Elementary Properties of Cyclotomic Polynomials

Yimin Ge

Abstract

Elementary properties of cyclotomic polynomials is a topic that has become very popular in Olympiad mathematics. The purpose of this article is to give an introduction into the theory of cyclotomic polynomials and present some classical examples.

1 Prerequisites

Definition 1. The Möbius Function $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is squarefree and } k \text{ is the number of prime divisors of } n \\ 0 & \text{else.} \end{cases}$$

Clearly, μ is multiplicative, that is, $\mu(mn) = \mu(m)\mu(n)$ for all coprime positive integers m and n. The following result can be found in many books on multiplicative functions.

Theorem 1. (Möbius Inversion Formula) Suppose that $F, H, f : \mathbb{Z}^+ \to \mathbb{Z}^+$ are functions such that

$$F(n) = \sum_{d|n} f(d), \quad H(n) = \prod_{d|n} f(d).$$

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)}.$$

Definition 2. Let n be a positive integer and ζ be an nth root of unity. Then the least positive integer k that satisfies $\zeta^k = 1$ is called the *order* of ζ and is denoted by $\operatorname{ord}(\zeta)$. Also ζ is called a *primitive nth root of unity* if $\operatorname{ord}(\zeta) = n$.

Lemma 1. Let n and k be positive integers and ζ be a primitive nth root of unity. Then ζ^k is a primitive nth root of unity if and only if $\gcd(k, n) = 1$.

Proof. Let $d = \mathrm{ord}(\zeta^k)$, then $\zeta^{kd} = 1$ and $n \mid kd$. If $\gcd(k, n) = 1$, then $n \mid kd$ implies $n \mid d$. But d also divides n, so $d = n$ and ζ^k is primitive.

If $\gcd(k, n) \neq 1$, then

$$\zeta^{k \frac{n}{\gcd(k,n)}} = 1,$$

so $d < n$. Thus ζ^k is not primitive. □

Corollary 1. Let n be a positive integer. Then there exist exactly $\varphi(n)$ primitive nth roots of unity.

2 Cyclotomic Polynomials

2.1 Definition and Elementary Properties

Definition 3. Let n be a positive integer. Then the *nth cyclotomic polynomial*, denoted as Φ_n, is the (monic) polynomial having exactly the primitive nth root of unity as roots, that is,

$$\Phi_n(X) \equiv \prod_{\substack{\zeta^n=1 \\ \mathrm{ord}(\zeta)=n}} (X - \zeta).$$

Since there are exactly $\varphi(n)$ primitive nth roots of unity, the degree of Φ_n is $\varphi(n)$. Further we present some elementary properties of cyclotomic polynomials which can be very useful at various competitions.

Theorem 2. Let n be a positive integer. Then

$$X^n - 1 \equiv \prod_{d \mid n} \Phi_d(X).$$

Proof. The roots of $X^n - 1$ are exactly the nth roots of unity. On the other hand, if ζ is an nth root of unity and $d = \mathrm{ord}(\zeta)$, then ζ is a primitive dth root of unity and thus a root of $\Phi_d(X)$. But $d \mid n$, so ζ is a root of the right hand side. It follows that the polynomials on the left and right hand side have the same roots and since they are both monic, they are equal. □

Notice that comparing degrees of the polynomials yields another proof of

$$n = \sum_{d \mid n} \varphi(d).$$

Lemma 2. Suppose that $f(X) \equiv X^m + a_{m-1}X^{m-1} + \ldots + a_0$ and $g(X) \equiv X^n + b_{n-1}X^{n-1} + \ldots + b_0$ are polynomials with rational coefficients. If all coefficients of the polynomial $f \cdot g$ are integers, then so are the coefficients of f and g.

Proof. Let M and N respectively be the least positive integers so that all coefficients of $Mf(X)$ and $Nf(X)$ are integers (that is, M and N are the least common multiples of the denominators of $a_0, \dots, a_{m-1}$ and $b_0, \dots, b_{n-1}$, respectively). Let $A_i = Ma_i$ for $i \in \{0, \dots, m-1\}$, $B_j = Nb_j$ for $j \in \{0, \dots, n-1\}$ and $A_m = M, B_n = N$. Then

$$MNf(X)g(X) \equiv A_m B_n X^{m+n} + \ldots + A_0 B_0.$$

Since $f(X)g(X) \in \mathbb{Z}[X]$, all coefficients of $MNf(X)g(X)$ are divisible by MN.

