Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43) 2** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.78979

Properties on Cyclotomic Polynomials and The Möbius Function

Enagandula Prasad

ABSTRACT: If n is a natural number, then the n^{th} cyclotomic polynomial denoted by $\Phi_n(x)$ and defined as the unique monic polynomial having exactly the primitive n^{th} roots of unity as its zeros. In this article we are going to derive properties related to cyclotomic polynomials using Mobious Inversion Formula.

Key Words: Cyclotomic polynoials, prime numbers, the Mobius function.

Contents

1. Introduction

Polynomials appearing in such factorizations are called cyclotomic polynomials. The first few cyclotomic polynomials are

$$\Phi_1(x) = x - 1 \quad \Phi_2(x) = x + 1 \quad \Phi_2(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1 \quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

Definition 1.1 *The n-th cyclotomic polynomial is defined as*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - e^{2\pi i k/n} \right) \tag{1.1}$$

Definition 1.2 *The cyclotomic polynomial, n-th root of unity is a primitive d-th root of unity for a unique d dividing n*

$$x^n - 1 = \prod_{d|n} \Phi_n(x) \tag{1.2}$$

Definition 1.3 *Suppose n is a positive integer. Then the function is Mobius function defined as* $\mu : N \to \{-1, 1, 0\}$ *then*

$$\mu(n) = \begin{cases} 1 & if \quad n = 1 \quad for \quad all \quad values \quad of \quad k \\ (-1)^n & if \quad n = p_1.p_2.p_3...p_k \quad for \quad distrinct \quad primes \\ 0 & \quad Otherwise \end{cases} \tag{1.3}$$

is called the M¨obius function

Definition 1.4 *The Möbius inversion formula allows $\Phi_n(x)$ to be expressed as an explicit rational fraction*

$$\Phi_n(x) = \prod_{d|n} \left((x^d - 1)^{\mu(n/d)} \right) \tag{1.4}$$

2010 *Mathematics Subject Classification:* 11R18, 11R11.
Submitted September 16, 2025. Published December 19, 2025

2. Results

Theorem 2.1 *Let $p_1, p_2, \ldots, p_n$ are distinct primes, and $a_1, a_2, \ldots, a_n$ are natural numbers then,*

$$\Phi_{p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}}(x) = \Phi_{p_1 p_2 \ldots p_n}\left(x^{a_1 . a_2 . \ldots . a_n}\right) \tag{2.1}$$

Proof: To prove the current theorem, it suffices to prove that $\Phi_{p_1^{a_1} p_2^{a_2}}(x) = \Phi_{p_1 p_2}(x^{a_1 a_2})$ we know that by (4)

$$\begin{aligned}
LHS = \Phi_{p_1^{a_1} p_2^{a_2}}(x) &= \prod_{d|(p_1^{a_1} p_2^{a_2})} (x^d - 1)^{\mu((p_1^{a_1} p_2^{a_2})/d)} \\
&= \prod_{d|(p_1^{a_1} p_2^{a_2})} (x^d - 1)^{\mu((p_1^{a_1} p_2^{a_2})/d)} \\
&= \prod_{d|(p_1^{a_1} p_2^{a_2})} (x^{((p_1^{a_1} . p_2^{a_2})/d)} - 1)^{\mu(d)} \\
&= \prod_{d|(p_1^{a_1} p_2^{a_2})} (x^{(p_1^{a_1} . p_2^{a_2} a_1 . a_2 d / a_1 a_2 . d^2)} - 1)^{\mu(d)} \\
&= \prod_{d|(p_1^{a_1} p_2^{a_2})} (x^{(a_1 a_2 . d)} - 1)^{\mu((p_1^{a_1} p_2^{a_2})/a_1 . a_2 . d^2)} \\
&= \prod_{(a_1 a_2 . d)|(p_1^{a_1} p_2^{a_2})} (x^{(a_1 a_2 . d)} - 1)^{\mu((p_1^{a_1} p_2^{a_2})/a_1 . a_2 . d)} \\
&\quad \prod_{(a_1 . a_2 . d)\nmid(p_1^{a_1} p_2^{a_2})} (x^{(a_1 . a_2)})^d - 1)^{\mu(p_1^{a_1} p_2^{a_2} / a_1 . a_2 . d)} \\
&= \prod_{(a_1 a_2 . d)|(p_1^{a_1} p_2^{a_2})} (x^{(a_1 a_2 . d)} - 1)^{\mu((p_1^{a_1} p_2^{a_2})/a_1 . a_2 . d)} \\
&= \Phi_{p_1 p_2}\left(x^{a_1 . a_2}\right) = RHS
\end{aligned}$$

