mathbb{Q} , which implies that $[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg \Phi_n = \phi(n)$.

There is a group isomorphism $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n)^*$ [16, p. 596, Theorem 26]. The **discriminant** [44, p. 12, Proposition 2.7]:

$$d(\mathbb{Q}(e^{2\pi i/n})) = \frac{(-1)^{\phi(n)/2} n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

It can be proved that $\mathcal{O}_{\mathbb{Q}(e^{2\pi i/n})} = \mathbb{Z}[e^{2\pi i/n}]$ [39, p. 60, Proposition 10.2].

Let p be prime, let $q = p^r$ for $r \geq 1$, let \mathbb{F}_q be a finite field with q elements, and for $n \geq 1$ with $\gcd(n, q) = 1$, let ν be the multiplicative order of q modulo n : ν is the minimum positive integer satisfying $q^\nu \equiv 1 \pmod{n}$. It can be proved that there are monic, degree ν , irreducible polynomials $P_1, \dots, P_{\phi(n)/\nu} \in \mathbb{F}_q[x]$ such that $\Phi_n = P_1 \cdots P_{\phi(n)/\nu} \in \mathbb{F}_q[x]$ [28, p. 65, Theorem 2.47]; cf. Bourbaki [7, p. 581] on Kummer. In particular, q is a generator of the multiplicative group $(\mathbb{Z}/n)^*$ if and only if $\nu = \phi(n)$ if and only if Φ_n is irreducible in $\mathbb{F}_q[x]$. We remark that $(\mathbb{Z}/n)^*$ is cyclic if and only if n is 2, 4, some power of an odd prime, or twice some power of an odd prime (Gauss, *Disquisitiones Arithmeticae*, Art. 89–92). This follows from (i) the multiplicative group $(\mathbb{Z}/n)^*$ is isomorphic with the direct product $(\mathbb{Z}/p_1^{\alpha_1})^* \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r})^*$ for $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, (ii) $(\mathbb{Z}/2^\alpha)^*$ is isomorphic with $\mathbb{Z}/2 \times \mathbb{Z}/2^{\alpha-2}$, $\alpha \geq 2$, and (iii) $(\mathbb{Z}/p^\alpha)^*$ is a cyclic group with $p^{\alpha-1}(p-1)$ elements when p is an odd prime, $\alpha \geq 1$ [16, p. 314, Corollary 20].

4. SPECIAL VALUES

Lemma 8. $\Phi_1(0) = -1$, and for $n \geq 2$, $\Phi_n(0) = 1$.

Proof. $\Phi_1(x) = x - 1$, so $\Phi_1(0) = -1$. For $n \geq 2$, using (1),

$$\Phi_n(0) = \prod_{d|n} (-1)^{\mu(n/d)} = (-1)^{\sum_{d|n} \mu(n/d)} = (-1)^{\sum_{d|n} \mu(d)} = (-1)^0 = 1.$$

\square

Let Λ be the **von Mangoldt function**: $\Lambda(n) = \log p$ if $n = p^\alpha$ for some prime p and some integer $\alpha \geq 1$, and is $\Lambda(n) = 0$ otherwise. Thus $\Lambda(2) = \log 2$, $\Lambda(8) = \log 2$, $\Lambda(3) = \log 3$, and $\Lambda(6) = 0$. One sees that

$$\log n = \sum_{d|n} \Lambda(d).$$

Therefore by the Möbius inversion formula,

$$\Lambda(n) = \sum_{d|n} \mu(n/d) \log d.$$

Theorem 9. For $n > 1$,

$$\Phi_n(1) = e^{\Lambda(n)}$$

and

$$\Phi'_n(1) = \frac{1}{2} e^{\Lambda(n)} \phi(n).$$

Proof. For $n > 1$,

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

hence

$$\log n = \sum_{d|n, d>1} \log \Phi_d(1).$$

Therefore by the Möbius inversion formula,

$$\log \Phi_n(1) = \sum_{d|n, d>1} \mu(n/d) \log d = \sum_{d|n} \mu(n/d) \log d = \Lambda(n).$$

Because $x^n - 1 = \prod_{d|n} \Phi_d(x)$, taking the logarithm and then taking the derivative yields

$$\frac{nx^{n-1}}{x^n - 1} = \sum_{d|n} \frac{\Phi'_d(x)}{\Phi_d(x)}.$$

$\Phi_1(x) = x - 1$ and so $\frac{\Phi'_1(x)}{\Phi_1(x)} = \frac{1}{x-1}$, hence

$$\frac{nx^{n-1}}{x^n - 1} - \frac{1}{x-1} = \sum_{d|n, d>1} \frac{\Phi'_d(x)}{\Phi_d(x)},$$

i.e.

$$\frac{nx^{n-1} - (x^{n-1} + x^{n-2} + \cdots + x + 1)}{x^n - 1} = \sum_{d|n, d>1} \frac{\Phi'_d(x)}{\Phi_d(x)}.$$

Doing polynomial long division we find

$$\frac{(n-1)x^{n-1} - x^{n-2} - \cdots - x - 1}{x-1} = (n-1)x^{n-2} + (n-2)x^{n-3} + \cdots + 2x + 1.$$

Hence

$$\frac{(n-1)x^{n-2} + (n-2)x^{n-3} + \cdots + 2x + 1}{x^{n-1} + x^{n-2} + \cdots + x + 1} = \sum_{d|n, d>1} \frac{\Phi'_d(x)}{\Phi_d(x)},$$

and for $x = 1$ this is

$$\frac{n-1}{2} = \sum_{d|n, d>1} \frac{\Phi'_d(1)}{\Phi_d(1)}.$$

By the Möbius inversion formula,

$$\frac{\Phi'_n(1)}{\Phi_n(1)} = \sum_{d|n, d>1} \mu(n/d) \cdot \frac{d-1}{2},$$

and using (i) $\Phi_n(1) = e^{\Lambda(n)}$ for $n > 1$, (ii) $\sum_{d|n} \mu(n/d) = 0$ for $n > 1$, and (iii) $\sum_{d|n} d \cdot \mu(n/d) = \phi(n)$, we have

$$\Phi'_n(1) = e^{\Lambda(n)} \frac{1}{2} \sum_{d|n} \mu(n/d) \cdot d - e^{\Lambda(n)} \frac{1}{2} \sum_{d|n} \mu(n/d) = \frac{1}{2} e^{\Lambda(n)} \phi(n).$$

□

Because $\Phi_n \in \mathbb{Z}[x]$, it is the case that $\Phi_n(-i) = \overline{\Phi_n(i)}$.

Theorem 10. $\Phi_1(i) = i - 1$, $\Phi_2(i) = i + 1$, $\Phi_4(i) = 0$, and otherwise we have the following.

- If n is odd and has a prime factor $p \equiv 1 \pmod{4}$, then $\Phi_n(i) = 1$.
- If $p \equiv 3 \pmod{4}$ is prime and $k \geq 1$ is odd, then $\Phi_{p^k}(i) = i$.
- If $p \equiv 3 \pmod{4}$ is prime and $k \geq 1$ is even, then $\Phi_{p^k}(i) = -i$.
- If $p \equiv 3 \pmod{4}$ is prime and $k \geq 1$ is odd, then $\Phi_{2p^k}(i) = -i$.
- If $p \equiv 3 \pmod{4}$ is prime and $k \geq 1$ is even, then $\Phi_{2p^k}(i) = i$.
- If $p, q \equiv 3 \pmod{4}$ are distinct primes and $k, l \geq 1$, then $\Phi_{p^k q^l}(i) = -1$.
- If $p, q \equiv 3 \pmod{4}$ are distinct primes and $k, l \geq 1$, then $\Phi_{2p^k q^l}(i) = -1$.
- If p is an odd prime and $k \geq 1$, then $\Phi_{4p^k}(i) = p$.
- If $\omega(n) \geq 3$ then $\Phi_n(i) = 1$.

Proof. $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, so $\Phi_1(i) = i - 1$ and $\Phi_2(i) = i + 1$. As $i \in \Delta_4$, $\Phi_4(i) = 0$.