Suppose that $MN > 1$ and let p be a prime divisor of MN. Then there exists an integer $i \in \{0, \dots, m\}$ so that $p \nmid A_i$. Indeed, if $p \nmid M$, then $p \nmid A_m$ and if $p \mid M$, then $p \mid A_i$ for all $i \in \{0, \dots, m\}$ would imply that $A_i/p = (M/p)a_i \in \mathbb{Z}$, yielding a contradiction to the minimality of M. Similary, there exists an integer $j \in \{0, \dots, n\}$ such that $p \nmid B_j$. Let I and J be the greatest integers among these numbers i and j, respectively. Then the coefficient of X^{I+J} in $MNf(X)g(X)$ is

$$[X^{I+J}] = \ldots + A_{I+1}B_{J-1} + A_I B_J + A_{I-1}B_{J+1} + \ldots \equiv A_I B_J + p \cdot R$$

where R is an integer, so in particular, it is not divisible by p which contradicts the fact that the coefficients of $MNf(X)g(X)$ are divisible by MN. □

Corollary 2. Let n be a positive integer. Then the coefficients of Φ_n are integers, that is, $\Phi_n(X) \in \mathbb{Z}[X]$.

Proof. The proof goes by induction on n. The statement is true for $n = 1$ since $\Phi_1(X) = X - 1$. Suppose that the statement is true for all $k < n$. Then from Theorem 2 we obtain

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d \neq n} \Phi_d(X)},$$

so the coefficients of $\Phi_n(X)$ are rational and thus by Lemma 2 integers. □

We can also use the Möbius Inversion to obtain a direct formula for the cyclotomic polynomials:

Theorem 3. Let n be a positive integer. Then

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

Proof. This immediately follows from the Theorems 1 and 2. □

Lemma 3. Let p be a prime number and n be a positive integer. Then

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{if } p \mid n \\ \dfrac{\Phi_n(X^p)}{\Phi_n(X)} & \text{if } p \nmid n. \end{cases}$$

Proof. Suppose first that $p \mid n$. Then

$$\begin{aligned}
\Phi_{pn}(X) &= \prod_{d \mid pn} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \\
&= \left(\prod_{d \mid n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{\substack{d \mid pn \\ d \nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \\
&= \Phi_n(X^p) \prod_{\substack{d \mid pn \\ d \nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}.
\end{aligned}$$

However, $d \mid pn$ and $d \nmid n$ implies that $p^2 \mid d$ (since $p \mid n$), so d is not squarefree and thus $\mu(d) = 0$. Therefore

$$\prod_{\substack{d \mid pn \\ d \nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} = 1$$

and hence $\Phi_{pn}(X) = \Phi_n(X^p)$.

Suppose now that $p \nmid n$. Then

$$\begin{aligned}
\Phi_{pn}(X) &= \prod_{d \mid pn} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \\
&= \left(\prod_{d \mid n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{d \mid n} \left(X^{\frac{pn}{pd}} - 1\right)^{\mu(pd)}\right) \\
&= \left(\prod_{d \mid n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{d \mid n} \left(X^{\frac{n}{d}} - 1\right)^{-\mu(d)}\right) \\
&= \frac{\Phi_n(X^p)}{\Phi_n(X)}.
\end{aligned}$$

□

From this we get the following corollary:

Corollary 3. Let p be a prime number and n, k be positive integers. Then

$$\Phi_{p^k n}(X) = \begin{cases} \Phi_n(X^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{if } p \nmid n. \end{cases}$$

Proof. From Lemma 3, we have

$$\Phi_{p^k n}(X) = \Phi_{p^{k-1} n}(X^p) = \ldots = \Phi_{pn}(X^{p^{k-1}}) = \begin{cases} \Phi_n(X^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{if } p \nmid n. \end{cases}$$

□

Lemma 4. Let p be a prime number. Suppose that the polynomial $X^n - 1$ has a double root modulo p, that is, there exists an integer a and a polynomial $f(X) \in \mathbb{Z}[X]$ such that

$$X^n - 1 \equiv (X-a)^2 f(X) \pmod{p}.$$

Then $p \mid n$.

Proof. [1] Clearly, $p \nmid a$. Substituting $y = X - a$, we get

$$(y+a)^n - 1 \equiv y^2 f(y+a) \pmod{p}.$$

Comparing coefficients, we see that the coefficient of y on the right hand side is 0. By the binomial theorem, the coefficient of y on the left hand side is na^{n-1}. It follows that $na^{n-1} \equiv 0 \pmod{p}$. But $p \nmid a$, so $p \mid n$. □

Corollary 4. Let n be a positive integer, $d < n$ a divisor of n integer. Suppose that p divides $\Phi_n(x_0)$ and $\Phi_d(x_0)$, where $x_0 \in \mathbb{Z}$. Then $p \mid n$.

Proof. By Theorem 2,

$$x^n - 1 = \prod_{t \mid n} \Phi_t(x),$$

so $x^n - 1$ is divisible by $\Phi_n(x)\Phi_d(x)$. It follows that the polynomial $X^n - 1$ has a double root at x_0 modulo p, so by Lemma 4, $p \mid n$. □

Theorem 4.
Let n be a positive integer and x be any integer. Then every prime divisor p of $\Phi_n(x)$ either satisfies $p \equiv 1 \pmod{n}$ or $p \mid n$.

