# Cyclotomic Polynomials

*A Complete Treatment*

# 1 Preliminaries

**Definition 1.1 (Primitive Root of Unity).** Let $n \geq 1$ be a positive integer. A complex number $\zeta$ is a *primitive $n$-th root of unity* if $\zeta^n = 1$ and $\zeta^k \neq 1$ for all $1 \leq k < n$. Equivalently, $\zeta$ is primitive if and only if $\operatorname{ord}(\zeta) = n$ in the multiplicative group $\mathbb{C}^\times$.

The $n$-th roots of unity are precisely $\zeta_n^k := e^{2\pi i k/n}$ for $k = 0, 1, \ldots, n-1$. Among these, $\zeta_n^k$ is primitive if and only if $\gcd(k, n) = 1$. The number of primitive $n$-th roots of unity is therefore $\varphi(n)$, Euler's totient function.

**Definition 1.2 (Cyclotomic Polynomial).** The *$n$-th cyclotomic polynomial* is defined as:

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

where $\zeta_n = e^{2\pi i/n}$. Equivalently, $\Phi_n(x)$ is the minimal polynomial over $\mathbb{Q}$ of any primitive $n$-th root of unity.

By construction, $\Phi_n(x)$ is a monic polynomial of degree $\varphi(n)$ with roots precisely the primitive $n$-th roots of unity.

**Index convention.** For a divisor $d \mid n$, each $n$-th root of unity $\zeta_n^k$ is a primitive $d$-th root of unity for exactly one $d$, namely $d = n/\gcd(k, n)$. This partitions the roots of $x^n - 1$ by their primitive order.

---

# 2 The Fundamental Factorisation

**Theorem 2.1 (Divisor Product Identity).** For all positive integers $n$:

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

*Proof.* Both sides are monic polynomials of degree $n$. The left side has roots $\{\zeta_n^k : 0 \leq k \leq n-1\}$. Each such root $\zeta_n^k$ has multiplicative order $d := n/\gcd(k, n)$, which divides $n$. Thus $\zeta_n^k$ is a primitive $d$-th root of unity and hence a root of $\Phi_d(x)$.

Conversely, every primitive $d$-th root of unity (for $d \mid n$) satisfies $\zeta^d = 1$, hence $\zeta^n = (\zeta^d)^{n/d} = 1$, so it is an $n$-th root of unity.

This establishes a bijection between the roots of $x^n - 1$ and the union $\bigcup_{d \mid n}\{\text{roots of } \Phi_d(x)\}$. Since the $\Phi_d(x)$ have pairwise disjoint root sets (a primitive $d$-th root has order exactly $d$), and since

$$\sum_{d|n} \deg \Phi_d(x) = \sum_{d|n} \varphi(d) = n,$$

the factorisation follows from unique factorisation in $\mathbb{C}[x]$. ∎

**Corollary 2.2.** The cyclotomic polynomial admits the recursive formula:

$$\Phi_n(x) = \frac{x^n - 1}{\displaystyle\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

## 3 Integrality of Coefficients

**Lemma 3.1 (Monic Division in $\mathbb{Z}[x]$).** Let $f(x), g(x) \in \mathbb{Z}[x]$ with $g(x)$ monic. If $g(x) \mid f(x)$ in $\mathbb{Q}[x]$, then $g(x) \mid f(x)$ in $\mathbb{Z}[x]$; that is, $f(x)/g(x) \in \mathbb{Z}[x]$.

*Proof.* By the division algorithm in $\mathbb{Q}[x]$, write $f(x) = g(x)q(x) + r(x)$ where $q(x), r(x) \in \mathbb{Q}[x]$ and $\deg r < \deg g$. Since $g \mid f$ in $\mathbb{Q}[x]$, we have $r(x) = 0$, so $f(x) = g(x)q(x)$.

We claim $q(x) \in \mathbb{Z}[x]$. Suppose not; let $q(x) = \sum_{i=0}^{m} q_i x^i$ with some $q_i \notin \mathbb{Z}$. Write $q_i = a_i/b_i$ in lowest terms. Let $p$ be a prime dividing some denominator $b_j$, and let $j$ be maximal such that $p \mid b_j$.