Suppose that n is odd, that $p \equiv 1 \pmod{4}$ is a prime factor of n , and write $n = p^k m$ with $\gcd(m, p) = 1$. Lemma 3 tells us

$$\Phi_n(x) = \Phi_{p^k m}(x) = \frac{\Phi_m(x^{p^k})}{\Phi_m(x^{p^{k-1}})},$$

and as $p^{k-1} \equiv 1 \pmod{4}$ and $i^4 = 1$, this yields

$$\Phi_n(i) = \frac{\Phi_m(i)}{\Phi_m(i)} = 1.$$

Suppose that n is odd, that $p \equiv 3 \pmod{4}$ is a prime factor of n , and write $n = p^k m$ with $\gcd(m, p) = 1$. If k is odd then $p^k \equiv 3 \pmod{4}$, so

$$\Phi_n(i) = \frac{\Phi_m(i^{p^k})}{\Phi_m(i^{p^{k-1}})} = \frac{\Phi_m(i^3)}{\Phi_m(i)} = \frac{\Phi_m(-i)}{\Phi_m(i)},$$

and if $m = 1$ then

$$\Phi_n(i) = \frac{\Phi_1(-i)}{\Phi_1(i)} = \frac{-i - 1}{i - 1} = i.$$

If k is even then $p^k \equiv 1 \pmod{4}$, so

$$\Phi_n(i) = \frac{\Phi_m(i)}{\Phi_m(-i)},$$

and if $m = 1$ then $\Phi_n(i) = -i$.

Suppose that $n = 2^k$, $k \geq 3$. Lemma 4 tells us that

$$\Phi_n(x) = \Phi_2(x^{n/2}) = \Phi_2(x^{2^{k-1}}) = x^{2^{k-1}} + 1,$$

thus

$$\Phi_n(i) = i^{2^{k-1}} + 1 = 1 + 1 = 2.$$

Suppose that $n = 2m$ with $m > 1$ odd. Lemma 6 tells us $\Phi_n(x) = \Phi_{2m}(x) = \Phi_m(-x)$, so $\Phi_n(i) = \Phi_m(-i)$.

Suppose that $n = 2^k m$ with $k \geq 2$ and $m > 1$ odd. Lemma 3 tells us

$$\Phi_{2^k m}(x) = \Phi_{2^{k-1} \cdot 2m}(x) = \Phi_{2m}(x^{2^{k-1}}),$$

and then Lemma 6 tells us $\Phi_{2m}(x^{2^{k-1}}) = \Phi_m(-x^{2^{k-1}})$. For $k = 2$ this yields

$$\Phi_{4m}(i) = \Phi_m(1),$$

and for $k > 2$,

$$\Phi_n(i) = \Phi_m(-i^{2^{k-1}}) = \Phi_m(-1).$$

□

Kurshan and Odlyzko [25]

Montgomery and Vaughan [36, pp. 131–132, Exercise 9].

Theorem 11. *If $n = \prod_{p \leq y, p \equiv 2, 3 \pmod{5}} p$ with $\omega(n)$ odd, then*

$$|\Phi_n(e^{2\pi i/5})| = \left(\frac{1 + \sqrt{5}}{2} \right)^{d(n)/2}.$$

Proof. Write $e(x) = e^{2\pi i x}$, let $d \mid n$, $d > 1$, and write $d = p_1 \cdots p_k \cdot q_1 \cdots q_l$ where $p_1, \dots, p_k \equiv 2 \pmod{5}$ and $q_1, \dots, q_l \equiv 3 \pmod{5}$ are prime. Then $\omega(d) = k + l$ and, as $2^3 \equiv 3 \pmod{5}$,

$$d \equiv 2^k 3^l \equiv 2^k 2^{3l} \equiv 2^{k+l} (-1)^l \pmod{5}.$$

If $\omega(d) \equiv 0 \pmod{4}$ then $2^{k+l} \equiv 1 \pmod{5}$ and if $\omega(d) \equiv 2 \pmod{4}$ then $2^{k+l} \equiv -1 \pmod{5}$, and therefore if $\omega(d)$ is even then $d \equiv 1 \pmod{5}$ or $d \equiv -1 \pmod{5}$. Since $|e(-1/5) - 1| = |e(1/5) - 1|$, we have $|e(d/5) - 1| = |e(1/5) - 1|$.

If $\omega(d) \equiv 1 \pmod{4}$ then $2^{k+l} \equiv 2 \pmod{5}$ and if $\omega(d) \equiv 3 \pmod{4}$ then $2^{k+l} \equiv -2 \pmod{5}$, and therefore if $\omega(d)$ is odd then $d \equiv 2 \pmod{5}$ or $d \equiv -2 \pmod{5}$. Since $|e(-2/5) - 1| = |e(2/5) - 1|$, we have $|e(d/5) - 1| = |e(2/5) - 1|$.

Now using Lemma 1 and $|e(1/5) - 1|^{-1} = |e(2/5) - 1|$,

$$\begin{aligned} |\Phi_n(e(1/5))| &= \prod_{d \mid n} |e(d/5) - 1|^{\mu(n/d)} \\ &= \prod_{d \mid n, \omega(d) \text{ even}} |e(1/5) - 1|^{-1} \cdot \prod_{d \mid n, \omega(d) \text{ odd}} |e(2/5) - 1|. \end{aligned}$$

Hence, for $\omega(n) = 2\nu + 1$ and for $A = |e(1/5) - 1|^{-1}$ and $B = |e(2/5) - 1|$,

$$\begin{aligned} \log |\Phi_n(e(1/5))| &= \sum_{r=0}^{\nu} \binom{2\nu+1}{2r} \log A + \sum_{r=0}^{\nu} \binom{2\nu+1}{2r+1} \log B \\ &= 2^{2\nu} \log A + 2^{2\nu} \log B \\ &= \log((AB)^{2^{\omega(n)}/2}), \end{aligned}$$

and using $d(n) = \sum_{r=0}^{\omega(n)} \binom{\omega(n)}{r} = 2^{\omega(n)}$ this is $|\Phi_n(e(1/5))| = (AB)^{d(n)/2}$. Finally,

$$AB = \frac{|e(2/5) - 1|}{|e(1/5) - 1|} = |e(1/5) + 1| = \frac{1 + \sqrt{5}}{2}.$$

□

5. PRIMES IN ARITHMETIC PROGRESSIONS

For prime p , $p \nmid n$, the following theorem relates the order of an element of the multiplicative group $(\mathbb{Z}/p)^*$ with Φ_n [44, p. 13, Lemma 2.9]. We remind ourselves that $\Phi_n \in \mathbb{Z}[x]$ (Theorem 7), and so $\Phi_n(a) \in \mathbb{Z}$ for $a \in \mathbb{Z}$.

Lemma 12. *Let p be prime, $p \nmid n$, and $a \in \mathbb{Z}$. Then $p \mid \Phi_n(a)$ if and only if n is the multiplicative order of a modulo p .*

Proof. Suppose that $p \mid \Phi_n(a)$. Now, let $b \in \mathbb{Z}$ with $p \mid \Phi_n(b)$. By Lemma 1, $b^n - 1 = \prod_{d|n} \Phi_d(b)$, and because $\Phi_n(b) \equiv 0 \pmod{p}$ this yields $b^n - 1 \equiv 0 \pmod{p}$, i.e. $b^n \equiv 1 \pmod{p}$; in particular, $p \nmid b$. Let $\nu = \min\{k > 0 : a^k \equiv 1 \pmod{p}\}$, the multiplicative order of a modulo p , so $\nu \mid n$, and suppose by contradiction that $\nu < n$. Using $x^\nu - 1 = \prod_{d|\nu} \Phi_d(x)$ we have $b^\nu - 1 = \prod_{d|\nu} \Phi_d(b)$. Using this with $b = a$, as $a^\nu \equiv 1 \pmod{p}$ and because p is prime it follows that for some $d_0 \leq \nu < n$, $\Phi_{d_0}(a) \equiv 0 \pmod{p}$. As $\nu \mid n$,

$$b^n - 1 = \Phi_n(b)\Phi_{d_0}(b) \cdot \prod_{d|n, d \neq d_0, n} \Phi_d(b).$$

Applying the above with $b = a$ yields $a^n - 1 \equiv 0 \pmod{p^2}$. Moreover, by the binomial theorem, $\Phi_n(a+p) \equiv \Phi_n(a) \equiv 0 \pmod{p}$ and $\Phi_{d_0}(a+p) \equiv \Phi_{d_0}(a) \equiv 0 \pmod{p}$, so applying the above with $b = a+p$ yields $(a+p)^n - 1 \equiv 0 \pmod{p^2}$. But by the binomial theorem, $(a+p)^n - 1 = \sum_{j=0}^n \binom{n}{j} a^{n-j} p^j - 1$, whence $(a+p)^n - 1 \equiv a^n + na^{n-1}p - 1 \pmod{p^2}$, hence $a^n + na^{n-1}p - 1 \equiv 0 \pmod{p^2}$. Together with $a^n - 1 \equiv 0 \pmod{p^2}$ this yields $na^{n-1}p \equiv 0 \pmod{p^2}$, i.e. $na^{n-1} \equiv 0 \pmod{p}$, contradicting that $p \nmid n, a$. Therefore $\nu = n$.

