

Cyclotomic Polynomial

Timo Chang

timo65537@protonmail.com

Last edited: December 25, 2025

In this essay, we introduce the cyclotomic polynomial $\Phi_n(x)$ over \mathbb{Q} for each $n \in \mathbb{N}$ and give various computational formulas. Moreover, we prove that it is the irreducible polynomial of any primitive n -th roots of unity over \mathbb{Q} with integer coefficients.

1 Definition and Computation

Definition 1.1 (Cyclotomic Polynomial). For any $n \in \mathbb{N}$, we define the n -th cyclotomic polynomial to be

$$\Phi_n(x) := \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (x - e^{2\pi i k/n}).$$

In other words, it is the monic polynomial having exactly all primitive n -th roots of unity as its roots. We note that $\deg \Phi_n(x) = \phi(n)$ is the *Euler's phi function*.

Proposition 1.2. For any $n \in \mathbb{N}$,

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

By considering the degrees of both sides, we see that $\sum_{d|n} \phi(d) = n$, which is a well known fact from basic number theory. In fact, as we will see, the proofs behind these two identities are essentially the same. Nevertheless, the best way to understand Proposition 1.2 is to compute a not-so-trivial example rather than giving a rigorous proof. The general argument can be done by exactly the same idea, which is left as an exercise.

Example 1.3. Let's take $n = 6$ as an example. Then we want to check that

$$\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = x^6 - 1. \tag{1}$$

We first consider the right-hand side. Put $\zeta_6 := e^{2\pi i/6}$. Then the roots of $x^6 - 1$ are precisely all sixth roots of unity:

$$\{\zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5, \zeta_6^6 = 1\} = \{e^{2\pi i/6}, e^{4\pi i/6}, e^{6\pi i/6}, e^{8\pi i/6}, e^{10\pi i/6}, e^{12\pi i/6} = 1\}.$$

On the other hand, by Definition 1.1, we see that the left hand side are

$$\begin{aligned}\Phi_1(x) &= (x - e^{2\pi i}), \\ \Phi_2(x) &= (x - e^{2\pi i/2}), \\ \Phi_3(x) &= (x - e^{2\pi i/3})(x - e^{4\pi i/3}), \\ \Phi_6(x) &= (x - e^{2\pi i/6})(x - e^{10\pi i/6}).\end{aligned}$$

Notice that both sides of (1) are monic and have exactly the same roots. So they must be identical.

The key observation in the proof of Proposition 1.2 is the following: Any n -th roots of unity is a primitive d -th roots of unity for some unique $d \mid n$. And conversely, any primitive d -th roots of unity where $d \mid n$ must be an n -th roots of unity. (For example, $e^{4\pi i/6} = e^{2\pi i/3}$ is a sixth roots of unity, which is also a primitive third roots of unity.)

In this manner, one shows that both sides of the equation to be proved have exactly the same roots. Since they are both monic, the equation follows. We further mention that what we are really concerning is the “fractions” on the exponents. And this idea is highly similar to one of the common proof of the identity $\sum_{d \mid n} \phi(d) = n$.

Proposition 1.4. $\Phi_n(x)$ is a monic polynomial with integer coefficients for all $n \in \mathbb{N}$.

Proof. We proceed by induction on n . The base case is trivial. So suppose the statement holds for any $k = 1, \dots, n - 1$. From Proposition 1.2 we know

$$\prod_{d \mid n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) = x^n - 1.$$

So

$$\Phi_n(x) = x^n - 1 \bigg/ \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x). \quad (2)$$

By induction hypothesis, all terms in the product are monic with integer coefficients, thus so is the denominator. This implies that $\Phi_n(x) \in \mathbb{Z}[x]$ by long division algorithm. \square

Example 1.5. Note that (2) provides a method to compute $\Phi_n(x)$. As an example, let us find $\Phi_8(x)$. Then we have

$$\Phi_8(x) = \frac{x^8 - 1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)}.$$

And by Definition 1.1, we see that

$$\begin{aligned}\Phi_1(x) &= x - e^{2\pi i} = x - 1, \\ \Phi_2(x) &= x - e^{2\pi i/2} = x + 1, \\ \Phi_4(x) &= (x - e^{2\pi i/4})(x - e^{6\pi i/4}) = (x - i)(x + i) = x^2 + 1.\end{aligned}$$

So

$$\Phi_8(x) = \frac{x^8 - 1}{(x-1)(x+1)(x^2+1)} = x^4 + 1.$$

Note that in order to compute $\Phi_n(x)$ using (2), it is required to find $\Phi_d(x)$ first for all proper divisors d of n . This sounds quite indirect and inefficient. So below, we give another formula of $\Phi_n(x)$ which resolves this problem, i.e., the one which involves no prior knowledge of $\Phi_d(x)$ (Proposition 1.8).

