Cyclotomic Polynomials

James Bang

November 26, 2019

Cyclotomic Polynomials are a very special type of polynomial which result when factoring expressions of the form $x^n - y^n$ over the integers. They are extremely useful when dealing with prime factors of numbers of such forms, especially when n is prime or composed of few prime factors (such as $2p$). This handout explores the properties of cyclotomic polynomials and some of their applications in the realm of Olympiad mathematics within Number Theory.

1 Motivation for Cyclotomic Polynomials

Consider factoring the expression $x^n - 1$ for each $n = 1, 2, \ldots$. Then, for each $n \geqslant 1$, there exists a factor of $x^n - 1$ which is **not** a factor of $x^k - 1$ for each $k < n$. For example, the factors coloured in red is the new polynomial not appearing before:

$$\begin{aligned}
x^1 - 1 &= (x - 1) \\
x^2 - 1 &= (x - 1)(x + 1) \\
x^3 - 1 &= (x - 1)(x^2 + x + 1) \\
x^4 - 1 &= (x - 1)(x + 1)(x^2 + 1) \\
x^5 - 1 &= (x - 1)(x^4 + x^3 + x^2 + x + 1)
\end{aligned}$$

For each new polynomial which occurs in the factorisation of $x^n - 1$, we label it $\Phi_n(x)$. Hence, for example, we have $\Phi_4(x) = x^2 + 1$, since $x^2 + 1$ is the new polynomial which occurs in the factorisation of $x^4 - 1$.

From basic high-school level mathematics, we know that the roots of $x^n - 1$ are in the form ζ^k where $\zeta = e^{2i\pi/n}$ is a **Primitive Root of Unity**. Hence, since $\Phi_n(x) \mid x^n - 1$ (by definition), the roots of $\Phi_n(x)$ must all lie on the unit circle and be of the form ζ^k. The question is, what exactly are the roots of $\Phi_n(x)$?

2 Definitions

A root $\omega = e^{2i\pi k/n}$ for some integer $k \leqslant n$ is called **Primitive** if $\gcd(k, n) = 1$. It turns out that the n-th Cyclotomic Polynomial $\Phi_n(x)$ is the polynomial with exactly the primitive roots of unity:

Definition. The n-th **Cyclotomic Polynomial** $\Phi_n(x)$ is defined to be the polynomial

$$\Phi_n(X) = \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(n,k)=1}} \left(X - \zeta^k\right)$$

where $\zeta = e^{2i\pi/k}$ is an n-th primitive root of unity.

For example, for the case $\Phi_4(X) = X^2 + 1$, we have $\Phi_4(X) = (X - i)(X + i) = \left(X - e^{2i\pi/4}\right)\left(X - e^{2i\pi \cdot 3/4}\right)$. Of course, we need to show that these two definitions are equivalent, which we shall do later; for now, we shall prove some properties about Φ_n (using the second definition) which will aid us in showing two definitions are equivalent.

Lemma 2.0.1

We have $\Phi_n(X) \mid X^n - 1$ for each n.

Proof. Clearly, each root of unity ζ^k of $\Phi_n(X)$ is also a root of $X^n - 1$, since we have

$$X^n - 1 = \left(\zeta^k\right)^n - 1 = (\zeta^n)^k - 1 = 1^k - 1 = 0.$$

Since $\Phi_n(x)$ has no double roots by definition, it follows that $\Phi_n(X) \mid X^n - 1$ for each n. $\square$

Lemma 2.0.2

For each pair of integers $A \neq B$, the polynomials $\Phi_A(X)$ and $\Phi_B(X)$ share no common roots (i.e. they are **coprime**).