Suppose that $a^n \equiv 1 \pmod{p}$ and that $a^\nu \not\equiv 1 \pmod{p}$ for $0 < \nu < n$. As $\prod_{d|n} \Phi_d(a) = a^n - 1 \equiv 0 \pmod{p}$, there is some $d_0 \mid n$ for which $\Phi_{d_0}(a) \equiv 0 \pmod{p}$. Suppose by contradiction that $d_0 < n$. As $d_0 \mid n$,

$$a^{d_0} - 1 = \prod_{d|d_0} \Phi_d(a) = \Phi_{d_0}(a) \cdot \prod_{d|d_0, d < d_0} \Phi_d(a) \equiv 0 \pmod{p},$$

contradicting that $a^\nu \not\equiv 1 \pmod{p}$ for $0 < \nu < n$. Therefore $\Phi_n(a) \equiv 0 \pmod{p}$, i.e. $p \mid \Phi_n(a)$. □

Lemma 13. *Let p be prime, $p \nmid n$. There is some $a \in \mathbb{Z}$ such that $p \mid \Phi_n(a)$ if and only if $p \equiv 1 \pmod{n}$.*

Proof. Suppose that $a \in \mathbb{Z}$ and $p \mid \Phi_n(a)$. Then by Lemma 12, n is the multiplicative order of a modulo p . As the multiplicative group $(\mathbb{Z}/p)^*$ has $p-1$ elements, this implies that $n \mid (p-1)$, i.e. $p-1 \equiv 0 \pmod{n}$.

Suppose that $p \equiv 1 \pmod{n}$, i.e. $n \mid (p-1)$. Because $(\mathbb{Z}/p)^*$ is a cyclic group with $p-1$ elements, it is a fact that there is some $a \in \mathbb{Z}$, $a + p\mathbb{Z} \in (\mathbb{Z}/p)^*$, whose multiplicative order modulo p is n . (Generally, if G is a cyclic group with m

elements and n divides m then there is some $g \in G$ with order n .) Then by Lemma 12, $p \mid \Phi_n(a)$. \square

We now use Lemma 13 to prove an instance of Dirichlet's theorem on primes in arithmetic progressions [44, p. 13, Lemma 2.9].

Theorem 14. *For any $n \geq 1$, there are infinitely many primes p with $p \equiv 1 \pmod{n}$.*

Proof. The claim for $n = 1$ follows from the claim for $n = 2$. For $n \geq 2$, by Lemma 8, $\Phi_n(0) = 1$, namely the constant coefficient of $\Phi_n(x)$ is 1. Suppose by contradiction that there are at most finitely many such primes p_1, \dots, p_t and let $M = np_1 \cdots p_t$. For $N \in \mathbb{Z}$, $\Phi_n(NM) \equiv 1 \pmod{M}$ and from $M \mid (\Phi_n(NM) - 1)$ it follows that $p_i \mid (\Phi_n(NM) - 1)$, $1 \leq i \leq t$, and $n \mid (\Phi_n(NM) - 1)$. Hence if p is a prime factor of $\Phi_n(NM)$ then $p \neq p_i$, $1 \leq i \leq t$, and $p \nmid n$. As Φ_n is a monic polynomial that is not a constant, for all sufficiently large N , $\Phi_n(NM)$ is an integer ≥ 2 and thus has a prime factor p , and we have established that $p \nmid n$. Therefore Lemma 13 tells us that $p \equiv 1 \pmod{n}$. But we have also established that $p \neq p_i$, $1 \leq i \leq t$, a contradiction. Therefore there are infinitely many primes p with $p \equiv 1 \pmod{n}$. \square

One can prove that for any integers $n, b \geq 2$ it holds that

$$\frac{1}{2} \cdot b^{\phi(n)} \leq \Phi_n(b) \leq 2 \cdot b^{\phi(n)}.$$

Using this, Thangadurai and Vatwani [42] prove that for $n \geq 2$, the least prime $p \equiv 1 \pmod{n}$ satisfies

$$p \leq 2^{\phi(n)+1} - 1.$$

6. ZSIGMONDY'S THEOREM

Write $M_n = 2^n - 1$ [20, pp. 167–169, §8.3.1].

Theorem 15 (Zsigmondy's theorem).

Proof. \square

7. NEWTON'S IDENTITIES AND RAMANUJAN SUMS

For positive integers n and n , let

$$c_n(k) = \sum_{1 \leq j \leq n, \gcd(n,j)=1} e^{2\pi ijk/n} = \sum_{\xi \in \Delta_n} \xi^k,$$

called a **Ramanujan sum**.

Lemma 16.

$$c_n(k) = \sum_{d \mid \gcd(n,k)} d \cdot \mu(n/d).$$

Proof. Let

$$\eta_n(k) = \sum_{j=1}^n e^{2\pi ijk/n} = \begin{cases} 0 & n \nmid k \\ n & n \mid k. \end{cases}$$

We can write $\eta_n(k)$ as

$$\eta_n(k) = \sum_{d|n} c_d(k),$$

so by the Möbius inversion formula,

$$c_n(k) = \sum_{d|n} \mu(n/d) \eta_d(k).$$

□

Theorem 17. *For $n > 1$ and for $|x| < 1$,*

$$\Phi_n(x) = \exp\left(-\sum_{m=1}^{\infty} \frac{c_n(m)}{m} x^m\right).$$

Proof. Using that $\xi \mapsto \xi^{-1}$ is a bijection $\Delta_n \rightarrow \Delta_n$,

$$\begin{aligned} \frac{d}{dx} \log \Phi_n(x) &= \frac{d}{dx} \sum_{\xi \in \Delta_n} \log(x - \xi) \\ &= \sum_{\xi \in \Delta_n} \frac{1}{x - \xi} \\ &= \sum_{\xi \in \Delta_n} -\frac{1}{\xi} \cdot \frac{1}{1 - \frac{x}{\xi}} \\ &= -\sum_{\xi \in \Delta_n} \frac{1}{\xi} \sum_{m=0}^{\infty} \left(\frac{x}{\xi}\right)^m \\ &= -\sum_{m=0}^{\infty} x^m \sum_{\xi \in \Delta_n} \xi^{m+1}. \end{aligned}$$

Because $n > 1$, $\Phi_n(0) = 1$, and integrating,

$$\Phi_n(x) = \exp\left(-\sum_{m=0}^{\infty} \frac{x^{m+1}}{m+1} \sum_{\xi \in \Delta_n} \xi^{m+1}\right) = \exp\left(-\sum_{m=1}^{\infty} \frac{x^m}{m} c_n(m)\right).$$

□

A formula due to Hölder [36, p. 110, Theorem 4.1] is that

$$(2) \quad c_n(k) = \frac{\mu(n/\gcd(n, k)) \cdot \phi(n)}{\phi(n/\gcd(n, k))}.$$

This identity is used to prove the following lemma that we use later.

Lemma 18. *If n is square-free then $k \mapsto \mu(n)c_n(k)$ is multiplicative.*

Lemma 19. *For $n \geq 1$ and $\operatorname{Re} s > 1$,*

$$\sum_{k=1}^{\infty} c_n(k) k^{-s} = \zeta(s) \cdot \sum_{d|n} \mu(n/d) d^{1-s}.$$

Proof. By Lemma 16,

$$\begin{aligned}
\sum_{k=1}^{\infty} c_n(k) k^{-s} &= \sum_{k=1}^{\infty} k^{-s} \sum_{d|n, d|k} \mu(n/d) d \\
&= \sum_{d|n} \sum_{m=1}^{\infty} (md)^{-s} \mu(n/d) d \\
&= \sum_{d|n} \sum_{m=1}^{\infty} m^{-s} d^{-s} \mu(n/d) d \\
&= \sum_{m=1}^{\infty} m^{-s} \sum_{d|n} d^{-s} \mu(n/d) d \\
&= \zeta(s) \cdot \sum_{d|n} \mu(n/d) d^{1-s}.
\end{aligned}$$