Definition 1.6 (Möbius Function). For any $n \in \mathbb{N}$, we define the *Möbius function* $\mu(n)$ to be

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^r, & \text{if } n = p_1 \cdots p_r \text{ where } p_i \text{ are distinct primes,} \\ 0, & \text{otherwise.} \end{cases}$$

The Möbius function is ubiquitous in number theory and possesses lots of nice properties. The one we are going to use is the following:

Lemma 1.7. For any $n \in \mathbb{N}$,

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

Proof. The case $n = 1$ is trivial, so let us consider $n > 1$. We write $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ into prime factorization where each $\alpha_i \geq 1$ and p_i, p_j are all distinct. Then every divisor d of n is of the form $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$ where $0 \leq \beta_i \leq \alpha_i$ for all i . Note that from Definition 1.6, we only need to consider when $\beta_i = 0, 1$ for all i , because otherwise, $\mu(d) = 0$. Grouping these divisors of n by the number of their prime divisors, we see that

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_i \mu(p_i) + \sum_{i \neq j} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ &= (1 + (-1))^r \\ &= 0. \end{aligned}$$

□

Proposition 1.8. For all $n \in \mathbb{N}$,

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

Proof. With Lemma 1.7 in hand, this formula is now fairly easy and immediate. One sees that

$$\begin{aligned}
\prod_{d|n} (x^d - 1)^{\mu(n/d)} &= \prod_{d|n} \left(\prod_{k|d} \Phi_k(x) \right)^{\mu(n/d)} && \text{(by Proposition 1.2)} \\
&= \prod_{d|n} \prod_{k|d} \Phi_k(x)^{\mu(n/d)} \\
&= \prod_{k|n} \Phi_k(x)^{\sum_{d'| \frac{n}{k}} \mu(d')} \\
&= \Phi_n(x) && \text{(by Lemma 1.7).}
\end{aligned}$$

The only thing that needs to be explained more is perhaps the third equality. Roughly speaking, what we are doing in there is to collect all $\Phi_k(x)$ in that double product for each fixed divisor k of n . Precisely, one observes that for each such k , we have

$$\left\{ \frac{n}{d} : d | n \text{ and } k | d \right\} = \left\{ d' : d' | \frac{n}{k} \right\}.$$

(If this is still not clear for you, consider an explicit example: $n = 60$ and $k = 6$ is probably good enough.) \square

We mention that in the above proof, we were simply applying the *Möbius inversion formula*.

Example 1.9. Let us use Proposition 1.8 to compute a slightly larger example: $\Phi_{18}(x)$. Note that the divisors of 18 are $d = 1, 2, 3, 6, 9, 18$, which correspond to

$$\begin{array}{c|c|c|c|c|c}
\mu(18/1) & \mu(18/2) & \mu(18/3) & \mu(18/6) & \mu(18/9) & \mu(18/18) \\
\hline
0 & 0 & 1 & -1 & -1 & 1
\end{array}.$$

So by Proposition 1.8, we have

$$\Phi_{18}(x) = \frac{(x^3 - 1)(x^{18} - 1)}{(x^6 - 1)(x^9 - 1)} = x^6 - x^3 + 1.$$

See how nice this formula is? When n/d is not square-free, we can simply ignore it!

Remark 1.10. Using the same method, it is also very easy to compute (?) that

$$\begin{aligned}
\Phi_{105}(x) &= x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} \\
&\quad + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} \\
&\quad + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.
\end{aligned}$$

What's interesting about the number 105 is the fact that it is the smallest positive integer whose corresponding cyclotomic polynomial has coefficients other than $0, 1, -1$ ¹. (In case you didn't see it, there are -2 in the x^{41} and x^7 -terms.) Let's call this property \mathcal{P} . So the follow-up questions are perhaps:

- What causes 105 having property \mathcal{P} (if there is a reason)?
- What about the other numbers? Can we classify all numbers satisfying \mathcal{P} ?
- Are there any deeper reasons or more advanced theory that are related to \mathcal{P} ?

2 The Irreducibility

Proposition 2.1. $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ for all $n \in \mathbb{N}$.

Proof. By Gauss lemma, it's sufficient to show that $\Phi(x) := \Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Suppose $\Phi(x) = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Z}[x]$. Since $\zeta_n := e^{2\pi i/n}$ is a root of $\Phi(x)$, we have either $f(\zeta_n) = 0$ or $g(\zeta_n) = 0$. We say without loss of generality that $f(\zeta_n) = 0$. Moreover, we may also assume $f(x)$ is irreducible in $\mathbb{Z}[x]$. This implies that $f(x)$ is the irreducible polynomial $\text{Irr}_{\mathbb{Q}}(\zeta_n)$ of ζ_n over \mathbb{Q} . Our goal is to show that $f(x) = \Phi(x)$. And since we already have $f(x) \mid \Phi(x)$, it's enough to show that

$$\Phi(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (x - \zeta_n^k) \mid f(x).$$

That is, we want to show that $f(\zeta_n^k) = 0$ for all $1 \leq k \leq n$ with $\gcd(k, n) = 1$.

