On the Coefficients of Cyclotomic Polynomials

R. Thangadurai

1. Properties of Cyclotomic Polynomials

Cyclotomy is the process of dividing a circle into equal parts, which is precisely the effect obtained by plotting the n-th roots of unity in the complex plane.

For integers $n \geq 1$, we know that $X^n - 1 = \prod_{m=0}^{n-1}(X - e^{\frac{2\pi i m}{n}})$ over $\mathbb{C}$. The n-th *cyclotomic polynomial* can be defined as

$$\Phi_n(X) = \prod_{m=1,(m,n)=1}^{n} (X - e^{\frac{2\pi i m}{n}})$$

where $e^{\frac{2\pi i}{n}}$ is a primitive n-root of unity. Clearly, the degree of $\Phi_n(X)$ is $\phi(n)$ where ϕ is the Euler totient function. We have $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Lemma 1.1 *The cyclotomic polynomial $\Phi_n(X)$ is a monic polynomial over integers.*

Proof. We use induction to prove this result. We have $\Phi_1(X) = X - 1$. We assume that the result is true for all $d < n$ and we prove the result for n. By the induction hypothesis, we have $F(X) \stackrel{\text{def}}{=} \prod_{d<n,d|n} \Phi_d(X) \in \mathbb{Z}[X]$ and its leading coefficient is 1. As $F(X)$ is monic, by division algorithm, $\exists\ h(X), r(X) \in \mathbb{Z}[X]$ such that $h(X)$ is monic and $X^n - 1 = F(X)h(X) + r(X)$, where $r(X) = 0$ or $\deg r(X) < \deg F(X)$.

But, $X^n - 1 = F(X)\Phi_n(X)$. Therefore, by uniqueness of quotient and remainder in $\mathbb{C}[X]$, we must have $h(X) = \Phi_n(X)$. Also it is clear that $\Phi_n(X)$ has leading coefficient 1. □

The *Möbius function*, $\mu(n)$, is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ for distinct primes } p_i\ , \\ 0 & \text{otherwise.} \end{cases}$$

Note that it can be easily seen that $\mu(mn) = \mu(m)\mu(n)$ whenever $(m, n) = 1$. Also, $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise} \end{cases}$

Lemma 1.2 If $\mu(n)$ denotes the Möbius function, then,

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

Proof. We shall prove that if $f(n) = \prod_{d|n} g(d)$, then $g(n) = \prod_{d|n} f(n/d)^{\mu(d)}$.

$$\begin{aligned} \text{We have, } \prod_{d|n} f(n/d)^{\mu(d)} &= \prod_{d|n} \left(\prod_{m|(n/d)} g(m) \right)^{\mu(d)} \\ &= \prod_{m|n} \left(\prod\nolimits_{d|(n/m)} g(m)^{\mu(d)} \right) \\ &= \prod_{m|n} g(m)^{\sum_{d|(n/m)} \mu(d)} \;=\; g(n). \end{aligned}$$

Since $X^n - 1 = \prod_{d|n} \Phi_d(X)$, we are done. □

Lemma 1.3
(i) If $n = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}$, $a_i > 0$, *and* $N = p_1 p_2 \cdots p_\ell$, *then* $\Phi_n(X) = \Phi_N(X^{n/N})$.
(ii) If $n > 1$ *and* $(2, n) = 1$, *then* $\Phi_{2n}(X) = \Phi_n(-X)$.
(iii) For all positive integers $n > 1$, *we have* $X^{\phi(n)} \Phi_n(1/X) = \Phi_n(X)$.