□

Write

$$\prod_{j=1}^n (x - \alpha_j) = \sum_{k=0}^n (-1)^k s_k x^{n-k},$$

and put, for $k \geq 1$,

$$p_k = \sum_{j=1}^n \alpha_j^k.$$

Newton's identities [19, p. 32, Proposition 3.4] state that for $k \geq 1$,

$$(3) \quad p_k = \sum_{j=1}^{k-1} (-1)^{j-1} s_j p_{k-j} + (-1)^{k-1} k s_k.$$

Write

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

Let $n > 1$, and for integer j define

$$\chi_1(j) = \begin{cases} 1 & \gcd(n, j) = 1 \\ 0 & \gcd(n, j) > 1, \end{cases}$$

namely the **principal Dirichlet character modulo n** . We can then write

$$\Phi_n(x) = \prod_{1 \leq k \leq n, \gcd(n, k)=1} (x - e^{2\pi i k/n}) = x^{-n+\phi(n)} \prod_{j=1}^n (x - \alpha_j)$$

for $\alpha_j = \chi_1(j) e^{2\pi i j/n}$, and thus

$$x^{n-\phi(n)} \Phi_n(x) = \prod_{j=1}^n (x - \alpha_j).$$

Because $\chi_1(j)^k = \chi_1(j)$ for $k \geq 1$,

$$p_k = \sum_{j=1}^n \alpha_j^k = \sum_{j=1}^n \chi_1(j) e^{2\pi i j k / n} = \sum_{1 \leq j \leq n, \gcd(n, j) = 1} e^{2\pi i j k / n} = c_n(k).$$

Now, from

$$x^{n-\phi(n)} \sum_{k=1}^{\phi(n)} a_n(k) x^k = \sum_{k=0}^n (-1)^k s_k x^{n-k}$$

we have, for $0 \leq k \leq n$,

$$(-1)^k s_k = a_n(\phi(n) - k).$$

In fact by Lemma 21, $a_n(\phi(n) - k) = a_n(k)$, so $a_n(k) = (-1)^k s_k$. Thus (3) yields the following, and in particular

$$a_n(1) = -c_n(1) = -\mu(n).$$

Theorem 20. For $n \geq 1$ and $k \geq 1$,

$$k a_n(k) = -c_n(k) - \sum_{j=1}^{k-1} a_n(j) c_n(k-j).$$

Let n be a product of distinct odd primes and for $a \in \mathbb{Z}$ let $\chi(a) = \left(\frac{a}{n}\right)$ be the **Jacobi symbol**. Dedekind, in Supplement I to Dirichlet's *Vorlesungen über Zahlentheorie* [15, pp. 208–210], §116, proves that

$$(4) \quad \sum_{1 \leq j \leq n} \chi(j) e^{2\pi i j h / n} = \chi(h) i^{(n-1)^2/4} \sqrt{n};$$

this is proved earlier by Gauss in his *Summatio quarumdam serierum singularium* [22, pp. 9–45], dated 1808. The expression $G(h, \chi) = \sum_{1 \leq j \leq n} \chi(j) e^{2\pi i j h / n}$ is called a **Gauss sum**. Dedekind, in Supplement VII to Dirichlet's *Vorlesungen*, says what amounts to the following. Define

$$A_n(x) = \prod_{1 \leq a \leq n, \chi(a) = 1} (x - e^{2\pi i a / n}) = \sum_j \alpha_n(j) x^j$$

and

$$B_n(x) = \prod_{1 \leq b \leq n, \chi(b) = -1} (x - e^{2\pi i b / n}) = \sum_j \beta_n(j) x^j,$$

and write

$$S_n(k) = \sum_{1 \leq a \leq n, \chi(a) = 1} e^{2\pi i k a / n}, \quad T_n(k) = \sum_{1 \leq b \leq n, \chi(b) = -1} e^{2\pi i k b / n}.$$

Then

$$\Phi_n(x) = A_n(x) B_n(x), \quad c_n(k) = S_n(k) + T_n(k),$$

and by (4), writing

$$n^* = (-1)^{(n-1)/2} n,$$

we have

$$S_n(k) - T_n(k) = \sum_{1 \leq j \leq n} \chi(j) e^{2\pi i k j / n} = \chi(k) \sqrt{n^*},$$

hence

$$2S_n(k) = c_n(k) + \chi(k) \sqrt{n^*}, \quad 2T_n(k) = c_n(k) - \chi(k) \sqrt{n^*}.$$

We have established in Lemma 16 that $c_n(k) \in \mathbb{Z}$, so this shows that $S_n(k), T_n(k) \in \mathbb{Q}(\sqrt{n^*})$. Newton's identities yield for $k \geq 1$,

$$S_n(k) = - \sum_{j=1}^{k-1} \alpha_n(n-j) S_n(k-j) - k \alpha_n(n-k)$$

and

$$T_n(k) = - \sum_{j=1}^{k-1} \beta_n(n-j) T_n(k-j) - k \beta_n(n-k),$$

and it follows that $\alpha_n(k), \beta_n(k) \in \mathbb{Q}(\sqrt{n^*})$. Furthermore, $\alpha_n(k), \beta_n(k)$ are algebraic integers, so $\alpha_n(k), \beta_n(k) \in \mathcal{O}_{\mathbb{Q}(\sqrt{n^*})}$. If D is a square-free, it is a fact [16, p. 698, §15.3] that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega]$ for

$$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod{4}, \end{cases}$$

and $n^* = (-1)^{(n-1)/2} n \equiv 1 \pmod{4}$, we have $\mathcal{O}_{\mathbb{Q}(\sqrt{n^*})} = \mathbb{Z}[(1 + \sqrt{n^*})/2]$. Thus $\alpha_n(k), \beta_n(k) \in \mathbb{Z}[(1 + \sqrt{n^*})/2]$.

It is a fact that $\mathbb{Q}(\sqrt{n^*}) \subset \mathbb{Q}(e^{2\pi i/n})$ [23, p. 19, Proposition 5.13] Gauss, *Disquisitiones Arithmeticae*, Art. 357

8. ALGEBRAIC THEOREMS ABOUT COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

For $n \geq 1$, we write

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

Let

$$A(n) = \max_{0 \leq k \leq \phi(n)} |a_n(k)|$$

and

$$S(n) = \sum_{k=0}^{\phi(n)} |a_n(k)|.$$

It is immediate that $A(n) \leq S(n)$.

Lemma 21. For $n > 1$ and for $0 \leq k \leq \phi(n)$,

$$a_n(\phi(n) - k) = a_n(k).$$

Proof. For $P(x) = \sum_{j=0}^n a(j)x^j$, check that $a(j) = a(n-j)$ for each $0 \leq j \leq n$ is equivalent to $x^n P(x^{-1}) = P(x)$. But because $n > 1$, by Lemma 5 we have $\Phi_n(x^{-1}) = x^{-\phi(n)} \Phi_n(x)$, so we obtain the claim. \square

Migotti [35] proves the following, and also calculates $a_{105}(7) = -2$. The following is also proved by Bang [2]; cf. Beiter [4].

Theorem 22 (Bang). For odd primes $p < q$,

$$a_{pq}(k) \in \{0, -1, 1\}.$$

Proof. By Lemma 1,

$$\begin{aligned}
\Phi_{pq}(x) &= \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)} \\
&= \frac{(1 - x) \sum_{\alpha=0}^{p-1} x^{\alpha q}}{1 - x^p} \\
&= (1 - x) \sum_{0 \leq \alpha \leq p-1} x^{\alpha q} \cdot \sum_{\beta \geq 0} x^{\beta p} \\
&= \sum_{0 \leq \alpha \leq p-1, \beta \geq 0} x^{\alpha q + \beta p} - \sum_{0 \leq \alpha \leq p-1, \beta \geq 0} x^{\alpha q + \beta p + 1} \\
&= \sum_{0 \leq \alpha \leq p-1, \beta \geq 0, 0 \leq \delta \leq 1} (-1)^\delta x^{\alpha q + \beta p + \delta}.
\end{aligned}$$

Suppose by contradiction that $\alpha_1 q + \beta_1 p + \delta_1 = \alpha_2 q + \beta_2 p + \delta_2$ with $\delta_1 = \delta_2$. Then $q(\alpha_1 - \alpha_2) = p(\beta_2 - \beta_1)$, which implies that p divides $\alpha_1 - \alpha_2$. But $0 \leq \alpha_1, \alpha_2 \leq p-1$ means $0 \leq |\alpha_1 - \alpha_2| \leq p-1$, so $\alpha_1 - \alpha_2 = 0$ and thence $\beta_2 - \beta_1 = 0$, which means that $(\alpha_1, \beta_1, \delta_1) = (\alpha_2, \beta_2, \delta_2)$. Therefore, for $0 \leq k \leq \phi(pq)$ there are zero, one, or two triples (α, β, δ) such that $k = \alpha q + \beta p + \delta$; if there are two such triples, then one has $\delta = 0$ and one has $\delta = 1$. If there are no such triples, then $a_n(k) = 0$. If there is one such triple (α, β, δ) , then $a_n(k) = (-1)^\delta$. If there are two such triples, then $a_n(k) = (-1)^0 + (-1)^1 = 0$. \square

Lam and Leung [26] determine the following explicit formula.