Consider the coefficient of $x^{j+\deg g}$ in $f(x) = g(x)q(x)$. Since $g$ is monic of degree $d := \deg g$, this coefficient is:

$$q_j + \sum_{i>j} g_{d-(i-j)} q_i$$

where we set $g_k = 0$ for $k < 0$. By maximality of $j$, each $q_i$ with $i > j$ has denominator coprime to $p$, and $g_{d-(i-j)} \in \mathbb{Z}$. Thus the sum $\sum_{i>j} g_{d-(i-j)} q_i$ has denominator coprime to $p$. But $q_j$ has $p$ in its denominator, so the total cannot be an integer, contradicting $f \in \mathbb{Z}[x]$. ∎

**Theorem 3.2 (Integrality).** For all $n \geq 1$, $\Phi_n(x) \in \mathbb{Z}[x]$.

*Proof.* We proceed by strong induction on $n$.

*Base case.* $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$.

*Inductive step.* Assume $\Phi_d(x) \in \mathbb{Z}[x]$ for all $d < n$. Define:

$$D_n(x) := \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$$

By the inductive hypothesis, each factor lies in $\mathbb{Z}[x]$, hence $D_n(x) \in \mathbb{Z}[x]$. Moreover, $D_n(x)$ is monic (being a product of monic polynomials).

By Corollary 2.2:

$$\Phi_n(x) = \frac{x^n - 1}{D_n(x)}$$

Both $x^n - 1 \in \mathbb{Z}[x]$ and $D_n(x) \in \mathbb{Z}[x]$ is monic. By Theorem 2.1, this division is exact in $\mathbb{C}[x]$. Since $\mathbb{Q}[x] \subseteq \mathbb{C}[x]$, polynomial division of $x^n - 1$ by $D_n(x)$ in $\mathbb{Q}[x]$ yields zero remainder, so the quotient lies in $\mathbb{Q}[x]$. By Lemma 3.1, $\Phi_n(x) \in \mathbb{Z}[x]$. ∎

---

## 4 The Möbius Inversion Formula

The divisor product identity admits an explicit inversion via the Möbius function.

**Definition 4.1 (Möbius Function).** The *Möbius function* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined by:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ for distinct primes } p_i \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \end{cases}$$

The fundamental property is:

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

**Theorem 4.2 (Möbius Inversion for Cyclotomic Polynomials).** For all $n \geq 1$:

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

*Proof.* Taking formal logarithms of the divisor product identity (Theorem 2.1):

$$\log(x^n - 1) = \sum_{d \mid n} \log \Phi_d(x)$$

Define $f(n) := \log \Phi_n(x)$ and $g(n) := \log(x^n - 1)$. The identity states $g(n) = \sum_{d \mid n} f(d)$. By Möbius inversion on the divisor poset:

$$f(n) = \sum_{d \mid n} \mu(n/d) \, g(d) = \sum_{d \mid n} \mu(n/d) \log(x^d - 1)$$

Exponentiating:

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

The substitution $d \mapsto n/d$ yields the equivalent form $\prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$.

Although the right-hand side is a priori in $\mathbb{Q}(x)$, it equals $\Phi_n(x)$ by inversion of Theorem 2.1, hence lies in $\mathbb{Z}[x]$ by Theorem 3.2. ∎

**Remark 4.3 (Validity of the formal argument).** The logarithmic manipulation is justified in the ring of formal power series $\mathbb{Q}[[x^{-1}]]$. Writing $x^n - 1 = x^n(1 - x^{-n})$, the expression $\log(1 - x^{-n}) = -\sum_{k \geq 1} x^{-nk}/k$ is a well-defined element of $\mathbb{Q}[[x^{-1}]]$. The identity holds in this ring, and the resulting polynomial identity can be verified by observing that both sides are polynomials (by Theorem 3.2) agreeing as formal Laurent series.

---

## 5 Explicit Formulae for Special Cases

**Proposition 5.1 (Prime Index).** For prime $p$:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 = \sum_{k=0}^{p-1} x^k$$

*Proof.* The divisors of $p$ are 1 and $p$. Thus $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x)$. ∎

**Proposition 5.2 (Prime Power Index).** For prime $p$ and $k \geq 1$:

$$\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = \sum_{j=0}^{p-1} x^{j \cdot p^{k-1}}$$

In particular, $\deg \Phi_{p^k} = \varphi(p^k) = p^{k-1}(p-1)$.