Proof. Suppose they share a root r. Then, since $\Phi_A(r) = 0$, by definition there exists k with $\gcd(k, A) = 1$ and $r = e^{2\pi i \cdot k/A}$, and similarly with $\Phi_B(r) = 0$ there exists ℓ with $\gcd(\ell, B) = 1$ and $r = e^{2\pi i \cdot \ell/B}$. Hence, equating both sides we have

$$e^{2\pi i \cdot \ell/B} = e^{2\pi i \cdot k/A} \implies \frac{2\pi i \cdot \ell}{B} \equiv \frac{2\pi i \cdot k}{A} \pmod{2\pi i}$$

which means $\ell/B - k/A$ is an integer. In particular, this means $AB \mid A\ell - Bk$ or that $A \mid A\ell - Bk$ so $A \mid Bk$. However, we had $\gcd(k, A) = 1$ and thus $A \mid B$. Similarly we also get $B \mid A$, implying $A = B$, which is a contradiction. Hence, $\Phi_A(X)$ and $\Phi_B(X)$ share no common roots for each $A \neq B$. $\square$

Lemma 2.0.3

The degree of the cyclotomic polynomial is $\deg(\Phi_n(X)) = \varphi(n)$, the Euler Totient Function.

Proof. By definition, we have $\Phi_n(X) = \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(n,k)=1}} (X - \zeta^k)$, and thus the degree is simply the number of factors, or the number of k with $\gcd(n, k) = 1$ and $k \leqslant n$. This is clearly $\varphi(n)$, and thus we have $\deg(\Phi_n(X)) = \varphi(n)$ for each $n \geqslant 1$. $\square$

Lemma 2.0.4

For each $n \geqslant 1$, we have

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

where the product ranges across all divisors $d \mid n$.

Proof. As discussed before, the roots of $X^n - 1$ are simply all the numbers of the form ζ^k. Hence, to show the two polynomials are equivalent, we need three things: (a) their leading coefficients are the same, (b) their roots are the same.

(a) This is pretty obvious, since by definition $\Phi_d(X)$ is a monic polynomial, and thus both leading coefficients of the left and right side are equal to 1.

(*b*) We have $\Phi_d(X) \mid X^d - 1$ by Lemma 2.0.1. However, then we have

$$\Phi_d(X) \mid X^d - 1 \mid X^{d(n/d)} - 1 = X^n - 1,$$

since $a \mid b$ means $X^a - 1 \mid X^b - 1$. Since no pair of factors on the right side have a common root of unity, we must have $RHS \mid LHS$.

To show $LHS \mid RHS$, it suffices to show that each root ζ^k of the left side is a root of exactly one factor of the right side. Clearly, Lemma 2.0.3 shows all the factors are coprime, and hence we just need to show ζ^k is a root of one of them. However, it can be checked that ζ^k is a root of $\Phi_d(X)$ when $d = \frac{n}{\gcd(n,k)}$ since $\gcd(d,k) = 1$ and ζ^k is in the form $e^{2\pi i \cdot \ell/d}$ for some ℓ coprime to d.

Hence, it follows that both the left and right side have the same set of roots, and thus they must be a multiple of each other by a constant. Since both polynomials are monic, the constant of proportionality must be 1, and thus they are equal. □

In particular, combining Lemma 2.0.3 and 2.0.4 and comparing the degrees gives the interesting corollary

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

3 Why is $\Phi_n(X)$ always an integer polynomial?

It seems like we have proved the equivalence between the two definitions: the "new" polynomial introduced is easily seen to be $\Phi_n(X)$ by the second definition, since it is coprime to every other cyclotomic polynomial $\Phi_k(X)$, $k < n$, and thus it must be the new polynomial. However, how do we know that $\Phi_n(X)$ must always be an integer polynomial, as per the first definition?

Lemma 3.0.1

Each cyclotomic polynomial $\Phi_n(X)$ must be a **rational** polynomial for each n, i.e. $\Phi_n(X) \in \mathbb{Q}[x]$.

Proof. We proceed by strong induction: clearly, we have $\Phi_1(X) = x - 1 \in \mathbb{Q}[x]$ and $\Phi_2(X) = x + 1 \in \mathbb{Q}[x]$, and so the base cases are done.