Theorem 23 (Lam and Leung). *Suppose that $p < q$ are primes. Then there are nonnegative integers r, s such $(p-1)(q-1) = rp + sq$, and for $0 \leq k \leq \phi(pq) = (p-1)(q-1)$,*

$$a_{pq}(k) = \begin{cases} 1 & 0 \leq i \leq r, 0 \leq j \leq s \text{ with } k = ip + jq \\ -1 & r+1 \leq i \leq q-1, s+1 \leq j \leq p-1 \text{ with } k + pq = ip + jq \\ 0 & \text{otherwise} \end{cases}$$

Furthermore,

$$|\{k : 0 \leq k \leq \phi(pq), a_{pq}(k) = 1\}| = (r+1)(s+1)$$

and

$$|\{k : 0 \leq k \leq \phi(pq), a_{pq}(k) = -1\}| = (p-s-1)(q-r-1).$$

Proof. Because $\gcd(p, q) = 1$, there is some $0 \leq r \leq q-1$ such that

$$rp \equiv -p + 1 \pmod{q}.$$

If $r = q-1$ then we get from the above that $1 \equiv 0 \pmod{q}$, which is false because $q \neq 1$, so in fact $0 \leq r \leq q-2$. Now,

$$s = \frac{(p-1)(q-1) - rp}{q} = \frac{pq - p - q + 1 - rp}{q}$$

is an integer and

$$s = \frac{p(q-r-1) - q + 1}{q} \geq \frac{-q + 1}{q} > -1,$$

hence $s \geq 0$. Also, $s \leq \frac{(p-1)(q-1)}{q} < p-1$, so $s \leq p-2$. We then have

$$rp + sq = rp + (p-1)(q-1) - rp = (p-1)(q-1).$$

For $\xi \in \Delta_{pq}$, because $\Phi_q(\xi^p) = 0$ and $\Phi_p(\xi^q) = 0$,

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

(Because $0 \leq r \leq q-2$ and $0 \leq s \leq p-2$, each of the above four sums has a nonempty index set.) From this we have

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

Because $\xi^{-pq} = 1$, this implies that each $\xi \in \Delta_{pq}$ is a zero of the polynomial

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

that this is indeed a polynomial follows from

$$(r+1)p + (s+1)q - pq = rp + sq + p + q - pq = 1.$$

The first product is a monic polynomial of degree $rp + sq = \phi(pq)$. The second product is a polynomial of degree

$$(q-1)p + (p-1)q - pq = -p - q + pq = \phi(pq) - 1.$$

Therefore $f(x)$ is a monic polynomial of degree $\phi(pq)$. Because each $\xi \in \Delta_{pq}$ is a zero of $f(x)$ and $f(x)$ is monic, $f(x) = \Phi_{pq}(x)$. \square

Carlitz [10] proves the following.

Theorem 24. *Let $p < q$ be primes, let*

$$qu \equiv -1 \pmod{p}, \quad 0 < u < p,$$

let $\theta(pq)$ be the number of terms of Φ_{pq} with nonzero coefficients, and let $\theta_0(pq)$ be the number of terms of Φ_{pq} with positive coefficients. Then

$$\theta(pq) = 2\theta_0(pq) - 1$$

and

$$\theta_0(pq) = (p-u)(uq+1)/p.$$

Cobeli, Gallot, Moree and Zaharescu [13] give an exposition of $a_{pqr}(k)$ where $p < q < r$ are primes, p is fixed, and q, r are free.

Bang [2] proves the following.

Theorem 25 (Bang). *For odd primes $p < q < r$,*

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

Beiter [5] proves the following improvement for a case of the above theorem. If $p, q, r, 3 < p < q < r$, are odd primes for which either $q \equiv \pm 1 \pmod{p}$ or $r \equiv \pm 1 \pmod{p}$, then

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

Bloom [6] proves the following.

Theorem 26 (Bloom). *For odd primes $p < q < r < s$,*

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

Gallot and Moree [21]

The following is from Lehmer [27], who says that it appears in an unpublished letter of Schur to Landau; cf. Bourbaki [8, V. 165, §11, Exercise 19].

Theorem 27 (Schur). *For any odd $m \geq 3$ there are primes $p_1 < p_2 < \dots < p_m$, with $p_1 + p_2 > p_m$. For such primes,*

$$a_{p_1 p_2 \dots p_m}(p_m) = -m + 1.$$

Proof. Write

$$\pi(x) = |\{p : p \text{ is prime and } p \leq x\}|.$$

For $m \geq 3$, suppose by contradiction that if $p_1 < p_2 < \dots < p_m$ are primes then $p_1 + p_2 \leq p_m$, and thus $2p_1 < p_m$. For $k \geq 1$, as there are infinitely many primes, let p_1 be the least prime $> k$, and let $k \leq p_1 < p_2 < \dots < p_m$. Then

$$\pi(2k) - \pi(k) = \pi(2k) - \pi(p_1) + 1 \leq \pi(2p_1) - \pi(p_1) + 1 \leq (m-1) + 1 = m.$$

This yields, for $j \geq 1$,

$$\pi(2^j) \leq m + \pi(2^{j-1}) \leq m + m + \pi(2^{j-2}) \leq \dots \leq jm.$$

But the prime number theorem tells us

$$\pi(2^j) \sim \frac{2^j}{j \log 2}, \quad j \rightarrow \infty,$$

with which we get a contradiction.

Let $m \geq 3$ be odd and let $p_1 < p_2 < \dots < p_m$ be primes satisfying $p_1 + p_2 > p_m$, and let $n = p_1 p_2 \dots p_m$. Since $p_1 + p_2 > p_m$, for $1 \leq j, k \leq m$ we have $p_j + p_k \geq p_m + 1$. It follows that if d is a divisor of n aside from 1 and p_1, \dots, p_m , and $\mu(n/d) \neq 0$, then

$$(x^d - 1)^{\mu(n/d)} \in x^{p_m+1} \mathbb{Z}[x].$$

Therefore

$$\begin{aligned} \Phi_n(x) + x^{p_m+1} \mathbb{Z}[x] &= \prod_{d|n} (x^d - 1)^{\mu(n/d)} + x^{p_m+1} \mathbb{Z}[x] \\ &= \prod_{d|n, \mu(d/n) \neq 0} (x^d - 1)^{\mu(n/d)} + x^{p_m+1} \mathbb{Z}[x] \\ &= (x-1)^{-1} \cdot \prod_{j=1}^m (x^{p_j} - 1)^{\mu(n/p_j)} + x^{p_m+1} \mathbb{Z}[x] \\ &= (x-1)^{-1} \cdot \prod_{j=1}^m (x^{p_j} - 1) + x^{p_m+1} \mathbb{Z}[x] \\ &= (x-1)^{-1} \cdot (-1 + x^{p_1} + \dots + x^{p_m}) + x^{p_m+1} \mathbb{Z}[x]. \end{aligned}$$

Now,

$$\begin{aligned} &(x-1)^{-1} \cdot (-1 + x^{p_1} + \dots + x^{p_m}) + x^{p_m+1} \mathbb{Z}[x] \\ &= (1 + x + x^2 + \dots + x^{p_m}) \cdot (1 - x^{p_1} - \dots - x^{p_m}) + x^{p_m+1} \mathbb{Z}[x]. \end{aligned}$$

For $1 \leq i \leq m$, there is one and only one $0 \leq j \leq p_m$ such that $p_i + j = p_m$. This implies that the coefficient of x^{p_m} in the above expression is $-m + 1$. \square

Lehmer also states that in Rolf Bungers' 1934 dissertation, *Über die Koeffizienten von Kreisteilungspolynomen* (University of Göttingen), it is proved that if there exist infinitely many twin primes then for any M there are primes $p < q < r$ such that $A(pqr) \geq M$. Lehmer proves this without the hypothesis that there are infinitely many twin primes.