Proof. Let p be a prime divisor of $\Phi_n(x)$. Note that $p \nmid x$, because $p \mid \Phi_n(x) \mid x^n - 1$. Let $k = \mathrm{ord}_p(x)$. Since $p \mid x^n - 1$, we have $x^n \equiv 1 \pmod{p}$, so $k \mid n$. Hence $k = n$ or $k < n$.

Case 1: $k = n$. By Fermat's little theorem, $p \mid x^{p-1} - 1$ since $p \nmid x$ and p is prime. But then $k|(p-1)$, and since $k = n$, $n|(p-1)$ so $p \equiv 1 \pmod{n}$.

Case 2: $k < n$. Since

$$0 \equiv x^k - 1 = \prod_{d \mid k} \Phi_d(x) \pmod{p},$$

there exists a divisor d of k so that $p \mid \Phi_d(x)$. Observe that $d \leq k$, because $d \mid k$. But $k < n$, so $d < n$. Furthermore d is a divisor of n, as $d \mid k \mid n$. Now let us consider

[1] We can also prove Lemma 4 with calculus modulo p by introducing the familiar rules for computing the derivative (and showing that they are consistent). The fact that a double root of a function is a root of its derivative remains invariant modulo p. The derivative of $X^n - 1$ is nX^{n-1}, so $na^{n-1} \equiv 0 \pmod{p}$. But $p \nmid a$, so $p \mid n$.

the decomposition of $x^n - 1$ into cyclotomic polynomials. We have two divisors of n (which are d and n) that divide n. So we have two cyclotomic polynomials in that factorization that have p as a factor. Thus it follows from Corollary 4 that $p \mid n$. $\square$

Corollary 5. Let p be a prime number and x be an integer. Then every prime divisor q of $1 + x + \ldots + x^{p-1}$ either satisfies $q \equiv 1 \pmod{p}$ or $q = p$.

Proof. Let q be a prime divisor of $1 + x + \ldots + x^{p-1}$. Since

$$1 + x + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1} = \frac{x^p - 1}{\Phi_1(x)},$$

we have $1 + x + \ldots + x^{p-1} = \Phi_p(x)$. It follows from Theorem 4 that $q \equiv 1 \pmod{p}$ or $q \mid p$, that is, $q = p$. $\square$

The following lemma is quite well known:

Lemma 5. Let a and b be positive integers and x be an integer. Then

$$\gcd(x^a - 1, x^b - 1) = |x^{\gcd(a,b)} - 1|.$$

Theorem 5. Let a and b be positive integers. Suppose that x is an integer so that $\gcd(\Phi_a(x), \Phi_b(x)) > 1$. Then $\frac{a}{b} = p^k$ for some prime number p and integer k.

Proof. Let p be a common prime divisor of $\Phi_a(x)$ and $\Phi_b(x)$. We prove that $\frac{a}{b}$ must be a power of p. Suppose that $a = p^\alpha A$ and $b = p^\beta B$, where $\alpha, \beta \geq 0$ are integers and A and B are positive integers not divisible by p. We prove that $A = B$. Since $p \mid \Phi_a(x) \mid x^a - 1$, we have $p \nmid x$.

We first show that $p \mid \Phi_A(x)$. This is clear if $\alpha = 0$. Otherwise, if $\alpha > 1$, it follows from Corollary 3 that

$$0 \equiv \Phi_a(x) = \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} \pmod{p},$$

so $\Phi_A(x^{p^\alpha}) \equiv 0 \pmod{p}$. But $x^{p^\alpha} \equiv x \cdot x^{p^\alpha - 1}$ and since $p^\alpha - 1$ is divisible by $p - 1$, it follows from Euler's theorem that $x^{p^\alpha - 1} \equiv 1 \pmod{p}$ and thus, $x^{p^\alpha} \equiv x \pmod{p}$. Hence

$$0 \equiv \Phi_A(x^{p^\alpha}) \equiv \Phi_A(x) \pmod{p}$$

and similarly, $p \mid \Phi_B(x)$.

Suppose that $A > B$. Let $t = \gcd(A, B)$, then $t < A$. We know that $p \mid \Phi_A(x) \mid x^A - 1$ and $p \mid \Phi_B(x) \mid x^B - 1$, so $p \mid \gcd(x^A - 1, x^B - 1)$. But from Lemma 5, it follows that

$$\gcd(x^A - 1, x^B - 1) = |x^t - 1|,$$

so $p \mid x^t - 1$. However,

$$0 \equiv x^t - 1 = \prod_{d|t} \Phi_d(x) \pmod{p},$$

thus there exists a divisor d of t such that $p \mid \Phi_d(x)$. But $d \mid t \mid A$, $d < A$ and $p \mid \Phi_A(x)$. By Corollary 4, we have $p \mid A$, a contradiction since we assumed that $p \nmid A$. □

2.2 Applications

A common application of cyclotomic polynomials is the proof of a special case of Dirichlet's Theorem.