Suppose the polynomial $\Phi_k(X)$ has rational coefficients for each $k = 1, 2, \ldots, N$ for some integer N. Then, by Lemma 2.0.4 we have

$$\Phi_{N+1}(X) = \frac{X^{N+1} - 1}{\prod_{\substack{1 \leqslant d < N+1 \\ d|N+1}} \Phi_d(X)}$$

which is clearly a polynomial with rational coefficients as well, since we can long divide the right hand side to get something in $\mathbb{Q}[x]$ (since we definitely know it's a polynomial). Hence, by Mathematical Induction, we have that $\Phi_n(X) \in \mathbb{Q}[x]$ for each $n \geqslant 1$. □

Ok, so we have the cyclotomic polynomial has rational coefficients for each n. The method of showing they actually have integer coefficients is similar, but we need a very strong lemma:

Lemma 3.0.2

Let $f(x)$ and $g(x)$ be two nonzero **monic** polynomials with rational coefficients. It is given that $f(x) \cdot g(x)$ is a polynomial with integer coefficients. Then, f and g also have all integer coefficients.

Proof. We denote $f(x) = \sum_{k=0}^{n} a_k x^k$ and $g(x) = \sum_{k=0}^{m} b_k x^k$ where $a_n = b_m = 1$. Let A be the least positive integer for which $A \cdot f(x)$ has all integer coefficients (that is, A is the GCD of all the denominators of a_i when written in reduced form), and similar with B for $g(x)$. Then, $AB \cdot f(x)g(x)$ is the product of two integer polynomials, and thus must also be an integer polynomial. We also denote $A_k = A \cdot a_k$ and $B_k = B \cdot b_k$ for every such coefficient: since A was the GCD of the denominators, it follows $A_k \in \mathbb{Z}$ for each k, and similarly $B_k \in \mathbb{Z}$. Furthermore, we have $\gcd(A_0, A_1, \ldots, A_n) = \gcd(B_0, B_1, \ldots, B_m) = 1$ since definition of GCD. Then we have:

$$AB \cdot f(x)g(x) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} A_i B_j \right) x^k = \sum_{k=0}^{m+n} c_k x^k.$$

Now, suppose f and g are not both integer polynomials: then, we must have $AB > 1$. Pick a prime $p \mid AB$: then, there exists some i, j for which $p \nmid A_i$ and $p \nmid B_j$. Indeed, for $p \nmid A$, we have $p \nmid A_n$ since $A_n = A \cdot a_n = A$; for $p \mid A$, we cannot have $p \mid A_i$ for each i since $\gcd_{0 \leqslant i \leqslant n}(A_i) = 1$. Similarly for $p \nmid B_j$.

Pick i, j such that the above conditions hold and furthermore i, j are the **greatest such numbers which satisfy these conditions**, and let $k = i + j$. Then, the coefficient of x^{i+j} would be

$$\sum_{i'+j'=k} A_{i'} B_{j'} = A_0 B_{i+j} + A_1 B_{i+j-1} + \cdots + A_{i+j} B_0$$

where we define $A_\ell = 0$ for $\ell > n$ and similar with B_ℓ. Then, by the maximality of i, j, all of these terms will be divisible by p **except** for $A_i B_j$, which is not a multiple of p (since $p \nmid A_i, B_j$). It follows that $p \nmid c_{i+j}$, contradicting the given condition that $f(x)g(x)$ is an integer polynomial (as then, $AB \cdot f(x)g(x)$ must have all coefficients divisible by AB and thus p, which is not true for c_{i+j}). Hence, it follows that $AB = 1$, i.e. both f, g are integer coefficients. □

Now, we are ready to prove that $\Phi_n(X) \in \mathbb{Z}[X]$ for each $n \geqslant 1$.

Problem 3.0

The cyclotomic polynomial $\Phi_n(X)$ is an integer polynomial.