*Proof.* The divisors of $p^k$ are $1, p, p^2, \ldots, p^k$. Among these, $\mu(p^j) \neq 0$ only for $j \in \{0, 1\}$, with $\mu(1) = 1$ and $\mu(p) = -1$. By Theorem 4.2:

$$\Phi_{p^k}(x) = \frac{(x^{p^k} - 1)^{\mu(1)}}{(x^{p^{k-1}} - 1)^{-\mu(p)}} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}$$

The substitution $y = x^{p^{k-1}}$ gives:

$$\Phi_{p^k}(x) = \frac{y^p - 1}{y - 1} = \Phi_p(y) = \Phi_p(x^{p^{k-1}}) \qquad ∎$$

**Proposition 5.3 (Product of Two Distinct Primes).** For distinct primes $p < q$:

$$\Phi_{pq}(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}$$

*Proof.* The divisors of $pq$ are $\{1, p, q, pq\}$ with Möbius values $\mu(1) = 1$, $\mu(p) = \mu(q) = -1$, $\mu(pq) = 1$. The formula follows from Theorem 4.2. ∎

**Proposition 5.4 (The Case $2p$ for Odd Prime $p$).** For odd prime $p$:

$$\Phi_{2p}(x) = \Phi_p(-x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1 = \sum_{k=0}^{p-1} (-1)^{p-1-k} x^k$$

*Proof.* By Proposition 5.3 with the pair $(2, p)$:

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

Observe that $x^{2p} - 1 = (x^p)^2 - 1 = (x^p - 1)(x^p + 1)$. Thus:

$$\Phi_{2p}(x) = \frac{x^p + 1}{x + 1}$$

Now $\Phi_p(-x) = ((-x)^p - 1)/((-x) - 1) = (-x^p - 1)/(-x - 1) = (x^p + 1)/(x + 1)$, using that $p$ is odd. ∎

---

## 6   Reduction Formulae

**Theorem 6.1 (Reduction Formulae).** Let $n > 1$ and let $p$ be a prime dividing $n$. Write $n = p^a m$ where $\gcd(p, m) = 1$.

(i) If $a = 1$ (so $n = pm$):

$$\Phi_{pm}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)}$$

(ii) If $a \geq 2$ (so $p^2 \mid n$):

$$\Phi_n(x) = \Phi_{n/p}(x^p)$$

*Proof of (i).* The divisors of $pm$ partition as $\{d : d \mid m\} \cup \{pd : d \mid m\}$. By Theorem 4.2:

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

Splitting by whether $p$ divides the divisor:

$$= \prod_{d|m}(x^d - 1)^{\mu(pm/d)} \cdot \prod_{d|m}(x^{pd} - 1)^{\mu(m/d)}$$

Since $\gcd(p, m) = 1$, for $d \mid m$ we have $\mu(pm/d) = \mu(p)\mu(m/d) = -\mu(m/d)$. Thus:

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

where the final identification uses Theorem 4.2 applied to $m$. ∎

*Proof of (ii).* Write $n = p^a m$ with $a \geq 2$ and $\gcd(p, m) = 1$. By Theorem 4.2:

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

For $\mu(n/d) \neq 0$, we require $n/d$ to be squarefree. If $p \nmid d$, then $p^2 \mid (n/d)$, so $n/d$ is not squarefree, hence $\mu(n/d) = 0$. Thus only divisors $d$ with $p \mid d$ contribute.

Writing $d = pe$ for $e \mid (n/p)$, and noting that $n/d = n/(pe) = (n/p)/e$:

$$\Phi_n(x) = \prod_{e|(n/p)}(x^{pe} - 1)^{\mu((n/p)/e)} = \prod_{e|(n/p)}((x^p)^e - 1)^{\mu((n/p)/e)}$$

The final product is precisely $\Phi_{n/p}(x^p)$ by Theorem 4.2 applied to $n/p$. ∎

## 7 The General Closed Form

**Theorem 7.1 (Canonical Form).** Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorisation of $n > 1$. Define the *radical* $\mathrm{rad}(n) := p_1 p_2 \cdots p_r$. Then:

$$\Phi_n(x) = \Phi_{\mathrm{rad}(n)}\left(x^{n/\mathrm{rad}(n)}\right)$$

For the squarefree case $n = p_1 p_2 \cdots p_r$:

$$\Phi_n(x) = \prod_{S \subseteq \{1,\ldots,r\}}\left(x^{n/\prod_{i \in S} p_i} - 1\right)^{(-1)^{|S|}}$$

Equivalently:

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

*Proof.* For the first identity, apply Theorem 6.1(ii) repeatedly for each prime $p$ with exponent $a \geq 2$ in $n$, reducing the exponent by one at each step until all exponents equal one, yielding $\mathrm{rad}(n)$.