For power series $A(x) = \sum_{k=0}^{\infty} a_k x^k$ and $B(x) = \sum_{k=0}^{\infty} b_k x^k$, write

$$A \preceq B$$

if $|a_k| \leq b_k$ for all k . For power series A, B, P, Q with $A \preceq P$ and $B \preceq Q$,

$$|a_k + b_k| \leq |a_k| + |b_k| \leq p_k + q_k,$$

so $A + B \preceq P + Q$, and

$$\left| \sum_{i+j=k} a_i b_j \right| \leq \sum_{i+j=k} |a_i b_j| \leq \sum_{i+j=k} p_i q_j,$$

so $AB \preceq PQ$.

Now,

$$x^d - 1 \preceq \sum_{k=0}^{\infty} x^{kd}, \quad 1 \preceq \sum_{k=0}^{\infty} x^{kd}, \quad (x^d - 1)^{-1} \preceq \sum_{k=0}^{\infty} x^{kd},$$

and since $\mu(n/d) \in \{0, 1, -1\}$,

$$(5) \quad \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \preceq \prod_{d|n} \left(\sum_{k=0}^{\infty} x^{kd} \right) = \prod_{d|n} \frac{1}{1 - x^d}.$$

Hence, because $1 \preceq \frac{1}{1-x^j}$,

$$\Phi_n(x) \preceq \prod_{j=1}^{\infty} \frac{1}{1 - x^j}.$$

Let $n \mapsto p(n)$ be the partition function, the number of ways of writing n as a sum of positive integers, where the order does not matter. $p(0) = 1$ and $p(n) = 0$ for $n < 0$, and for example, $p(4) = 5$ because $4 = 4, 3 + 1, 2 + 2, 2 + 1 + 1, 1 + 1 + 1 + 1$. It is a fact that for $|x| < 1$,

$$\prod_{j=1}^{\infty} \frac{1}{1 - x^j} = \sum_{k=0}^{\infty} p(k) x^k,$$

found by Euler.

Theorem 28.

$$|a_n(k)| \leq p(k),$$

and so

$$A(n) = \max_{0 \leq k \leq \phi(n)} |a_n(k)| \leq \max_{0 \leq k \leq \phi(n)} p(k) \leq p(\phi(n)) \leq p(n).$$

It is proved by Hardy and Ramanujan [12, p. 166, Chapter VII] that for $K = \pi\sqrt{\frac{2}{3}}$ and $\lambda_n = \sqrt{n - \frac{1}{24}}$,

$$p(n) = \frac{e^{K\lambda_n}}{4\sqrt{3} \cdot \lambda_n^2} + O\left(\frac{e^{K\lambda_n}}{\lambda_n^3}\right), \quad n \rightarrow \infty.$$

This implies

$$p(n) \sim \frac{e^{K\sqrt{n}}}{4\sqrt{3} \cdot n}, \quad n \rightarrow \infty.$$

Therefore,

$$A(n) = O\left(\frac{e^{K\sqrt{n}}}{n}\right), \quad S(n) = O(e^{K\sqrt{n}}), \quad n \rightarrow \infty$$

Now let

$$Q_n(x) = \prod_{d|n} (1 + x^d + x^{2d} + \cdots + x^{n-d}).$$

It is straightforward that for $0 \leq k < n$, the coefficient of x^k in $Q_n(x)$ is equal to the coefficient of x^k in $\prod_{d|n} \frac{1}{1-x^d}$. For $n > 1$, because the degree of $\Phi_n(x)$ is $\phi(n) < n$, using (5) we get

$$\Phi_n(x) \leq Q_n(x).$$

Let

$$d(n) = \sum_{d|n} 1,$$

the number of positive integer divisors of n . It is straightforward that

$$\prod_{d|n} d = n^{d(n)/2},$$

so

$$Q_n(1) = \prod_{d|n} \frac{n}{d} = \prod_{d|n} d = n^{d(n)/2}.$$

But from $\Phi_n(x) \leq Q_n(x)$ we have that $S(n)$ is \leq the sum of the coefficients of the polynomial $Q_n(x)$, i.e.

$$S(n) \leq Q_n(1) = n^{d(n)/2}.$$

This is found by Bateman [3]; cf. [36, p. 64, Exercise 7].

Theorem 29 (Bateman).

$$S(n) \leq \exp\left(\frac{1}{2}d(n)\log n\right).$$

A result due to Wigert [12, p. 19, Theorem 6], proved using the prime number theorem, is that

$$\limsup_{n \rightarrow \infty} \log d(n) \cdot \frac{\log \log n}{\log n} = \log 2.$$

Thus, for each $\epsilon > 0$, there is some n_ϵ such that when $n \geq n_\epsilon$,

$$\log d(n) \cdot \frac{\log \log n}{\log n} \leq \log 2 + \epsilon,$$

so

$$\log d(n) \leq \frac{\log n}{\log \log n} (\epsilon + \log 2).$$

Then

$$\log S(n) \leq \frac{d(n)}{2} \cdot \log n \leq \frac{\log n}{2} \exp\left(\frac{\log n}{\log \log n} (\epsilon + \log 2)\right).$$

Wirsing [46]

Konyagin, Maier and Wirsing [24]

Maier [29], [30], [31], [32]

Bachman [1]

Bzdęga [9]

Nicolas and Terjanian [41]

Let $\Psi_n(x) = \frac{x^n - 1}{\Phi_n(x)}$, i.e. $\Psi_n(x) = \prod_{d|n, d < n} \Phi_d(x)$, which belongs to $\mathbb{Z}[x]$ and is monic. Moree [37] proves the following.

9. ANALYTIC THEOREMS ABOUT COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

Erdős [17]

Erdős and Vaughan [18] prove the following.

Vaughan [43] proves the next theorem. Vaughan's original proof is complicated and delightful, and we first outline it and then give a radically simplified proof using Theorem 11, attributed to Saffari by Montgomery and Vaughan [36, pp. 131–132, Exercise 9].

For $n = \prod_{p \leq y, p \equiv 2, 3 \pmod{5}} p$ with $\omega(n)$ odd, let $c_m = -\frac{c_n(m)}{m}$. Because n is square-free and $\mu(n) = -1$, it follows from Lemma 18 that $m \mapsto c_m$ is multiplicative. Because $c_m = O(m^{-1})$, the following Euler product expansions hold [36, p. 20, Theorem 1.9]:

$$\sum_{m=1}^{\infty} c_m m^{-s} = \prod_p \sum_{k=0}^{\infty} c_{p^k} p^{-ks}, \quad \operatorname{Re} s > 0$$

and

$$\sum_{m=1}^{\infty} \chi(m) c_m m^{-s} = \prod_p \sum_{k=0}^{\infty} \chi(p^k) c_{p^k} p^{-ks}, \quad \operatorname{Re} s > 0,$$

where χ is the quadratic Dirichlet character modulo 5. Using Hölder's formula (2) one works out that for $p \mid n$,

$$\sum_{k=0}^{\infty} c_{p^k} p^{-ks} = \frac{1 - p^{-s}}{1 - p^{-(s+1)}}$$

and for $p \nmid n$,

$$\sum_{k=0}^{\infty} c_{p^k} p^{-ks} = \frac{1}{1 - p^{-(s+1)}},$$

thus

$$\sum_{m=1}^{\infty} c_m m^{-s} = \zeta(1+s) \prod_{p \mid n} (1 - p^{-s}), \quad \operatorname{Re} s > 0.$$

Using Hölder's formula and that χ is completely multiplicative, one works out that for $p \mid n$,

$$\sum_{k=0}^{\infty} \chi(p^k) c_{p^k} p^{-ks} = \frac{1 + p^{-s}}{1 - \chi(p) p^{-(s+1)}}$$

and for $p \nmid n$,

$$\sum_{k=0}^{\infty} \chi(p^k) c_{p^k} p^{-ks} = \frac{1}{1 - \chi(p) p^{-(s+1)}},$$

thus

$$\sum_{m=1}^{\infty} \chi(m) c_m m^{-s} = L(1+s, \chi) \prod_{p \mid n} (1 + p^{-s}), \quad \operatorname{Re} s > 0.$$

Using (i) the fact that the Gauss sum $\sum_{r=1}^4 \chi(r)e^{2\pi ira/5}$ is equal to $\chi(a)\sqrt{5}$, (ii) the fact that $c_{5m} = \frac{c_m}{5}$, and (iii) $e^{2\pi im/5} + e^{2\pi i \cdot 4m/5} = 2 \cdot \operatorname{Re} e^{2\pi im/5}$, one works out that for $x > 0$,

$$4 \cdot \operatorname{Re} \sum_{m=1}^{\infty} c_m e^{2\pi im/5} e^{-m/x} = \sum_{m=1}^{\infty} c_m \left(\sqrt{5} \cdot \chi(m) e^{-m/x} + e^{-5m/x} - e^{-m/x} \right).$$