Proof. Set up the induction as in the proof they have rational coefficients. We have

$$\Phi_{N+1}(X) \cdot \left(\prod_{\substack{1 \leqslant d < N+1 \\ d \mid N+1}} \Phi_d(X) \right) = X^{N+1} - 1 \in \mathbb{Z}[x].$$

By the lemma, since we have two rational polynomials multiplying to form an integer polynomial, it follows that both are integer polynomials. It follows that $\Phi_{N+1}(X) \in \mathbb{Z}[X]$, and the inductive step is complete. □

4 Why is $\Phi_n(X)$ irreducible over $\mathbb{Z}$?

We still haven't quite proven why the two definitions are equivalent (!): what if, for some strange reason, $\Phi_n(X)$ has a nontrivial factorisation for some n? This would mean there would be *multiple* new polynomials appearing at some step. This can be shown not to happen, by showing $\Phi_n(X)$ is irreducible for each $n \geqslant 1$.

Lemma 4.0.1

For a polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$, we define the **derivative** in $\mathbb{Z}_p$ as $f'(x) := \sum_{k=0}^{n} k a_k x^{k-1}$. Suppose that there exists some nonconstant irreducible polynomial $u(x)$ for which $u(x)^2 \mid f(x)$, i.e.

there exists polynomials $A, B \in \mathbb{Z}_p$ for which

$$f(x) = (u(x))^2 A(x) + p \cdot B(x).$$

Then, we have $u(x) \mid f'(x)$ as well.

Proof. The standard sum and product rules from calculus obviously carries onto derivatives modulo p, i.e.

- $(f(x) + g(x))' = f'(x) + g'(x)$
- $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

(Just notice they hold for polynomials in $\mathbb{R}[x]$, and reducing mod p has no effect.) Hence, we have

$$\begin{aligned} f'(x) &= (u(x)^2 A(x) + p \cdot B(x))' \\ &= (u(x)^2 A(x))' + p \cdot B'(x) \\ &\equiv (u(x)^2)' A(x) + u(x)^2 A'(x) \pmod{p} \\ &\equiv u(x)\left(2u'(x)A(x) + u(x)A'(x)\right) \pmod{p}. \end{aligned}$$

Hence, there exists polynomials $C(x) = 2u'(x)A(x) + u(x)A'(x)$ and $D(x) = B'(x)$ for which $f'(x) = u(x)C(x) + p \cdot D(x)$, and hence $u(x) \mid f'(x)$ as well. □

Problem 4.0

The n-th cyclotomic polynomial $\Phi_n(X)$ is **irreducible** in $\mathbb{Z}$ for each $n \geqslant 1$, i.e. if there are polynomials $f(x)$ and $g(x)$ with integer coefficients such that $\Phi_n(X) = f(X)g(X)$, then one of f and g is constant.

Proof. Suppose otherwise that $\Phi_n(X) = f(X)g(X)$ for some nonconstant polynomials $f, g \in \mathbb{Z}[X]$. We can further assume that $f(X)$ is the **minimum polynomial** of ζ, that is, we have $f(\zeta) = 0$ and f is the integer polynomial with smallest positive degree for which this is true. We use the fact that if F is the minimum polynomial of some complex α and $G(\alpha) = 0$ for some nonzero polynomial G, then we must have $F \mid G$ (as polynomials).

Suppose that for some prime p for which $p \nmid n$, we **do not have** $f(\zeta^p) = 0$: then, since $\Phi_n(\zeta^p) = 0$ due to $\gcd(n, p) = 1$, we must have $g(\zeta^p) = 0$. This means ζ is a root of the polynomial $g(X^p)$, and hence there exists another polynomial $P(x)$, for which $g(X^p) = f(x) \cdot P(x)$ (since $f(x) \mid g(X^p)$ due to minimal polynomial). Thus, we have

$$\Phi_n(X^p) = f(X^p) \cdot g(X^p) = f(X^p) \cdot f(x) \cdot P(x).$$

Recall the well-known multinomial expansion

$$(a_1 + a_2 + \cdots + a_n)^p = \sum_{z_1 + \cdots + z_n = p} \binom{p}{z_1, z_2, \ldots, z_n} a_1^{z_1} a_2^{z_2} \ldots a_n^{z_n},$$

and since we have $\binom{p}{z_1, \ldots, z_n} \equiv 0 \pmod{p}$ except when one of $z_i = p$, we have