For the squarefree expansion, note that $\mu(d) \neq 0$ precisely when $d$ is squarefree. For $n$ squarefree with $r$ prime factors, the divisors $d \mid n$ biject with subsets $S \subseteq \{1, \ldots, r\}$ via $d = \prod_{i \in S} p_i$. Then $\mu(d) = (-1)^{|S|}$ and $n/d = \prod_{i \notin S} p_i$. ∎

---

## 8  Application: Explicit Computation of $\Phi_{12}(x)$

Setting $n = 12 = 2^2 \cdot 3$, we have $\mathrm{rad}(12) = 6$ and $12/\mathrm{rad}(12) = 2$.

**Step 1.** Compute $\Phi_6(x)$. Since $6 = 2 \cdot 3$, by Proposition 5.3:

$$\Phi_6(x) = \frac{(x^6 - 1)(x - 1)}{(x^2 - 1)(x^3 - 1)}$$

Factoring: $x^6 - 1 = (x^3 - 1)(x^3 + 1)$ and $x^2 - 1 = (x - 1)(x + 1)$. Thus:

$$\Phi_6(x) = \frac{(x^3 - 1)(x^3 + 1)(x - 1)}{(x - 1)(x + 1)(x^3 - 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

**Step 2.** Apply Theorem 7.1:

$$\Phi_{12}(x) = \Phi_6(x^2) = (x^2)^2 - (x^2) + 1 = x^4 - x^2 + 1$$

**Verification.** The degree is $\varphi(12) = \varphi(4)\varphi(3) = 2 \cdot 2 = 4$. ✓

The roots are $e^{2\pi i k/12}$ for $\gcd(k, 12) = 1$, i.e., $k \in \{1, 5, 7, 11\}$. ✓

---

## 9  Table of Cyclotomic Polynomials

| $n$ | $\Phi_n(x)$ | $\deg \Phi_n = \varphi(n)$ |
|---|---|---|
| 1 | $x - 1$ | 1 |

| $n$ | $\Phi_n(x)$ | $\deg \Phi_n = \varphi(n)$ |
|---|---|---|
| 2 | $x + 1$ | 1 |
| 3 | $x^2 + x + 1$ | 2 |
| 4 | $x^2 + 1$ | 2 |
| 5 | $x^4 + x^3 + x^2 + x + 1$ | 4 |
| 6 | $x^2 - x + 1$ | 2 |
| 7 | $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ | 6 |
| 8 | $x^4 + 1$ | 4 |
| 9 | $x^6 + x^3 + 1$ | 6 |
| 10 | $x^4 - x^3 + x^2 - x + 1$ | 4 |
| 12 | $x^4 - x^2 + 1$ | 4 |
| 15 | $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ | 8 |

## 10  Values at Special Points

**Lemma 10.0.** For all odd $m > 1$:

$$\Phi_{2m}(x) = \Phi_m(-x)$$

*Proof.* By Theorem 6.1(i) with $p = 2$ and $\gcd(2, m) = 1$:

$$\Phi_{2m}(x) = \frac{\Phi_m(x^2)}{\Phi_m(x)}$$

We show this equals $\Phi_m(-x)$. By Theorem 4.2:

$$\frac{\Phi_m(x^2)}{\Phi_m(x)} = \prod_{d|m} \frac{(x^{2d} - 1)^{\mu(m/d)}}{(x^d - 1)^{\mu(m/d)}} = \prod_{d|m} \left(\frac{x^{2d} - 1}{x^d - 1}\right)^{\mu(m/d)} = \prod_{d|m}(x^d + 1)^{\mu(m/d)}$$

For the right-hand side, since $m$ is odd, every divisor $d \mid m$ is odd, so $(-x)^d = -x^d$. Thus:

$$\Phi_m(-x) = \prod_{d|m}((-x)^d - 1)^{\mu(m/d)} = \prod_{d|m}(-x^d - 1)^{\mu(m/d)} = \prod_{d|m}(-(x^d + 1))^{\mu(m/d)}$$

Since $\mu(m/d) \in \{-1, 0, 1\}$, each factor contributes either 1 or $-1$ accordingly. The total sign is $(-1)^{\sum_{d|m} \mu(m/d)} = (-1)^0 = 1$, since $\sum_{d|m} \mu(m/d) = 0$ for $m > 1$. Hence $\Phi_{2m}(x) = \Phi_m(-x)$. ∎

**Proposition 10.1.**

(i) For $n > 1$:

$$\Phi_n(1) = \begin{cases} p & \text{if } n = p^k \text{ for some prime } p \\ 1 & \text{otherwise} \end{cases}$$

(ii) For $n \geq 1$:

$$\Phi_n(-1) = \begin{cases} -2 & \text{if } n = 1 \\ 0 & \text{if } n = 2 \\ 2 & \text{if } n = 2^k \text{ for } k \geq 2 \\ p & \text{if } n = 2p^k \text{ for an odd prime } p, \ k \geq 1 \\ 1 & \text{otherwise} \end{cases}$$

*Proof of (i).* From Theorem 2.1, $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Differentiating and evaluating at $x = 1$:

$$n = \frac{d}{dx}(x^n - 1)\Big|_{x=1} = \sum_{d|n} \Phi_d'(1) \prod_{\substack{e|n \\ e \neq d}} \Phi_e(1)$$

Since $\Phi_1(1) = 0$, only the term $d = 1$ survives, yielding:

$$n = \Phi_1'(1) \cdot \prod_{\substack{d|n \\ d>1}} \Phi_d(1) = 1 \cdot \prod_{\substack{d|n \\ d>1}} \Phi_d(1)$$

Thus $\prod_{d|n,d>1} \Phi_d(1) = n$. We prove the closed form by strong induction on $n$.

For $n = p$ prime, the only divisor greater than 1 is $p$ itself, so $\Phi_p(1) = p$.

For $n = p^k$ with $k \geq 2$, the divisors greater than 1 are $p, p^2, \ldots, p^k$. By induction, $\Phi_{p^j}(1) = p$ for $j < k$. Thus:

$$\prod_{j=1}^{k} \Phi_{p^j}(1) = p^k \implies p^{k-1} \cdot \Phi_{p^k}(1) = p^k \implies \Phi_{p^k}(1) = p$$

For $n$ with at least two distinct prime factors, write $n = p^a m$ with $\gcd(p, m) = 1$ and $m > 1$. The divisors of $n$ greater than 1 include all divisors of $m$ greater than 1, all divisors of $p^a$ greater than 1, and mixed divisors. By the multiplicative structure:

$$\prod_{\substack{d|n \\ d>1}} \Phi_d(1) = n = p^a \cdot m$$

The divisors $p^j$ for $1 \leq j \leq a$ contribute $p^a$ (by induction). The divisors of $m$ greater than 1 contribute $m$ (by induction on $m$). The remaining divisors (those involving both $p$ and primes

of $m$) must therefore contribute 1. Each such $\Phi_d(1)$ is a positive integer: it lies in $\mathbb{Z}$ by Theorem 3.2, and $\Phi_d(1) > 0$ because pairing conjugate roots gives $\Phi_d(1) = \prod |1 - \zeta|^2 > 0$. Since their product is 1 and each factor is a positive integer, each equals 1. In particular, $\Phi_n(1) = 1$. ∎

*Proof of (ii).* Write $n = 2^a m$ with $m$ odd.

**Case 1: $a = 0$ ($n$ odd).** For $n = 1$, direct computation gives $\Phi_1(-1) = -2$. For odd $n > 1$, Lemma 10.0 gives $\Phi_{2n}(x) = \Phi_n(-x)$, so $\Phi_n(-1) = \Phi_{2n}(1)$. Because $n > 1$ is odd, it has an odd prime divisor $p$, so $2n$ is divisible by both 2 and $p$. Hence $2n$ is not a prime power, and $\Phi_{2n}(1) = 1$ by part (i).