Using this and the above Euler product expansions we get for $s > 0$,

$$\begin{aligned} & \int_0^{\infty} \left(\operatorname{Re} \sum_{m=1}^{\infty} c_m e^{(m/5)} e^{-m/x} \right) x^{-s-1} dx \\ &= \frac{\Gamma(s)}{4} \left(\sqrt{5} \cdot L(1+s, \chi) \prod_{p|n} (1+p^{-s}) - (1-5^{-s}) \zeta(1+s) \prod_{p|n} (1-p^{-s}) \right). \end{aligned}$$

For $x > 0$, writing $f(x) = \operatorname{Re} \sum_{m=1}^{\infty} c_m e^{2\pi im/5} e^{-m/x}$, one has for $0 < \sigma < 1$,

$$\int_0^{\infty} f(x) x^{-\sigma-1} dx \leq \frac{1}{1-\sigma} + \frac{1}{\sigma} \sup_{x \geq 1} f(x),$$

so

$$\begin{aligned} & \sup_{x \geq 1} f(x) \\ & \geq \sigma \int_0^{\infty} f(x) x^{-\sigma-1} dx - \frac{\sigma}{1-\sigma} \\ &= \frac{\sigma \Gamma(\sigma)}{4} \left(\sqrt{5} \cdot L(1+\sigma, \chi) \prod_{p|n} (1+p^{-\sigma}) - (1-5^{-\sigma}) \zeta(1+\sigma) \prod_{p|n} (1-p^{-\sigma}) \right) \\ & \quad - \frac{\sigma}{1-\sigma}. \end{aligned}$$

As $\sigma \rightarrow 0$ we have $\sigma \Gamma(\sigma) = 1 + O(\sigma)$, $(1-5^{-\sigma}) \zeta(1+\sigma) = \log 5 + O(\sigma)$, and $1-p^{-\sigma} = \sigma \log p + O(\sigma^2)$, thus

$$\sup_{x \geq 1} f(x) \geq \frac{1}{4} \cdot \sqrt{5} \cdot L(1, \chi) \cdot 2^{\omega(n)} = \frac{1}{4} \cdot \sqrt{5} \cdot L(1, \chi) \cdot d(n).$$

But Theorem 17 tells us that for $|z| < 1$,

$$|\Phi_n(z)| = \exp \left(\operatorname{Re} \sum_{m=1}^{\infty} c_m z^m \right),$$

so $|\Phi_n(e^{2\pi i/5} e^{-1/x})| = e^{f(x)}$ and thus

$$\sup_{|z| < 1} |\Phi_n(z)| \geq \exp \left(\frac{1}{4} \cdot \sqrt{5} \cdot L(1, \chi) \cdot d(n) \right).$$

As χ is the quadratic Dirichlet character modulo 5, it is a fact that $L(1, \chi)$ can be explicitly evaluated (this is an instance of Dirichlet's class number formula), and using this one checks that $\exp \left(\frac{1}{2} \cdot \sqrt{5} \cdot L(1, \chi) \right) = \frac{1+\sqrt{5}}{2}$. Therefore

$$\sup_{|z| < 1} |\Phi_n(z)| \geq \left(\frac{1+\sqrt{5}}{2} \right)^{d(n)/2}.$$

Theorem 30 (Vaughan). *If $n = \prod_{p \leq y, p \equiv 2,3 \pmod{5}} p$ with $\omega(n)$ odd, then*

$$|\Phi_n(e^{2\pi i/5})| = \left(\frac{1 + \sqrt{5}}{2} \right)^{d(n)/2}.$$

There are infinitely many n such that

$$\log A(n) > \exp\left(\frac{(\log 2)(\log n)}{\log \log n}\right).$$

Proof.

□

Vaughan further proves the following.

Theorem 31 (Vaughan). *There is some C such that for infinitely many k ,*

$$\log \max_{n \geq 1} |a_n(k)| \geq Ck^{1/2}(\log k)^{-1/4}.$$

10. FOURIER ANALYSIS

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. For $p \geq 1$, define

$$\|f\|_{L^p} = \left(\int_0^1 |f(x)|^p dx \right)^{1/p}$$

and $\|f\|_{L^\infty} = \sup_{x \in [0,1]} |f(x)|$. By Jensen's inequality, if $1 \leq p \leq q \leq \infty$ then

$$\|f\|_{L^p} \leq \|f\|_{L^q}.$$

For $f \in L^1(\mathbb{T})$, define $\widehat{f}: \mathbb{Z} \rightarrow \mathbb{C}$ by

$$\widehat{f}(k) = \int_0^1 e^{-2\pi i k x} f(x) dx.$$

Define

$$\|\widehat{f}\|_{\ell^p} = \left(\sum_{k \in \mathbb{Z}} |\widehat{f}(k)|^p \right)^{1/p}$$

and $\|\widehat{f}\|_{\ell^\infty} = \sup_{k \in \mathbb{Z}} |\widehat{f}(k)|$. For $1 \leq p \leq q \leq \infty$,

$$\|\widehat{f}\|_{\ell^q} \leq \|\widehat{f}\|_{\ell^p}.$$

Plancherel's theorem tells us that

$$\|f\|_{L^2} = \|\widehat{f}\|_{\ell^2}.$$

The Hausdorff-Young inequality states that for $1 \leq p \leq 2$ and $\frac{1}{p} + \frac{1}{q} = 1$,

$$\|\widehat{f}\|_{\ell^q} \leq \|f\|_{L^p}.$$

Nikolsky's inequality [14, p. 102, Theorem 2.6] says that if $\widehat{f}(k) = 0$ for $|k| > n$, namely f is a trigonometric polynomial of degree n , then for $0 < p \leq q \leq \infty$ and for $r \geq \frac{p}{2}$ an integer,

$$\|f\|_{L^q} \leq (2nr + 1)^{\frac{1}{p} - \frac{1}{q}} \|f\|_{L^p}.$$

On the other hand, using Jensen's inequality for sums one proves that if f is a trigonometric polynomial of degree n , then for $1 \leq p \leq q \leq \infty$,

$$\| \hat{f} \|_{\ell^p} \leq (2n+1)^{\frac{1}{p}-\frac{1}{q}} \| \hat{f} \|_{\ell^q}.$$

For $f : \mathbb{T} \rightarrow \mathbb{C}$, define

$$\| \hat{f} \|_{\ell^0} = |\text{supp } \hat{f}| = |\{n \in \mathbb{Z} : \hat{f}(n) \neq 0\}|.$$

McGehee, Pigno and Smith [33] prove that there is some K such that for all N , if n_1, \dots, n_N are distinct integers and $c_1, \dots, c_N \in \mathbb{C}$ satisfy $|c_k| \geq 1$, then

$$\left\| \sum_{k=1}^N c_k e^{2\pi i n_k t} \right\|_{L^1} \geq K \log N.$$

That is, if $f : \mathbb{T} \rightarrow \mathbb{C}$ is a trigonometric polynomial with $|\hat{f}(n)| \geq 1$ when $\hat{f}(n) \neq 0$, then

$$\| f \|_{L^1} \geq K \log \| \hat{f} \|_{\ell^0}.$$

For $F : \mathbb{Z}/N \rightarrow \mathbb{C}$, define $\hat{F} : \mathbb{Z}/N \rightarrow \mathbb{C}$ by

$$\hat{F}(k) = \frac{1}{N} \sum_{j=0}^{N-1} F(j) e^{-2\pi i j k / N}, \quad 0 \leq k \leq N-1.$$

One checks that [36, pp. 109–110, §4.1]

$$F(j) = \sum_{k=0}^{N-1} \hat{F}(k) e^{2\pi i j k / N}, \quad 0 \leq j \leq N-1$$

and

$$\sum_{k=0}^{N-1} |\hat{F}(k)|^2 = \frac{1}{N} \sum_{j=0}^{N-1} |F(j)|^2.$$

For $a_0, \dots, a_{N-1} \in \mathbb{C}$, define $f : \mathbb{T} \rightarrow \mathbb{C}$ by

$$f(x) = \sum_{k=0}^{N-1} a_k e^{2\pi i k x}$$

and define $F : \mathbb{Z}/N \rightarrow \mathbb{C}$ by

$$F(j) = f(j/N) = \sum_{k=0}^{N-1} a_k e^{2\pi i k j / N}, \quad 0 \leq j \leq N-1,$$

for which we calculate $\hat{F}(k) = a_k$, for $0 \leq k \leq N-1$. Then

$$\sum_{k=0}^{N-1} |a_k|^2 = \sum_{k=0}^{N-1} |\hat{F}(k)|^2 = \frac{1}{N} \sum_{j=0}^{N-1} |F(j)|^2 = \frac{1}{N} \sum_{j=0}^{N-1} |f(j/N)|^2.$$