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \pmod{p},$$

and thus similarly we also get

$$(a_0 x^0 + a_1 x^1 + \cdots + a_n x^n)^p \equiv (a_0 x^0)^p + (a_1 x^1)^p + \cdots + (a_n x^n)^p \equiv a_0 x^{0 \cdot p} + a_1 x^{1 \cdot p} + \cdots + a_n x^{np} \pmod{p}$$

by Fermat's Little Theorem, and hence $f(x^p) \equiv f(x)^p \pmod{p}$ for any $f(x) \in \mathbb{Z}[x]$ (by setting $f(x) = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n$). Hence, reducing both sides of the earlier equation mod p gets

$$(\Phi_n(X))^p \equiv f(x)^{p+1} \cdot P(x) \pmod{p}.$$

Take an irreducible factor $u(x) \mid f(x)$. Then, by unique factorisation in the integers modulo p, it follows that $u(x)^{p+1} \mid (\Phi_n(X))^p$, and since u is irreducible, we must have $u^2 \mid \Phi_n$.

However, we then also have $(u(x))^2 \mid \Phi_n(X) \mid X^n - 1$, and thus by Lemma 4.0.1 we also get $u(X) \mid (X^n-1)' = nX^{n-1}$. Since $u(x)$ is irreducible, and $p \nmid n$ (and hence the right side is not congruent to 0 (mod p)), it follows that $u(X) = X$, which is trivially impossible since $u \mid X^n - 1$. This is a contradiction, and thus it follows that whenever $\Phi_n(X) = f(X)g(X)$ for which f is the minimum polynomial of ζ, we also have $f(\zeta^p) = 0$ as well.

Let P denote the set of primes $p \leqslant n$ for which $\gcd(p, n) = 1$. From above, we have that whenever $p \in P$, we also have ζ^p is a root of f. It follows by trivial induction that for each subset $A \subseteq P$, we also have $\zeta^{\prod_{q \in A} q}$ is a root of f, and thus all the numbers k for which $\gcd(k, n)$ has $f(\zeta^k) = 0$. There are $\varphi(n)$ such $k \leqslant n$, and furthermore $\deg(\Phi_n(X)) = \varphi(n)$. It follows that $\deg(f) \geqslant \deg(\Phi_n)$, and hence g is constant, which proves $\Phi_n(X)$ is irreducible for each $n \geqslant 1$. $\square$

Finally, it can be seen that all the previous lemmas imply the two definitions from the start are equivalent to each other.

5 Computing $\Phi_n(X)$

Of course, we already have a formula for $\Phi_n(X)$ as per the second definition of the Cyclotomic Polynomial. However, this formula seems ridiculous to actually use, since how does one even compute those roots of unity in an Olympiad competition? Furthermore, we can now use the first definition to completely factor $X^n - 1$ to find $\Phi_n(X)$, but are there any better ways?

5.1 The Möbius Function

Definition. The **Möbius Function** $\mu : \mathbb{Z}^+ \to \{0, \pm 1\}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } \exists p \in \mathbb{P} \text{ with } p^2 \mid n \\ (-1)^k & \text{if } n = p_1 p_2 \dots p_k. \end{cases}$$

In particular, it can easily be seen that whenever $\gcd(m, n) = 1$, we have $\mu(mn) = \mu(m) \cdot \mu(n)$ (i.e. μ is **multiplicative**): this is because if either m, n are not squarefree, then their product will also not be squarefree, and if both of them are products of r and s distinct primes respectively, distinct with each other, then we simply have the identity $(-1)^r \times (-1)^s = (-1)^{r+s}$.