In general $\quad \Phi_{p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}}(x) = \Phi_{p_1 p_2}(x^{a_1 . a_2 \ldots . a_n})$ ☐

Example 2.1 $\Phi_{2^2 3^1}(x) = \Phi_{2.3}(x^{2.1}$

Example 2.2 $\Phi_{2^2 3^2}(x) = \Phi_{2.3}(x^{2.2})$

Proof: 2.1. We need to prove that $\Phi_{12}(x) = \Phi_6(x^2)$
L.H.S $=\Phi_{12}(x)$

$$\begin{aligned}
&= (x^1 - 1)^{\mu(2^2.3/1)} . (x^2 - 1)^{\mu(2^2.3/2)} . (x^3 - 1)^{\mu(2^2.3/3)} . (x^4 - 1)^{\mu(2^2.3/4)} \\
&(x^6 - 1)^{\mu(2^2.3/6)} . (x^{12} - 1)^{\mu(2^2.3/12)} \\
&= (x^1 - 1)^{\mu(2^2.3/1)} . (x^2 - 1)^{\mu(2^2.3/2)} . (x^3 - 1)^{\mu(2^2.3/3)} . (x^4 - 1)^{\mu(2^2.3/4)} \\
&(x^6 - 1)^{\mu(2^2.3/6)} . (x^{12} - 1)^{\mu(2^2.3/12)} \\
&= (x^1 - 1)^{\mu(2^2.3/1)} . (x^2 - 1)^{\mu(2^2.3/2)} . (x^3 - 1)^{\mu(2^2.3/3)} . (x^4 - 1)^{\mu(2^2.3/4)} \\
&(x^6 - 1)^{\mu(2^2.3/6)} . (x^{12} - 1)^{\mu(2^2.3/12)} \\
&= (x^1 - 1)^{\mu(2^2.3)} . (x^2 - 1)^{\mu(2.3)} . (x^3 - 1)^{\mu(2.2)} . (x^4 - 1)^{\mu(1.3)} \\
&\quad (x^6 - 1)^{\mu(1.2)} . (x^{12} - 1)^{\mu(1.1)} \\
&= (x^1 - 1)^{\mu(12)} . (x^2 - 1)^{\mu(6)} . (x^3 - 1)^{\mu(4)} . (x^4 - 1)^{\mu(3)} \\
&(x^6 - 1)^{\mu(2)} . (x^{12} - 1)^{\mu(1)} \\
&= x^4 + -x^2 + 1 = 0 = \Phi_6(x^2) = R.H.S
\end{aligned}$$

□

Lemma 2.1 *Let $m \in \mathbb{N}$ with $m \geq 1$, and let $\Phi_{2^m}(x)$ be the 2^m-th cyclotomic polynomial. Then for any prime p,then $\Phi_{2^m}(p)$ is even.*

Proof: Let us assume that for all integers $m \geq 1$, the cyclotomic polynomial of the form $\Phi_{2^m}(p)$ is odd,then $\exists$ an integer k such that

$$\Phi_{2^m}(p) = 2k + 1.$$

$$k = \frac{\Phi_{2^m}(p) - 1}{2}$$

Then as we have taken $\Phi_{2^m}(p)$ odd then k must be a rational number. Contradiction to $\Phi_n(x)$ is never be a rational number for any n natural number □

Example 2.3 $\Phi_{2^3}(3) = 82$

Lemma 2.2 *Let $n \in \mathbb{N}$ with $n \geq 1$, and let $\Phi_{2^n}(x)$ be the 2^n-th cyclotomic polynomial,then*

$$\Phi_{2^n}(x) = \Phi_{2^n}(-x) \tag{2.2}$$

for all $n \in \mathbb{N}$,$n \geq 2$.