Proof. (i) Since $\mu(m) = 0$ for all integers m which are not square free, we have,

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

This proves part (i).
(ii) Consider

$$\begin{aligned} \Phi_{2n}(X) &= \prod_{d|(2n)} (X^d - 1)^{\mu(2n/d)} \\ &= \prod_{2|d} (X^d - 1)^{\mu((2n)/d)} \prod_{d|n} (X^d - 1)^{\mu((2n)/d)} \\ &= \prod_{d|n} \left[(X^d - 1)^{\mu(2n/d)} (X^{2d} - 1)^{\mu(n/d)} \right] \\ &= \prod_{d|n} (X^d + 1)^{\mu(n/d)}, \text{ as } \mu(2m) = -\mu(m) \; for \; odd \; m \\ &= \prod_{d|n} (-X^d - 1)^{\mu(n/d)} = \Phi_n(-X). \end{aligned}$$

(iii) Now, consider

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

Therefore we get,

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

Since $\sum_{d|n} d\mu(n/d) = \phi(n)$, we get the result. □

2. The Coefficients of Cyclotomic Polynomials

Since $\Phi_n(X)$ is a polynomial with degree $\phi(n)$, we can write

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

where $a_n(i)$ denotes the i-th coefficient.

Lemma 2.1
(i) $a_n(i) \in \mathbb{Z}$ *for all* $i,\ 0 \le i \le \phi(n),\ n \in \mathbb{N}$.
(ii) $a_n(i) = a_n(\phi(n) - i)$ *for all* $i,\ 0 \le i \le \phi(n),\ n\ (>1) \in \mathbb{N}$. *That is, the coefficients of cyclotomic polynomials are symmetric.*

Proof. (i) follows from Lemma 1.1. Also (ii) follows from Lemma 1.3(iii) immediately. □

Remark 2.2
(1) Lemma 1.3(i) says that

$$a_n(i) = \begin{cases} a_N(iN/n) & \text{if } \frac{n}{N}|i \\ 0 & \text{otherwise.} \end{cases}$$

(2) From Lemma 1.3(ii) we get for odd $n > 1$, $a_{2n}(i) = (-1)^i a_n(i)$.
(3) When $n = p$ a prime number, from Lemma 1.2 we have

$$\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Hence $a_p(i) = 1$ for all $i = 0, 1, \cdots, p-1$.

Thus 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.

When $n = p$ a prime number, as we had seen earlier,

$$a_p(i) = \begin{cases} 1 & \text{if } i = 0, 1, \cdots, p-1 \\ 0 & \text{for all integers } i > p-1. \end{cases}$$

We shall now pass on to the next interesting case when $n = pq$ where p and q are two distinct odd prime numbers. Here are two explicit examples:

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

$$\text{and } \Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1.$$

In 1883, Migotti [27] showed that all $a_{pq}(i) \in \{0, \pm 1\}$. Marion Beiter [5] and [8] gave a criterion on i for $a_{pq}(i)$ to be $0, 1$ or -1. Also Carlitz [11] computed the number of non-zero $a_{pq}(i)$'s. Here, we shall give a simpler proof of the following theorem due to Lam and Leung [19].

Theorem 2.3 *Let r and s be non-negative integers such that $(p-1)(q-1) = rp + sq$ written uniquely. Then we have*

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

Also, for $0 \le k \le (p-1)(q-1)$, we have
(1) $a_{pq}(k) = 1$ if and only if $k = ip + jq$ for some $i \in [0, r]$ and $j \in [0, s]$;
(2) $a_{pq}(k) = -1$ if and only if $k + pq = ip + jq$ for some $i \in [r+1, q-1]$ and $j \in [s+1, p-1]$; and
(3) $a_{pq}(k) = 0$ otherwise.

The number of terms of the former two kinds are, respectively, $(r+1)(s+1)$ and $(p-s-1)(q-r-1)$, with difference 1.

Proof. We know that $\phi(pq) = (p-1)(q-1)$ can be expressed uniquely in the form $rp + sq$ where r, s are non-negative integers (see for instance [23], Page 22, Ex. 4). Since $(p-1)(q-1) = rp + sq$, it is clear that $r \le q-2$ and $s \le p-2$.