Lemma 5.1.1

Suppose $n \geqslant 1$. Then we have

$$\sum_{d \mid n} \mu(d) = \delta_{1,n} = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n \geqslant 2, \end{cases}$$

where δ represents the Kronecker Delta.

Proof. The result is trivial for $n = 1$ by definition. For $n \geqslant 2$, consider $r = \text{rad}(n)$ as the squarefree (radical) part of n, i.e.

$$\text{rad}(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}) = p_1 p_2 \dots p_n.$$

Then, it becomes obvious that

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid r} \mu(d)$$

since any other term has a prime dividing it twice and thus has a value of 0. Now, take some prime $p \mid r$, let $r = p \cdot N$ and consider pairing each divisor $d \mid N$ with that of pd: we get

$$\sum_{d|r} \mu(d) = \sum_{d|N} (\mu(d) + \mu(pd)) = \sum_{d|N} (\mu(d) - \mu(d)) = 0,$$

since $\mu(pd) = \mu(p) \cdot \mu(d) = -\mu(d)$. $\square$

This allows us to prove the following **Möbius Inversion Formula.**

Problem 5.1

For a function $f : \mathbb{Z} \to \mathbb{R}$, consider defining the **Möbius Transform** (a special case of Dirichlet's convolution)

$$F(n) = (f * \mathbf{1})(n) = \sum_{d|n} f(d).$$

Then, we have

$$f(n) = \sum_{d|n} \mu(n/d) F(d) = (\mu * F)(n).$$

Proof. By definition of F, we have

$$\sum_{d|n} \mu(n/d) F(d) = \sum_{d|n} \mu(n/d) \sum_{N|d} f(N) = \sum_{N|n} f(N) \cdot \sum_{d|n/N} \mu\left(\frac{n}{Nd}\right).$$

Performing the transformation $d \mapsto \frac{n}{Nd}$ leaves the condition $d \mid n/N$ intact, and the sum turns into

$$\sum_{N|n} f(N) \cdot \sum_{d|n/N} \mu(d) = \sum_{N|n} f(N) \delta_{1,n/N} = f(n)$$

since $\delta_{1,n/N} = 1$ if and only if $n = N$ (for which we get the $f(n)$ term) and 0 for any other value of N. $\square$

Similarly, it is possible to perform this entire computation with sums replaced by products: if we perform the transformation $F \to \log(F)$ and $f \to \log(f)$, then we get

$$\log F(n) = \sum_{d|n} \log f(d) \implies F(n) = \prod_{d|n} f(d),$$

and the Möbius transformation then becomes $f(n) = \prod_{d|n} F(d)^{\mu(n/d)}$. In particular, if we substitute $f(n) = \Phi_n(X)$ and $F(n) = X^n - 1$, then the Möbius Involution Formula gives

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

Example. To compute $\Phi_{15}(x)$, we can use this formula to obtain:

$$\Phi_{15}(x) = \prod_{d|15} \left(X^d - 1\right)^{\mu(15/d)} = \frac{(X^{15} - 1) \cdot (X - 1)}{(X^3 - 1) \cdot (X^5 - 1)} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

5.2 Cases when large prime powers divide n

It turns out we can find considerably simpler expressions for $\Phi_n(X)$ in the cases where n is expressible in the form $n = p^A \cdot B$.

Problem 5.2

Let $n \geqslant 1$, and p be a prime number. Then we have:

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

Proof. Both of these formulae follow from algebraic manipulations from the Möbius Inversion formula as per above. For $p \mid n$, by the transformation $d \to pn/d$, we have

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

where the last equality follows because $d \mid pn$ but $d \nmid n$ implies $p^2 \mid d$, which implies d is not squarefree and thus $\mu(d) = 1$ for each such d.