Proof: We know that by (1.4) LHS=$\Phi_{2^n}(x)$

$$\begin{aligned}
&= \prod_{d|2^n} (x^d - 1)^{\mu(2^n/d)} \\
&= \prod_{d|2^n} (x^{(2^n/d)} - 1)^{\mu(d)} \\
&= \prod_{d|2^n} ((-x)^{(2^n/d)} - 1)^{\mu(d)} \\
&= \prod_{d|2^n} ((-x)^d - 1)^{\mu(2^n/d)} \\
&= \Phi_{2^n}(-x) = R.H.S
\end{aligned}$$

□

Example 2.4

$$\Phi_{2^2}(3) = \Phi_{2^2}(-3) = 10$$

Lemma 2.3 *Let p and q are primes and $p, q \in \mathbb{N}$ with $p, q \geq 1$,let $\Phi_n(x)$ be the n-th cyclotomic polynomial,then*

$$\Phi_p(x)\Phi_q(x) = \frac{(x^p - 1)(x^q - 1)}{(x - 1)^2} \tag{2.3}$$

Proof: We know that by (1.1)
LHS =$\Phi_p(x)\Phi_q(x)$

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

Since p and q are prime only values of d =1,p and q and gcd(p,q)=1

$$= (x^1-1)^{\mu(p)}(x^p-1)^{\mu(1)}(x^1-1)^{\mu(q)}(x^q-1)^{\mu(1)}$$

Since p and q are prime only values of d =1,p and q and $\mu(p) = -1, \mu(q) = -1, \mu(p) = 1$

$$\begin{aligned}
&= (x^1-1)^{\mu(p)}(x^p-1)^{\mu(1)}(x^1-1)^{\mu(q)}(x^q-1)^{\mu(1)} \\
&= (x^1-1)^{\mu(p)}(x^p-1)^{\mu(1)}(x^1-1)^{\mu(q)}(x^q-1)^{\mu(1)} \\
&= (x^1-1)^{-1}(x^p-1)^{1}(x^1-1)^{-1}(x^q-1)^{1} \\
&= \frac{(x^p-1)(x^q-1)}{(x-1)^2} = RHS
\end{aligned}$$

Therefore

$$\therefore \Phi_p(x)\Phi_q(x) = \frac{(x^p-1)(x^q-1)}{(x-1)^2}$$

general

$$\Phi_{p_1}(x)\Phi_{p_2}(x)\ldots,\Phi_{p_n}(x) = \frac{(x^{p_1}-1)(x^{p_2}-1)\ldots,(x^{p_n}-1)}{(x-1)^n}$$

□

Example 2.5

$$\Phi_2(x)\Phi_3(2) = \frac{(x^2-1)(2^3-1)}{(2-1)^2} = 21$$

Theorem 2.2 ***Proved:*** *For any prime p and $m \in \mathbb{N}$*

$$\Phi_{p^m}(x) = \sum_{k=1}^{p-1} x^{kp^{m-1}}$$

Lemma 2.4 *Let p is prime and $m \in \mathbb{N}$ with $p, m \geq 1$,let $\Phi_n(x)$ be the n-th cyclotomic polynomial,then*

$$\Phi_{p^m}(x) \equiv 1(mod \quad p) \tag{2.4}$$

Proof: We know that by (1.1)

$$a \equiv b \pmod{n} \quad \text{iff} \quad n \mid (b-a)$$

It is understood that p divides $\Phi_{p^m}(x) - 1$. Assume that p does not divides $\Phi_{p^m}(x) - 1$
Then there exists a $k \in \mathbb{N}$ such that
$\Phi_{p^m}(x) - 1 = pk + 1$
$\Longleftrightarrow \Phi_{p^m}(x) = pk + 2$

$$\therefore k = \frac{\Phi_{p^m}(x) - 2}{2}$$

□

Therefore k is even or fraction always which is contradiction the above theorem and definition of cyclotomic polynomial. and therefore
= p | $(\Phi_{p^m}(x) - 1)$
Hence

$$\Phi_{p^m}(x) \equiv 1(mod \quad p)$$

Example 2.6 $\Phi_{3^2}(2) \equiv 1(mod \quad 3)$
$\Longleftrightarrow \Phi_9(2) \equiv 1(mod \quad 3)$
$\Longleftrightarrow 73 = 1(mod \quad 3)$
$\Longleftrightarrow 3 \mid 72$

Lemma 2.5 *Let p and q are prime and $p, q \in \mathbb{N}$,let $\Phi_n(x)$ be the n-th cyclotomic polynomial,then*

$$\Phi_p(x)\Phi_q(x^p) = \Phi_q(x)\Phi_p(x^q) \tag{2.5}$$

Proof: We know that by (1.4)
LHS=$\Phi_p(x)\Phi_q(x^p)$

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

Since p and q are prime gcd(p,q)=1 and using the definition of $\mu(n)$

$$\begin{aligned}
&= \prod_{d|p}((x^q)^d - 1)^{\mu(p/d)}\prod_{d|q}(x^d - 1)^{\mu(q/d)} \\
&= \Phi_p(x^q)\Phi_q(x) \\
&= RHS
\end{aligned}$$

□

Example 2.7 $\Phi_3(x)\Phi_2(x^3) = \Phi_2(x)\Phi_3(x^2)$ *LHS*=$\Phi_3(x)\Phi_2(x^3)$

$$= \prod_{d|3}(x^d - 1)^{\mu(3/d)}\prod_{d|2}((x^3)^d - 1)^{\mu(2/d)}$$

Since p and q are prime gcd(p,q)=1 and using the definition of $\mu(n)$ for the part 1 we have d=1,3 and second part d=1,2

$$\begin{aligned}
&= (x^1 - 1)^{\mu(3)}(x^3 - 1)^{\mu(1)}((x^3)^1 - 1)^{\mu(2)}((x^3)^2 - 1)^{\mu(1)} \\
&= (x^1 - 1)^{-1}(x^3 - 1)^1((x^3)^1 - 1)^{-1}((x^3)^2 - 1)^1 \\
&= (x^1 - 1)^{-1}(x^3 - 1)^1((x^3)^1 - 1)^{-1}(x^6 - 1)^1 \\
&= (x^1 - 1)^{-1}(x^3 - 1)^1((x^3 - 1)^{-1}(x^6 - 1)^1 \\
&= (x^1 - 1)^{-1}(x^3 - 1)^1((x^3 - 1)^{-1}(x^6 - 1)^1 \\
&= (x^1 - 1)^{-1}((x^2)^3 - 1)^1(x^3 - 1)^1((x^3 - 1)^{-1} \\
&= (x^1 - 1)^{-1}((x^2)^3 - 1)^1 \\
&= (x^1 - 1)^{-1}((x^2)^3 - 1)^1(x^2 - 1)^1((x^2 - 1)^{-1} \\
&= ((x^2 - 1)^{-1}((x^2)^3 - 1)^1(x^1 - 1)^{-1}((x^2 - 1)^{-1} \\
&= \prod_{d|3}((x^2)^d - 1)^{\mu(3/d)}\prod_{d|2}(x^d - 1)^{\mu(2/d)} \\
&= \Phi_3(x^2)\Phi_2(x) \\
&= RHS
\end{aligned}$$

Lemma 2.6 *For a natural number $n \in \mathbb{N}$,let $\Phi_n(x)$ be the n-th cyclotomic polynomial,then*

$$\Phi_{2^m}(x) = \begin{cases} Odd & if \quad x \quad for \quad even \\ Even & if \quad x \quad for \quad odd \end{cases} \tag{2.6}$$

Proof: We know that,Power of an even number is even, Power of an odd number is odd
and we have a property

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

Case:1 For x even,
If x is even then there exists k natural number such that x=2k

$$\begin{aligned}\Phi_{2^n}(2k) &= (2k)^{(2)^{(m-1)}} + 1\\ &= (2k)^{(2)^{(m-1)}} + 1\\ &= (k)^{(2)^{(m-1)}}(2)^{(2)^{(m-)}} + 1\\ &= Odd\end{aligned}$$

Case:2 For x odd,
If x is odd then there exists k natural number such that x=2k+1

$$\begin{aligned}\Phi_{2^n}(2k+1) &= (2k+1)^{(2)^{(m-1)}} + 1\\ &= (2k+1)^{(2)^{(m-1)}} + 1\\ &= Even\end{aligned}$$

Hence, the lemma □

Example 2.8

$$\Phi_{2^3}(3) = \Phi_8(3) = 82 \quad and \quad \Phi_{2^3}(2) = \Phi_8(2) = 17$$

3. Useful Table Values

:

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1

n	11	12	13	14	15	16	17	18	19	20
$\mu(n)$	−1	0	−1	1	1	0	−1	0	−1	0

n	21	22	23	24	25	26	27	28	29	30
$\mu(n)$	1	1	−1	0	0	1	0	0	−1	−1

n	31	32	33	34	35	36	37	38	39	40
$\mu(n)$	−1	0	1	1	1	0	−1	1	1	0

n	41	42	43	44	45	46	47	48	49	50
$\mu(n)$	−1	−1	−1	0	0	1	−1	0	0	0

Figure 1: The values of $\mu(n)$ upto 50

x / $\varphi_n(x)$	1	2	3	4	5	6	7	8	9	10
$\varphi_1(x)$	0	1	2	3	4	5	6	7	8	9
$\varphi_2(x)$	2	3	4	5	6	7	8	9	10	11
$\varphi_3(x)$	3	7	13	21	31	43	57	73	91	111
$\varphi_4(x)$	2	5	10	17	26	37	50	65	82	101
$\varphi_5(x)$	5	31	121	341	781	1555	2801	4681	7381	11111
$\varphi_6(x)$	1	3	7	13	21	31	43	57	73	91
$\varphi_7(x)$	7	127	1093	5461	19531	55987	137257	299593	597871	1111111
$\varphi_8(x)$	2	17	82	257	626	1297	2402	4097	6562	10001
$\varphi_9(x)$	3	73	757	4161	15751	46873	117993	262657	532171	1001001
$\varphi_{10}(x)$	1	11	61	205	521	1111	2101	3641	5905	9091
$\varphi_{11}(x)$	11	2047	88573	1398101	12207031	72559411	329554457	1227133513	3922632451	11111111111
$\varphi_{12}(x)$	1	13	73	241	601	1261	2353	4033	6481	9091
$\varphi_{13}(x)$	13	8191	797161	22369621	305175781	2612138803	16148168401	78536544841	317733228541	1111111111111
$\varphi_{14}(x)$	1	43	547	3277	13021	399991	102943	233017	478297	909091
$\varphi_{15}(x)$	1	151	4561	49981	315121	1406371	4956001	14709241	38316961	90090991
$\varphi_{16}(x)$	2	257	6562	65537	390626	1679617	5764802	16777217	43046722	100000001

Figure 2: The values of $\Phi_n(x)$ upto 16

Acknowledgments

The author would like to sincerely thank the referee for the very helpful comments that improved the article. The author declares that there is no conflict of interest with respect to the publication of this article.

References

1. Brookfield,G, *The Coefficients of Cyclotomic Polynomials*. Mathematics Magazine, 89(3), 179–188,2016
2. Freed-Brown, J., Holden, M., Orrison, M.E., *Cyclotomic Polynomials, Symmetric Polynomials, and a Generalization of Eulers Totient Function*. Mathematics Magazine, 85, 44-50,2012
3. Dresden, G. P., *On the Middle Coefficient of a Cyclotomic Polynomial*. The American Mathematical Monthly, 111(6), 531–533,2004
4. D. Caragea, V. Ene., *Problem 10802*. Amer. Math. Monthly, 107 , 462–462,(2000)
5. P. A. Damianou., *On prime values of cyclotomic polynomials*. arXiv:1101.1152
6. Y. Gallot., *Cyclotomic polynomials and Prime Numbers*.
7. https://mileti.math.grinnell.edu Evens Odds Sets.

Enagandula Prasad,
Mathematics Division,
VIT Bhopal University,
Kothrikalan, Sehore, Madhya Pradesh,
India-466114
orcid id:https://orcid.org/0000-0002-3918-1131
E-mail address: eprasadsai@gmail.com