First, we consider when $k = p$ is a prime and claim that $f(\zeta_n^p) = 0$. In fact, we will claim a slightly more general result that if $f(\zeta) = 0$ where ζ is any primitive n -th roots of unity, then $f(\zeta^p) = 0$ for all prime p with $p \nmid n$.

Since ζ^p is again a primitive n -th roots of unity, it is also a root of $\Phi(x)$. Thus, we have $0 = \Phi(\zeta^p) = f(\zeta^p)g(\zeta^p)$. If $f(\zeta^p) = 0$, we are done. So suppose on the other hand that $g(\zeta^p) = 0$. We prove that this will lead to a contradiction.

Let $h(x) := g(x^p) \in \mathbb{Z}[x]$. Note that $h(\zeta) = g(\zeta^p) = 0$. On the other hand, recall that we assumed $f(\zeta) = 0$ in the claim and $f(x)$ is irreducible at the beginning. This implies that $f(x) = \text{Irr}_{\mathbb{Q}}(\zeta)$ and so $f(x) \mid h(x)$. We then write $h(x) = g(x^p) = f(x)a(x)$ for some $a(x) \in \mathbb{Z}[x]$. By considering the coefficients modulo p , we have

$$\bar{h}(x) = \bar{g}(x^p) = \bar{g}(x)^p = \bar{f}(x) \cdot \bar{a}(x) \in (\mathbb{Z}/p\mathbb{Z})[x].$$

¹The On-Line Encyclopedia of Integer Sequences (OEIS): smallest order of cyclotomic polynomial containing n or $-n$ as a coefficient

Note that if $\bar{f}(x)$ and $\bar{g}(x)$ are relatively prime, then so are $\bar{f}(x)$ and $\bar{g}(x)^p$, which is absurd. So we know $\bar{f}(x)$ and $\bar{g}(x)$ have a common factor in $(\mathbb{Z}/p\mathbb{Z})[x]$, say $\bar{d}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ where $\deg \bar{d}(x) \geq 1$. Now, by Propositions 1.2 and 1.4 (see (2) also),

$$f(x)g(x) = \Phi(x) \mid x^n - 1$$

in $\mathbb{Z}[x]$. This implies

$$\bar{d}(x)^2 \mid \bar{f}(x)\bar{g}(x) = \bar{\Phi}(x) \mid x^n - \bar{1}$$

in $(\mathbb{Z}/p\mathbb{Z})[x]$. So we may write $x^n - \bar{1} = \bar{d}(x)^2 \cdot \bar{b}(x)$ for some $\bar{b}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. By differentiating both sides, we have

$$\bar{n}x^{n-1} = 2\bar{d}(x)\bar{d}'(x) \cdot \bar{b}(x) + \bar{d}(x)^2 \cdot \bar{b}'(x),$$

which is non-zero (as $p \nmid n$) and divisible by $\bar{d}(x)$. But this is a contradiction because $\bar{d}(x) \mid x^n - \bar{1}$.

We have shown that if $f(\zeta) = 0$ where ζ is a primitive n -th roots of unity, then $f(\zeta^p) = 0$ for all prime p with $p \nmid n$. We now use this to prove our desired result. Let $1 \leq k \leq n$ with $\gcd(k, n) = 1$. We write $k = p_1 \cdots p_r$ into product of prime numbers (not necessarily distinct). Note that $p_i \nmid n$ for all $i = 1, \dots, r$. Recall that $f(\zeta_n) = 0$ where $\zeta_n = e^{2\pi i/n}$ is a primitive n -th roots of unity and $p_1 \nmid n$, so by our claim, we have $f(\zeta_n^{p_1}) = 0$. Next, since $\zeta_n^{p_1}$ is also a primitive n -th roots of unity and $p_2 \nmid n$, by our claim again, we have $f(\zeta_n^{p_1 p_2}) = 0$. Repeating this argument, we see that

$$0 = f(\zeta_n) = f(\zeta_n^{p_1}) = f(\zeta_n^{p_1 p_2}) = \dots = f(\zeta_n^{p_1 \cdots p_r}) = f(\zeta_n^k).$$

And this is exactly what we want. □

Remark 2.2. We have also shown that $\text{Irr}_{\mathbb{Q}}(\zeta_n) = \Phi_n(x)$ for any primitive n -th roots of unity ζ_n . So the degree of the field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (the n -th cyclotomic extension) is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n)$.

Remark 2.3. Let A be a polynomial ring over a finite field and k be its field of fractions. We think of A and k as the analogs of \mathbb{Z} and \mathbb{Q} , respectively. Then there is the analogous notion of *Carlitz cyclotomic polynomials* over k . And everything we have seen in this essay (and more) has a parallel statement under this setting. In fact, their proofs are essentially the same. A good reference to this topic is [Pap23, Chapter 7.1].

References

- [Pap23] Mihran Papikian. *Drinfeld modules*. Vol. 296. Grad. Texts in Math. Springer Nature Switzerland AG, 2023.