Now, we shall prove that

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

Let $\zeta = e^{2i\pi/(pq)}$ be a primitive pq-th root of unity. Then since $\zeta^p = e^{2i\pi/q}$ and $\zeta^q = e^{2i\pi/p}$, we have $\Phi_p(\zeta^q) = \Phi_q(\zeta^p) = 0$. That is, we have

$$\sum_{i=0}^{q-1} (\zeta^p)^i = 0 = \sum_{j=0}^{p-1} (\zeta^q)^j.$$

Therefore,

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

Hence multiplying these two, we get the identity

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

Thus ζ is a zero of the polynomial

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

Since $rp+sq=(p-1)(q-1)$, the first product in (1) is a monic polynomial of degree $(p-1)(q-1)$. In the second product, the lowest term has degree $(r+1)p+(s+1)q-pq=rp+sq+p+q-pq=1$ and its highest term has degree $(q-1)p+(p-1)q-pq=(p-1)(q-1)-1$. Hence the second product is also a monic polynomial of degree $(p-1)(q-1)-1$. Therefore $f(X)\in\mathbb{Z}[X]$ is a monic polynomial of degree $(p-1)(q-1)=\phi(pq)$. Moreover, we know that $f(\zeta)=0$. If ζ' is any other primitive pq-th 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 $(m,pq)=1$, we must have $f(X)=\Phi_{pq}(X)$.

Now note that if $i,i'\in[0,q-1]$, $j,j'\in[0,p-1]$, and $ip+jq$ is equal to $i'p+j'q$ or $i'p+j'q-pq$, then $q|(i-i')$ and $p|(j-j')$. This implies that $i=i'$ and $j=j'$.

If we expand the products in equation (1), then using the above note, the rest of the assertions follow immediately. □

Remark 2.4 Theorem 2.3 together with our earlier observations proves that the coefficients of the first 104 cyclotomic polynomials are all $\pm1,0$.

Corollary 2.5 *Assume that $q>p$, and let $\ell=(p-1)(q-1)/2$. Then the middle coefficient $a_{pq}(\ell)$ of $\Phi_{pq}(X)$ is $(-1)^r$.*

Proof. By Remark 2.2(2), we can assume that $p>2$. Since $(p-1)(q-1)=rp+sq$, r and s have the same parity. If r is even, then $\ell=(r/2)p+(s/2)q$. Therefore, by Theorem 2.3, we have $a_{pq}(\ell)=1$. If r is odd, then so is s, and we can write,

$$\ell+pq=\left(\frac{r+q}{2}\right)p+\left(\frac{s+p}{2}\right)q.$$

Since $r\le q-2$ and $s\le p-2$, we have $(r+q)/2\in[r+1,q-1]$ and $(s+p)/2\in[s+1,p-1]$. Therefore by Theorem 2.3, we have $a_{pq}(\ell)=-1$. Note that when $p=2$, by Remark 2.2(2), we have $a_{2q}(\ell)=(-1)^\ell a_q(\ell)=(-1)^{(q-1)/2}=(-1)^r$. (since $2r+sq=q-1\Longrightarrow r=(q-1)/2$). □

Thus, Theorem 2.3 finishes the problem of finding the values of the coefficients of cyclotomic polynomials explicitly in the case when $n = pq$ where p and q are two distinct odd primes.

If n is a product of more than two distinct primes, then the explicit values of the coefficients are not known in general. But in the case when $n = pqr$, some good amount of progress has been made. Let us discuss this case briefly.

In 1895, Bang [2] proved that the upper bound for the magnitude of the coefficients of $\Phi_{pqr}(X)$ where p, q, r are odd primes such that $p < q < r$ is $p - 1$. Then, in 1968, Marion Beiter [6] and Bloom [9] simultaneously established $(p+1)/2$ as the upper bound in the special case where q and/or r is congruent to ± 1 modulo p. In 1971, Beiter [7] gave the following better general bound.

Theorem 2.6 [7] *The magnitude of the largest coefficient of $\Phi_{pqr}(X)$ where p, q, r are odd primes such that $p < q < r$ is less than or equal to $p - k$ or $p - (k + 1)$ for $p = 4k + 1$ or $4k + 3$ respectively.*

We shall skip the proof of this theorem.

Remark 2.7 Note that when $p = 3$, Theorem 2.6 says that $|a_{3qr}(i)| \leq 2$ for all i. Remark 2.5 together with this, we see that the first cyclotomic polynomial $\Phi_{105}(X)$ where we can look for a non-zero coefficient whose magnitude is not just one; but two. In fact this is the case. Indeed, it was shown by Migotti [27] in 1883 that the coefficient of X^7 in the 105-th cyclotomic polynomial is equal to -2. In fact, the 105th cyclotomic polynomial is as follows:

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

Later, P. Erdös [13] showed that $a_n(i) = 0, \pm 1$ for all i and for all $n < 105$ and that $a_{105}(7) = 2$. Also M. Endo [12] proved that $(k, n) = (7, 105)$ is the smallest pair for which $|a_n(k)| > 1$ by a different method.

Conjecture (Beiter, 1971) *$a_{pqr}(i) \leq (p+1)/2$ for all i and for any $p < q < r$ and this upper bound is the best possible.*

Indeed, Beiter remarks in the same paper [7] that the above conjecture is true for $p = 3, 5$ and for any $q < r$. In support of the above conjecture, Möller [29] proved the following theorem.

Theorem 2.8 *Let $3 < p < q < r$ be prime numbers satisfying $q \equiv 2 \pmod{p}$ and $r = \frac{1}{2}(mpq - 1)$ for some integer m. Then,*

$$a_{pqr}((p-1)(qr+1)/2) = \frac{1}{2}(p+1).$$

Recently, W. Bosma [10] has written an expository article on the various methods which are helpful in computing cyclotomic polynomials and its coefficients.

Thus from the above theorems and remarks, it appears that the growth of the magnitude of the coefficients of cyclotomic polynomials is very slow. However, it is not very clear at this stage whether the coefficients can take arbitrarily large values.

Schur [33] was the first one to show that there are cyclotomic polynomials whose coefficients are arbitrarily large. If we let $A(n) = \max_m |a_n(m)|$, then Schur showed that $\limsup_{n \longrightarrow \infty} A(n) = \infty$.

We shall give a trivial upper bound for $|a_n(m)|$ for all m in terms of n alone as follows.

Lemma 2.9 *We have* $\log(A(n)) \ll \sqrt{n}$.

Proof. Since using Lemma 1.2, it can be seen that the coefficient of z^m in $\prod_{d \geq 1}(1 - z^d)^{-1}$ is greater than or equal to $|a_n(m)|$ and the former is nothing but $p(m)$ where $p(m)$ is the number of partitions of m, we get $|a_n(m)| \leq p(m)$ for all m.

This inequality together with the Hardy-Ramanujan [18] asymptotic formula for $p(m)$ in the form

$$\log |p(m)| \sim \pi\sqrt{2/3}\ \sqrt{m} \quad \text{as} \quad m \to \infty$$

implies the estimate $\log(a_n(m)) \ll \sqrt{m}$. Since $a_n(m) = 0$ for all $m > n$, the above estimate yields the bound that $\log(A(n)) \ll \sqrt{n}$. □

Since $A(p) = 1$, the only lower bound for $A(n)$ which is valid for all n is the trivial bound $A(n) \geq 1$.

Erdös [14] and [15] has shown that occasionally the coefficients can get very large indeed. More precisely, he showed that $\exists\ c > 0$ such that

$$\log A(n) \gg \exp\left(\frac{c \log n}{\log \log n}\right).$$

Using the refinement of the above argument in Lemma 2.9, Bateman improved the bound in Lemma 2.9 which gives the following bound for the

maximum of the absolute values of the coefficients of cyclotomic polynomials:

$$\log A(n) < \left\{ \exp\left((\log 2 + o(1)) \frac{\log n}{\log\log n} \right) \right\}.$$

The constant $\log 2$, here, is the best possible. This was first asked by P. Erdös [14] and then shown by Vaughan [31].