Carlitz [11]

11. ALGEBRAIC TOPOLOGY

Musiker and Reiner [38]

Meshulam [34]

REFERENCES

1. Gennady Bachman, *On the coefficients of cyclotomic polynomials*, Memoirs of the American Mathematical Society **106** (1993), no. 510, 1–80.
2. Alfred Sophus Bang, *Om Ligningen $\Phi_m(X) = 0$* , Nyt Tidsskrift for Mathematik, Afdeling B **6** (1895), 6–12.
3. P. T. Bateman, *Note on the coefficient of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **55** (1949), no. 12, 1180–1181.
4. Marion Beiter, *The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$* , Amer. Math. Monthly **71** (1964), no. 7, 769–770.
5. ———, *Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$* , Amer. Math. Monthly **75** (1968), no. 4, 370–372.
6. D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly **75** (1968), 372–377.
7. Nicolas Bourbaki, *Elements of mathematics. Commutative algebra*, Addison-Wesley, 1972.
8. ———, *Elements of mathematics. Algebra II, chapters 4–7*, Springer, 1990, Translated by P. M. Cohn and J. Howie.
9. Bartłomiej Bzdega, *On the height of cyclotomic polynomials*, Acta Arith. **152** (2012), no. 4, 349–359.
10. L. Carlitz, *The number of terms in the cyclotomic polynomial $F_{pq}(x)$* , Amer. Math. Monthly **73** (1966), no. 9, 979–981.
11. ———, *The sum of the squares of the coefficients of the cyclotomic polynomial*, Acta Math. Acad. Sci. Hungar. **18** (1967), 295–302.
12. K. Chandrasekharan, *Arithmetical functions*, Die Grundlehren der mathematischen Wissenschaften, vol. 167, Springer, 1970.
13. Cristian Cobeli, Yves Gallot, Pieter Moree, and Alexandru Zaharescu, *Sister Beiter and Kloosterman: A tale of cyclotomic coefficients and modular inverses*, Indagationes Mathematicae **24** (2013), 915–929.
14. Ronald A. DeVore and George G. Lorentz, *Constructive approximation*, Die Grundlehren der mathematischen Wissenschaften, vol. 303, Springer, 1993.
15. P. G. L. Dirichlet, *Lectures on number theory*, History of Mathematics, vol. 16, American Mathematical Society, Providence, RI, 1999, Supplements by R. Dedekind, translated from the German by John Stillwell.
16. David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, 2004.
17. P. Erdős, *On the growth of the cyclotomic polynomial in the interval $(0, 1)$* , Proceedings of the Glasgow Mathematical Association **3** (1957), no. 2, 102–104.
18. P. Erdős and R. C. Vaughan, *Bounds for the r -th coefficients of cyclotomic polynomials*, J. London Math. Soc. (2) **8** (1974), no. 3, 393–400.
19. Jean-Pierre Escofier, *Galois theory*, Graduate Texts in Mathematics, vol. 204, Springer, 2001, Translated by Leila Schneps.
20. Graham Everest and Thomas Ward, *An introduction to number theory*, Graduate Texts in Mathematics, vol. 232, Springer, 2005.
21. Yves Gallot and Pieter Moree, *Ternary cyclotomic polynomials having a large coefficient*, J. reine angew. Math. **632** (2009), 105–125.
22. Carl Friedrich Gauss, *Carl Friedrich Gauss. Werke. Zweiter Band*, Königlichen Gesellschaft der Wissenschaften zu Göttingen, 1876.
23. Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito, *Number theory 2: Introduction to class field theory*, Translations of Mathematical Monographs, vol. 240, American Mathematical Society, Providence, RI, 2011, Translated by Masato Kuwata and Katsumi Nomizu.
24. Sergei Konyagin, Helmut Maier, and Eduard Wirsing, *Cyclotomic polynomials with many primes dividing their orders*, Period. Math. Hungar. **49** (2004), no. 2, 99–106.
25. R. P. Kurshan and A. M. Odlyzko, *Values of cyclotomic polynomials at roots of unity*, Math. Scand. **49** (1981), 15–35.
26. T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial $\Phi_{pq}(X)$* , Amer. Math. Monthly **103** (1996), no. 7, 562–564.
27. Emma Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **42** (1936), no. 6, 389–392.

28. Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1997.
29. Helmut Maier, *The coefficients of cyclotomic polynomials*, Analytic Number Theory. Proceedings of a Conference in Honor of Paul T. Bateman (Bruce C. Berndt, Harold G. Diamond, Heini Halberstam, and Adolf Hildebrand, eds.), Progress in Mathematics, vol. 85, Birkhäuser, 1990, pp. 349–366.
30. ———, *The size of the coefficients of cyclotomic polynomials*, Analytic Number Theory. Proceedings of a Conference in Honor of Heini Halberstam, Volume 2 (Bruce C. Berndt, Harold G. Diamond, and Adolf J. Hildebrand, eds.), Progress in Mathematics, vol. 139, Birkhäuser, 1996, pp. 633–639.
31. ———, *The distribution of the L^2 -norm of cyclotomic polynomials on the unit circle*, Elementare und analytische Zahlentheorie (Wolfgang Schwarz and Jörn Steuding, eds.), Schriften der Wissenschaftlichen Gesellschaft an der Johann Wolfgang Goethe-Universität Frankfurt am Main, vol. 20, Franz Steiner Verlag, Stuttgart, 2006, pp. 164–179.
32. ———, *Anatomy of integers and cyclotomic polynomials*, Anatomy of Integers (Jean-Marie De Koninck, Andrew Granville, and Florian Luca, eds.), CRM Proceedings & Lecture Notes, vol. 46, American Mathematical Society, Providence, RI, 2008, pp. 89–95.
33. O. Carruth McGehee, Louis Pigno, and Brent Smith, *Hardy's inequality and the L^1 norm of exponential sums*, Ann. of Math. (2) **113** (1981), no. 3, 613–618.
34. Roy Meshulam, *Homology of balanced complexes via the Fourier transform*, J. Algebraic Combin. **35** (2012), 565–571.
35. Adolf Migotti, *Zur Theorie der Kreistheilungsgleichung*, Sitzungsberichte der Mathematisch-Naturwissenschaftlichen Classe der Kaiserlichen Akademie der Wissenschaften **87** (1883), 7–14, Heft I, Abt. II.
36. Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory I: Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, 2006.
37. Pieter Moree, *Inverse cyclotomic polynomials*, J. Number Theory **129** (2009), 667–680.
38. Gregg Musiker and Victor Reiner, *The cyclotomic polynomial topologically*, J. reine angew. Math. **687** (2014), 113–132.
39. Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer, 1999, Translated from the German by Norbert Schappacher.
40. Olaf Neumann, *The Disquisitiones Arithmeticae and the theory of equations*, The Shaping of Arithmetica after C. F. Gauss's Disquisitiones Arithmeticae (Catherine Goldstein, Norbert Schappacher, and Joachim Schwermer, eds.), Springer, 2007, pp. 107–127.
41. Jean-Louis Nicolas and Guy Terjanian, *Une majoration de la longueur des polynômes cyclotomiques*, Enseign. Math. (2) **45** (1999), no. 3-4, 301–309.
42. R. Thangadurai and A. Vatwani, *The least prime congruent to one modulo n* , Amer. Math. Monthly **118** (2011), no. 8, 737–742.
43. R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. **21** (1974), 289–295 (1975).
44. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer, 1997.
45. André Weil, *Number theory: An approach through history from Hammurapi to Legendre*, Birkhäuser, 1984.
46. Eduard Wirsing, *The third logarithmic momentum of the cyclotomic polynomial on the unit circle and factorizations with a linear side condition*, Elementare und analytische Zahlentheorie (Wolfgang Schwarz and Jörn Steuding, eds.), Schriften der Wissenschaftlichen Gesellschaft an der Johann Wolfgang Goethe-Universität Frankfurt am Main, vol. 20, Franz Steiner Verlag, Stuttgart, 2006, pp. 297–312.

E-mail address: jordan.bell@gmail.com

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO