Cyclotomic Polynomials

A Complete Treatment

December 2025

1 Preliminaries

Definition 1.1 (Primitive Root of Unity). Let n ≥ 1 be a positive integer. A complex number ζ is a *primitive n-th root of unity* if ζ^n = 1 and ζ⊠ ≠ 1 for all 1 ≤ k < n. Equivalently, ζ is primitive if and only if ord(ζ) = n in the multiplicative group ⊠⊠.

The n-th roots of unity are precisely ζ⊠⊠ := e^{2πik/n} for k = 0, 1, …, n−1. Among these, ζ⊠⊠ is primitive if and only if gcd(k, n) = 1. The number of primitive n-th roots of unity is therefore φ(n), Euler's totient function.

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

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

where ζ⊠ = e^{2πi/n}. Equivalently, Φ⊠(x) is the minimal polynomial over ⊠ of any primitive n-th root of unity.

By construction, Φ⊠(x) is a monic polynomial of degree φ(n) with roots precisely the primitive n-th roots of unity.

Index convention. For a divisor d | n, each n-th root of unity ζ⊠⊠ 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:

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

Proof. Both sides are monic polynomials of degree n. The left side has roots {ζ⊠⊠ : 0 ≤ k ≤ n−1}. Each such root ζ⊠⊠ has multiplicative order d := n/gcd(k, n), which divides n. Thus ζ⊠⊠ is a primitive d-th root of unity and hence a root of Φ_d(x).

Conversely, every primitive d-th root of unity (for d | n) satisfies ζ⊠ = 1, hence ζ^n = (ζ⊠)^{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 ⊠_{d | n} {roots of Φ_d(x)}. Since the Φ_d(x) have pairwise disjoint root sets (a primitive d-th root has order exactly d), and since

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

the factorisation follows from unique factorisation in ⊠[x]. ⊠

Corollary 2.2. The cyclotomic polynomial admits the recursive formula:

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

---

3 Integrality of Coefficients

Lemma 3.1 (Monic Division in ⊠[x]). Let f(x), g(x) ⊠ ⊠[x] with g(x) monic. If g(x) | f(x) in ⊠[x], then g(x) | f(x) in ⊠[x]; that is, f(x)/g(x) ⊠ ⊠[x].

Proof. By the division algorithm in ⊠[x], write f(x) = g(x)q(x) + r(x) where q(x), r(x) ⊠ ⊠[x] and deg r < deg g. Since g | f in ⊠[x], we have r(x) = 0, so f(x) = g(x)q(x).

We claim q(x) ⊠ ⊠[x]. Suppose not; let q(x) = Σ_{i=0}^{m} q⊠x⊠ with some q⊠ ⊠ ⊠. Write q⊠ = a⊠/b⊠ in lowest terms. Let p be a prime dividing some denominator b⊠, and let j be maximal such that p | b⊠.

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⊠ = 0 for k < 0. By maximality of j, each q⊠ with i > j has denominator coprime to p, and g_{d−(i−j)} ⊠ ⊠. Thus the sum Σ*{i>j} g*{d−(i−j)} q⊠ has denominator coprime to p. But q⊠ has p in its denominator, so the total cannot be an integer, contradicting f ⊠ ⊠[x]. ⊠

Theorem 3.2 (Integrality). For all n ≥ 1, Φ⊠(x) ⊠ ⊠[x].

Proof. We proceed by strong induction on n.

Base case. Φ₁(x) = x − 1 ⊠ ⊠[x].

Inductive step. Assume Φ_d(x) ⊠ ⊠[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 ☒[x], hence D☒(x) ☒ ☒[x]. Moreover, D☒(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 ☒ ☒[x] and D☒(x) ☒ ☒[x] is monic. By Theorem 2.1, this division is exact in ☒[x]. Since ☒[x] ☒ ☒[x], polynomial division of x^n − 1 by D☒(x) in ☒[x] yields zero remainder, so the quotient lies in ☒[x]. By Lemma 3.1, Φ☒(x) ☒ ☒[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* μ: ☒ → {−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:

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

Theorem 4.2 (Möbius Inversion for Cyclotomic Polynomials). For all n ≥ 1:

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

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

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

Define f(n) := log Φ☒(x) and g(n) := log(x^n − 1). The identity states g(n) = Σ_{d | n} f(d). By Möbius inversion on the divisor poset:

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

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 ⊠ n/d yields the equivalent form ∏_{d | n} (x^{n/d} − 1)^{μ(d)}.

Although the right-hand side is a priori in ⊠(x), it equals Φ⊠(x) by inversion of Theorem 2.1, hence lies in ⊠[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 ⊠[[x⊠^{1}]]. Writing x^n − 1 = x^n(1 − x⊠^{n}), the expression log(1 − x⊠^{n}) = −∑_{k≥1} x⊠^{n}⊠/k is a well-defined element of ⊠[[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⊠ − 1 = Φ_1(x)Φ⊠(x) = (x−1)Φ⊠(x). ⊠

Proposition 5.2 (Prime Power Index). For prime p and k ≥ 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 Φ_{p⊠} = φ(p⊠) = p^{k−1}(p−1).

Proof. The divisors of p⊠ are 1, p, p^2, …, p⊠. Among these, μ(p⊠) ≠ 0 only for j ⊠ {0, 1}, with μ(1) = 1 and μ(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:

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

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 μ(1) = 1, μ(p) = μ(q) = −1, μ(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□)² − 1 = (x□ − 1)(x□ + 1). Thus:

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

Now Φ□(−x) = ((−x)□ − 1)/((−x) − 1) = (−x□ − 1)/(−x − 1) = (x□ + 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□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 ≥ 2 (so p² | n):

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

Proof of (i). The divisors of pm partition as {d : d | m} □ {pd : d | 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 | m we have μ(pm/d) = μ(p)μ(m/d) = −μ(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☒m with a ≥ 2 and gcd(p, m) = 1. By Theorem 4.2:

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

For μ(n/d) ≠ 0, we require n/d to be squarefree. If p ☒ d, then p² | (n/d), so n/d is not squarefree, hence μ(n/d) = 0. Thus only divisors d with p | d contribute.

Writing d = pe for e | (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 Φ_{n/p}(x^p) by Theorem 4.2 applied to n/p. ☒

---

7 The General Closed Form

Theorem 7.1 (Canonical Form). Let n = p₁^{a₁} p₂^{a₂} ☒ p☒^{a☒} be the prime factorisation of n > 1. Define the *radical* rad(n) := p₁p₂☒p☒. Then:

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

For the squarefree case n = p₁p₂☒p☒:

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

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 ≥ 2 in n, reducing the exponent by one at each step until all exponents equal one, yielding rad(n).

For the squarefree expansion, note that μ(d) ≠ 0 precisely when d is squarefree. For n squarefree with r prime factors, the divisors d | n biject with subsets S ⊠ {1, …, r} via d = ∏*{i ⊠ S} p⊠. Then μ(d) = (−1)^{|S|} and n/d = ∏*{i ⊠ S} p⊠. ⊠

---

8 Application: Explicit Computation of Φ₁₂(x)

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

Step 1. Compute Φ₆(x). Since 6 = 2 · 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 φ(12) = φ(4)φ(3) = 2 · 2 = 4. ✓

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

---

9 Table of Cyclotomic Polynomials

n	Φ⊠(x)	deg Φ⊠ = φ(n)
1	x − 1	1
2	x + 1	1

n	Φ⊠(x)	deg Φ⊠ = φ(n)
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 Φ⊠(−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 | 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 μ(m/d) ⊠ {−1, 0, 1}, each factor contributes either 1 or −1 accordingly. The total sign is (−1)^{Σ*{d | m} μ(m/d)} = (−1)^0 = 1, since Σ*{d | m} μ(m/d) = 0 for m > 1. Hence Φ_{2m}(x) = Φ⊠(−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 ≥ 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 = Π_{d | n} Φ_d(x). Differentiating and evaluating at x = 1:

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

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 Π_{d | n, d > 1} Φ_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 ≥ 2, the divisors greater than 1 are p, p^2, …, p^k. By induction, Φ_{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^am 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⌧ for 1 ≤ j ≤ a contribute p⌧ (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 Φ_d(1) is a positive integer: it lies in ⌧ by Theorem 3.2, and Φ_d(1) > 0 because pairing conjugate roots gives Φ_d(1) = ∏ |1 − ζ|² > 0. Since their product is 1 and each factor is a positive integer, each equals 1. In particular, Φ⌧(1) = 1. ⌧

Proof of (ii). Write n = 2⌧m with m odd.

Case 1: a = 0 (n odd). For n = 1, direct computation gives Φ₁(−1) = −2. For odd n > 1, Lemma 10.0 gives Φ_{2n}(x) = Φ⌧(−x), so Φ⌧(−1) = Φ_{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 Φ_{2n}(1) = 1 by part (i).

Case 2: a = 1 (n = 2m with m odd). For m = 1, direct computation gives Φ₂(−1) = 0. For m > 1, Lemma 10.0 gives Φ_{2m}(x) = Φ⌧(−x), hence Φ_{2m}(−1) = Φ⌧(1). By part (i), Φ⌧(1) = p if m = p⌧ for some odd prime p, and Φ⌧(1) = 1 otherwise. This yields Φ_{2p⌧}(−1) = p for odd primes p, and Φ_{2m}(−1) = 1 for other odd m > 1.

Case 3: a ≥ 2 (4 | n). Apply Theorem 6.1(ii) repeatedly with p = 2:

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

Evaluating at x = −1:

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

since 2^{a−1} ≥ 2 implies (−1)^{2^{a−1}} = 1. If m = 1, this gives Φ_{2⌧}(−1) = Φ₂(1) = 2. If m > 1, then 2m is not a prime power (having both 2 and an odd prime as factors), so Φ_{2m}(1) = 1 by part (i), yielding Φ_{2⌧m}(−1) = 1. ⌧

11 Generalisations

11.1 Cyclotomic Polynomials over Finite Fields

For a finite field ⌧_q with gcd(q, n) = 1, the polynomial Φ⌧(x) ⌧ ⌧[x] reduces to Φ⌧(x) ⌧ ⌧_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 φ(n)/d.

11.2 Generalised Cyclotomic Polynomials

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

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

This is a homogeneous polynomial in a, b of degree φ(n) with integer coefficients. The substitution a = x, b = 1 recovers Φ☒(x).

12 Concluding Remarks

The cyclotomic polynomial Φ☒(x) admits a closed form via Möbius inversion:

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

The integrality Φ☒(x) ☒ ☒[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 | n.
2. **Möbius inversion.** The divisor sum g(n) = Σ*{d | n} f(d) inverts to f(n)* = Σ{d | n} μ(n/d) g(d).
3. **Monic divisibility.** Division by monic polynomials preserves integrality in ☒[x].

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

13 Appendix: Algorithmic Summary

To compute Φ⌧(x):

1. Compute the prime factorisation n = p₁^{a₁} ⌧ p⌧^{a⌧}.
2. Compute m := rad(n) = p₁ ⌧ p⌧ and e := n/m = p₁^{a₁−1} ⌧ p⌧^{a⌧−1}.
3. Compute Φ⌧(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 Φ⌧(x) = Φ⌧(x⌧).

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|.