**Case 2: $a = 1$ ($n = 2m$ with $m$ odd).** For $m = 1$, direct computation gives $\Phi_2(-1) = 0$. For $m > 1$, Lemma 10.0 gives $\Phi_{2m}(x) = \Phi_m(-x)$, hence $\Phi_{2m}(-1) = \Phi_m(1)$. By part (i), $\Phi_m(1) = p$ if $m = p^k$ for some odd prime $p$, and $\Phi_m(1) = 1$ otherwise. This yields $\Phi_{2p^k}(-1) = p$ for odd primes $p$, and $\Phi_{2m}(-1) = 1$ for other odd $m > 1$.

**Case 3: $a \geq 2$ ($4 \mid n$).** Apply Theorem 6.1(ii) repeatedly with $p = 2$:

$$\Phi_{2^a m}(x) = \Phi_{2m}\left(x^{2^{a-1}}\right)$$

Evaluating at $x = -1$:

$$\Phi_{2^a m}(-1) = \Phi_{2m}\left((-1)^{2^{a-1}}\right) = \Phi_{2m}(1)$$

since $2^{a-1} \geq 2$ implies $(-1)^{2^{a-1}} = 1$. If $m = 1$, this gives $\Phi_{2^a}(-1) = \Phi_2(1) = 2$. If $m > 1$, then $2m$ is not a prime power (having both 2 and an odd prime as factors), so $\Phi_{2m}(1) = 1$ by part (i), yielding $\Phi_{2^a m}(-1) = 1$. ∎

---

## 11 Generalisations

### 11.1 Cyclotomic Polynomials over Finite Fields

For a finite field $\mathbb{F}_q$ with $\gcd(q, n) = 1$, the polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ reduces to $\bar{\Phi}_n(x) \in \mathbb{F}_q[x]$. This reduced polynomial factors into irreducible factors of equal degree $d$, where $d$ is the multiplicative order of $q$ modulo $n$. The number of irreducible factors is $\varphi(n)/d$.

### 11.2 Generalised Cyclotomic Polynomials

For integers $a, b$ with $\gcd(a, b) = 1$, define:

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

This is a homogeneous polynomial in $a, b$ of degree $\varphi(n)$ with integer coefficients. The substitution $a = x, b = 1$ recovers $\Phi_n(x)$.

---

## 12 Concluding Remarks

The cyclotomic polynomial $\Phi_n(x)$ admits a closed form via Möbius inversion:

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

The integrality $\Phi_n(x) \in \mathbb{Z}[x]$ follows from strong induction using monic polynomial division. The derivation rests on three principles:

1. **Divisor partition.** The $n$-th roots of unity partition by primitive order into disjoint sets indexed by $d \mid n$.
2. **Möbius inversion.** The divisor sum $g(n) = \sum_{d|n} f(d)$ inverts to $f(n) = \sum_{d|n} \mu(n/d)g(d)$.
3. **Monic divisibility.** Division by monic polynomials preserves integrality in $\mathbb{Z}[x]$.

The reduction $\Phi_n(x) = \Phi_{\mathrm{rad}(n)}(x^{n/\mathrm{rad}(n)})$ shows that computation of $\Phi_n(x)$ reduces to the squarefree case, where the Möbius formula involves $2^r$ terms for $r$ distinct prime factors.

---

## 13   Appendix: Algorithmic Summary

To compute $\Phi_n(x)$:

1. Compute the prime factorisation $n = p_1^{a_1} \cdots p_r^{a_r}$.
2. Compute $m := \mathrm{rad}(n) = p_1 \cdots p_r$ and $e := n/m = p_1^{a_1-1} \cdots p_r^{a_r-1}$.
3. Compute $\Phi_m(x)$ via:

$$\Phi_m(x) = \prod_{S \subseteq \{1,\ldots,r\}} \left( x^{m/\prod_{i \in S} p_i} - 1 \right)^{(-1)^{|S|}}$$

4. Return $\Phi_n(x) = \Phi_m(x^e)$.

For implementation, the product in step 3 is computed iteratively: initialise $P(x) := 1$ (empty product), then for each subset $S$, multiply or divide by $x^{m/d_S} - 1$ according to the parity of $|S|$.