In 1981, Bateman, Pomerence and Vaughan [4] have refined these results by giving estimates for $A(n)$ in terms of prime factors of n. More recently, Maier [26] showed that for any function $\chi(n)$ tending to infinity, the inequality $A(n) \leq n^{\chi(n)}$ for almost all n.

On the other hand, Maier [24] had earlier proved that, for any function $\epsilon(n)$ defined for all positive integers such that $\epsilon(n)$ tends to zero as n tends to infinity, the inequality $A(n) \geq n^{\epsilon(n)}$ holds except perhaps for a set of positive integers of zero natural density. This settled a long-standing conjecture ($A(n) \to \infty$ for almost all n) of Erdös. Later, he [25] proved that for any $N > 0$, there exists a positive constant $C(N)$ depending on N such that the lower density of the set of n's for which the inequality $A(n) \geq n^N$ is at least $C(N)$. Therefore, Maier's upper bound for $A(n)$ is the best possible one.

In the proof of Lemma 2.9, we first gave an upper bound for $|a_n(m)|$ which is independent of n. More precisely, we proved that $|a_n(m)| \leq p(m)$ where $p(m)$ is the number of partitions of m. Indeed, Möller [28] showed that $|a_n(m)| \leq p(m) - p(m-2)$.

Now we define a dual function (which was first considered by Erdös and Vaughan [16])

$$B(m) = \max_n |a_n(m)|.$$

Note that in the definition of $B(m)$, we can replace maximum by limit supremum. This is because $a_n(m) = a_{npq}(m)$ for all primes p and q with $(n,p) = 1 = (m,q)$ and they are greater than m. Hence from the arguments given in the proof of Lemma 2.9, we can conclude that

$$\log B(m) \ll \sqrt{m}.$$

The first non-trivial result in this direction is due to Erdös and Vaughan [16] who showed that

$$|a_n(m)| < \exp\left\{ \left(\tau^{1/2} + o(1) \right) m^{1/2} \right\}$$

uniformly in n as m tends to infinity, where

$$\tau = \prod_p \left(1 - \frac{2}{p(p+1)} \right).$$

They also further showed that for every large m

$$\log B(m) \ll \sqrt{\frac{m}{\log m}}$$

and conjectured that $\log(B(m)) = o(m^{1/2})$.

Vaughan [31] has obtained a sharper bound for infinitely many m; viz.

$$\limsup_{n\to\infty} \left(m^{-1/2} (\log m)^{1/4} \log(B(m)) \right) > 0.$$

Montgomery and Vaughan [30] proved the conjecture of Erdös *et al.* in this connection, by proving that $B(m)$ is of exact order $m^{1/2}(\log m)^{-1/4}$.

Recently, Bachman [1] improved the work of Montgomery and Vaughan. He derived the asymptotic formula

$$\log B(m) = C_o \frac{\sqrt{m}}{(\log m)^{1/4}} \left(1 + O\left(\frac{\log\log m}{\sqrt{\log m}} \right) \right).$$

Though some coefficients of cyclotomic polynomials can grow arbitrarily large, it is not still apparent that the collection of all of $a_n(m)$ for all n and m can cover the whole set of integers. This was proved by Jiro Suzuki [34] in 1987.

Theorem 2.10 [34]

$$\mathbb{Z} = \{ a_n(k) | \quad k, n \in \mathbb{N} \}.$$

Proof. Let us first prove the following claim. The claim says that if t is any integer greater than 2, then there exist t distinct primes $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$.

Assume the contrary, that is, there exists an integer $t > 2$ for which the claim is false. For this t, given any t distinct primes $p_1 < p_2 \cdots < p_t$, 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 $p_1 > 2^{k-1} \Longrightarrow 2p_1 > 2^k > p_t$ 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 $\pi(x) > x/\log x$ 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 $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$.

Let $p = p_t$ and $n = p_1 p_2 \cdots p_t$. Now consider $\Phi_n(X)$. We have, $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$. 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

$i = 1, 2, \cdots, t$ we have

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

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

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

then, $\mathbf{S}$ contains $\{\ell \in \mathbb{Z} \mid \ell \leq -1\}$ as t varies over all the odd integer greater than or equal to 3. By Theorem 2.3, already we know $\{0, \pm 1\} \subset \mathbf{S}$. In order to prove that $\mathbf{S}$ contains all positive integers greater than or equal to 2, consider $\Phi_{2n}(X)$ where $n = p_1p_2\cdots p_t$. By Lemma 1.3(ii), 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 $\mathbf{S}$ contains all the positive integers greater than or equal to 1. □

Theorem 2.10 says that given any integer k, then there exist natural numbers n and m for which $a_n(m) = k$. In 1991, Grytczuk and Tropak [17] considered the following problem:

Given integer k such that $|k| \geq 2$, find the minimal m for which there exists a natural number n such that $a_n(m) = k$.

If m is one such, then for all n, we must have $a_n(r) \neq k$ for all $r < m$.

For example, if $k = -2$, then we know that $m = 7$ is the minimal integer for which $a_{105}(7) = -2$.

From Lemma 1.2, we know that

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

by setting $\mu(n/d) = 0$ whenever n/d is not an integer.

From this identity, it follows that, for a square-free integer n, the value $a_n(m)$ depends only on the values of $\mu(n), \mu(n/d)$ and on the primes less than $m+1$ which happent to divide n.

Using this identity, we can derive a formula for $a_n(m)$ for a fixed m as follows.

$$a_n(1) = -\mu(n), a_n(2) = 1/2\mu(n)(\mu(n)-1) - \mu(n/2)$$

$$a_n(3) = 1/2\mu(n)^2 - 1/2\mu(n) + \mu(n/2)\mu(n) - \mu(n/3), \cdots$$

This method has been used by D. H. Lehmer [20] and H. Möller [28].

A. Grytczuk and B. Tropak [17] derived a recurrence relation for the coefficients of n-cyclotomic polynomial as follows.

$$a_n(m) = -\frac{1}{m}\sum_{\ell=0}^{m-1} a_n(\ell)T_{m-\ell}$$

where $T_{m-\ell} = \mu(n)\mu((n, m-\ell))\phi((n, m-\ell))$ with $a_n(0) = 1$.

Using this recurrence relation, they found for $k = \pm 2, \pm 3, \cdots, \pm 9$ and 10, the minimal values of m for which there exist n such that $a_n(m) = k$.

Acknowledgement: I would like to thank Professor S. A. Katre for carefully going through the manuscript and pointing out several corrections.

References

[1] G. Bachman, *On the coefficients of cyclotomic polynomial*, Mem. Amer. Math. Soc., 106, no. 510 (1993).

[2] A. S. Bang, *Om ligningen* $\Phi_n(X) = 0$, Tidsskrift for Math., 6-12, (1985).

[3] P. T. Bateman, *Note on the coefficients of cyclotomic polynomial*, Bull. Amer. Math. Soc., 55, 1180-1181 (1949).

[4] P. T. Bateman, C. Pomerance and R. C. Vaughan, *On the coefficients of cyclotomic polynomial*, Coll. Math. Soc. J. Bolyai, 34, Topics in classical number theory, 171-202, Budapest, (1981).

[5] M. Beiter, *The midterm coefficient of the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, 71, 769-770 (1964).

[6] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomials* $\Phi_{pqr}(X)$, Amer. Math. Monthly, 75, 370-372 (1968).

[7] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomials* $\Phi_{pqr}(X)$ *II*, Duke Math. Jour., 38(3), 591-594 (1971).

[8] M. Beiter, *Coefficients in the Cyclotomic polynomial for numbers with at most three distinct odd primes in their factorization*, The catholic university of America Press, Washington, (1960).

[9] D. M. Bloom, *On the coefficients of the cyclotomic polynomials,* Amer. Math. Monthly, 75, 372-377 (1968).

[10] W. Bosma, *Computation of cyclotomic polynomials with Magma*, in: W. Bosma et al (eds.) Computational algebra and Number Theory, Netherlands: Kluwer Academic Publishers, 216-225 (1995).

[11] L. Carlitz, *The number of terms in the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, 73, 979-981 (1966).

[12] M. Endo, *On the coefficients of the cyclotomic polynomials,* Comment. Math. Univ. St. Pauli, 23, 121-126, (1974/75).

[13] P. Erdös, *On the coefficients of the cyclotomic polynomials,* Bull. Amer. Math. Soc., 52, 179-181, (1946).

[14] P. Erdös, *On the coefficients of the cyclotomic polynomials,* Portugal. Math. 8, 63-71 (1949).

[15] P. Erdös, *On the growth of the cyclotomic polynomials in the interval* $(0, 1)$*,* Proc. Glasgow Math. Assoc. 3, 102-104 (1957).

[16] P. Erdös and R. C. Vaughan, *Bounds for* r*-th coefficients of cyclotomic polynomials*, J. London Math. Soc.(2) 8, 393-400 (1974).

[17] A. Grytczuk and B. Tropak, *A numerical method for the determination of the cyclotomic polynomial coefficients*, in: A. Pethö et al (eds.), Computational Number Theory, Berlin: de Gruyter, 15-19 (1991).
[18] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatorial analysis*, Proc. London Math. Soc. 17, 75-115 (1918).
[19] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, 562-564 (1996).
[20] D. H. Lehmer, *Some properties of cyclotomic polynomials*, J. Math. Anal. Appl., 15, 105-117 (1966).
[21] E. Lehmer, *On the magnitude of coefficients of the cyclotomic polynomials*, Bull. Amer. Math. Soc., 42 (1936).
[22] H. W. Lenstra, Jr, *Vanishing sums of roots of unity*, Proc. Bicentennial Congress Wiskundig Genootshapp. Part II, Math. Centre Tracts, 101, Math. Centrum, Amsterdam, 249-268 (1979).
[23] W. LeVeque, *Topics in number theory*, Vol 1, Addison-Wesley, Reading, Mass., (1956).
[24] H. Maier, *The coefficients of cyclotomic polynomials*, Analytic number theory, Proc. of a Conf. in Honor of P. T. Bateman, Prog. Math. 85, 349-366 (1990).
[25] H. Maier, *Cyclotomic polynomials with large coefficients*, Acta Arith., 64, 227-235 (1993).
[26] H. Maier, *The size of the coefficients of cyclotomic polynomials*, Analytic number theory, Proc. of a Conf. in Honor of P. T. Bateman, Prog. Math. , 633-639 (1995).
[27] A. Migotti, *Aur Theorie der Kreisteilungsgleichung*, Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, 87, 7-14 (1883).
[28] H. Möller, *Über die i-ten Koeffizienten der Kreisteilungspolynome*, Math. Ann., 188, 26-38 (1970).
[29] H. Möller, *Über die Koeffizienten des n-ten Kreisteilungspolynome*, Math. Z., 119, 34-40 (1971).
[30] H. L. Montgomery and R. C. Vaughan, *The order of the m-th coefficients of cyclotomic polynomials*, Glasgow Math. J., 143-159 (1985).
[31] R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. 21, 289-295 (1975).
[32] R. C. Vaughan, *Adventures in arithmetick, or: How to make good use of a Fourier transform*, The Math. Intelligencer, 9(2), 53-60 (1987).
[33] I. Schur, *Letter to Landau* (1935). (see [21]).
[34] J. Suzuki, *On coefficients of cyclotomic polynomials*, Proc. Japan Acad., 63, Ser. A, 279-280 (1987).

R. Thangadurai
Mehta Research Institute
Chhatnag Road, Jhusi
Allahabad 211 019, India.

Current Address:
Institute of Mathematical Sciences
Tharamani
Chennai 600 113
e-mail: thanga@imsc.ernet.in