Theorem 6. Let n be a positive integer. Then there exist infinitely many prime numbers p with $p \equiv 1 \pmod{n}$.

Proof. Suppose that there exist only finitely many prime numbers p with $p \equiv 1 \pmod{n}$. Let T be the product of these primes and all primes diving n. Clearly $T > 1$. Let k be a sufficiently large positive integer such that $\Phi_n(T^k) > 1$ (since Φ_n is a nonconstant monic polynomial, such k exists) and let q be a prime divisor of $\Phi_n(T^k)$. Because q divides $T^{kn} - 1$, q does not divide T, so $q \not\equiv 1 \pmod{n}$ and $q \nmid n$, a contradiction to Theorem 4. □

Another nice application is a generalisation of a problem from the IMO Shortlist 2002:

Problem 1. Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Prove that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.

The official solution comments that using cyclotomic polynomials, it can be proved that $2^{p_1 p_2 \cdots p_n} + 1$ has at least $2^{2^{n-1}}$ divisors (which is much more than 4^n when n is large). We are going to prove this generalisation now.

Problem 2. Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Prove that $2^{p_1 p_2 \cdots p_n} + 1$ has at least $2^{2^{n-1}}$ divisors.

Solution. It is sufficient to prove that $2^{p_1 \cdots p_n} + 1$ has at least 2^{n-1} pairwise coprime divisors and hence at least 2^{n-1} distinct prime divisors. We have

$$\begin{aligned}
\left(2^{p_1 \cdots p_n} - 1\right)\left(2^{p_1 \cdots p_n} + 1\right) = 2^{2p_1 \cdots p_n} - 1 &= \prod_{d|2p_1 \cdots p_n} \Phi_d(2) \\
&= \left(\prod_{d|p_1 \cdots p_n} \Phi_d(2) \right) \left(\prod_{d|p_1 \cdots p_n} \Phi_{2d}(2) \right) \\
&= \left(2^{p_1 \cdots p_n} - 1\right) \left(\prod_{d|p_1 \cdots p_n} \Phi_{2d}(2) \right)
\end{aligned}$$

and hence

$$2^{p_1 \cdots p_n} + 1 = \prod_{d \mid p_1 \cdots p_n} \Phi_{2d}(2).$$

From Theorem 5, we know that if $\Phi_a(2)$ and $\Phi_b(2)$ are not coprime, then a/b must be a prime power. We thus have to prove that there exists a set of 2^{n-1} divisors of $p_1 \ldots p_n$ so that no two of them differ by exactly one prime number. But this is clear, because we can take the divisors of $p_1 \ldots p_n$ which have an even number of prime divisors and since there are equally many divisors having an even number of prime divisors and divisors having an odd number of prime divisors, there exist exactly 2^{n-1} of them. □

Problem 3. Find all integer solutions of the equation

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Solution. The equation is equivalent to

$$1 + x + \ldots + x^6 = (y - 1)(1 + y + \ldots + y^4).$$

We know from Corollary 5 that every prime divisor p of $1 + x + \ldots + x^6$ either satisfies $p = 7$ or $p \equiv 1 \pmod 7$. This implies that every divisor of $1 + x + \ldots + x^6$ is either divisible by 7 or congruent to 1 modulo 7. Thus, $(y - 1) \equiv 0 \pmod 7$ or $(y - 1) \equiv 1 \pmod 7$, that is, $y \equiv 1 \pmod 7$ or $y \equiv 2 \pmod 7$. If $y \equiv 1 \pmod 7$ then $1 + y + \ldots + y^4 \equiv 5 \not\equiv 0, 1 \pmod 7$, a contradiction and if $y \equiv 2 \pmod 7$ then $1 + y + \ldots + y^4 \equiv 31 \equiv 3 \not\equiv 0, 1 \pmod 7$, also a contradiction. Hence, this equation has no integer solutions. □

References

[1] Yves Gallot, *Cyclotomic Polynomials and Prime Numbers*, `http://perso.orange.fr/yves.gallot/papers/cyclotomic.pdf`

[2] Titu Andreescu, Dorin Andrica, Zuming Feng, *104 Number Theory Problems: From the Training of the USA IMO Team*, Birkhauser, 2007, pp. 36-38.

[3] Titu Andreescu, Dorin Andrica, *Complex Numbers from A to ...Z*, Birkhauser, 2006, pp.45-51.

[4] Mathlinks, *Cyclotomic Property*, `http://www.mathlinks.ro/Forum/viewtopic.php?t=126566`

Author: Yimin Ge, Vienna, Austria