For the other case where $p \nmid n$, we similarly have

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

Hence, we have proven the identities. □

In particular, we can generalise the following statement. Let n be a positive integer and p is prime such that $\nu_p(n) \geqslant 1$. Let $n = N \cdot p^{\nu_p(n)} = N \cdot P$. Then, have

$$\boxed{\Phi_{P \cdot N}(X) = \frac{\Phi_N(X^P)}{\Phi_N(X^{P/p})},}$$

which follows from using the statement of Problem 5.2 $\nu_p(n)$ times.

Example. To compute $\Phi_{27}(X)$, we plug into the above formula, to get

$$\Phi_{27}(X) = \frac{\Phi_1(X^{27})}{\Phi_1(X^9)} = \frac{X^{27} - 1}{X^9 - 1} = X^{18} + X^9 + 1.$$

In general, we can also compute

$$\Phi_{p^k}(X) = \frac{\Phi_1(X^{p^k})}{\Phi_1(X^{p^{k-1}})} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1.$$

6 Cyclotomic Polynomials in Number Theory

Now, we get to the main section of this handout. We have seen some quite amazing algebraic properties about cyclotomic polynomials; yet their use of them in Olympiad mathematics comes almost exclusively from the properties of primes that divide $\Phi_n(X)$ for some integer X.

Lemma 6.0.1

Take a divisor $d \mid n$, and $k \in \mathbb{Z}$. Suppose that there exists some common prime divisor p between $\Phi_n(k)$ and $\Phi_d(k)$ for some n. Then, we must have $p \mid n$.

We shall prove a great generalisation of this theorem later, but for now we'll focus on the weaker version.

Proof. We had

$$X^n - 1 = \prod_{D|n} \Phi_D(X).$$

Hence, we have $\Phi_n(X) \cdot \Phi_d(X) \mid X^n - 1$, and thus $X^n - 1$ has a double root at $X = k$, meaning we have the factorisation

$$X^n - 1 \equiv (X-k)^2 P(X) \pmod{p}$$

for some polynomial $P(X) \in \mathbb{Z}[X]$. Taking derivatives, we have $X - a \mid nX^{n-1}$ as polynomials in $\mathbb{Z}_p[x]$, and hence $n \equiv 0 \pmod{p} \implies p \mid n$. $\square$

This allows us to prove perhaps the most important property about Cyclotomic Polynomials, at least when used in Olympiad number theory.

Problem 6.0

Let $n \geqslant 1$ and x be integers. For **any** prime $p \mid \Phi_n(x)$, we have either $p \equiv 1 \pmod{n}$ or $p \mid n$.

Proof. We have $p \mid \Phi_n(x) \mid x^n - 1$. However, we also have $p \mid x^{p-1} - 1$ by Fermat's Little Theorem, and thus $p \mid x^{\gcd(n,p-1)} - 1$. If we have $p \nmid x^k - 1$ for any $k < n$, then we have $\gcd(n, p-1) = n$ and thus it follows that $n \mid p - 1$, or so $p \equiv 1 \pmod{n}$.

Otherwise, there exists $k < n$ for which $p \mid x^k - 1$, and thus we can choose a smallest such k. It follows that $p \mid \Phi_k(x)$ (since we have $x^k - 1 = \prod_{d|k} \Phi_d(x)$, so there exists some $K \mid k$ for which $p \mid \Phi_K(x) \mid x^K - 1$, contradicting the minimality of k). Since we have $x^n = \prod_{d|n} \Phi_d(x)$, we have $\Phi_k(x)\Phi_n(x) \mid x^n - 1$, and thus the polynomial $X^n - 1$ has a double root at $X = x$. By the previous lemma, it follows that $p \mid n$. $\square$

In particular, if we take $n = q$ as another prime number, then we if $p \mid \Phi_q(x) = x^{q-1} + x^{q-2} + \cdots + x + 1$, then we have either $p \equiv 1 \pmod{q}$ or $p = q$. If we manage to show that $p \neq q$, then it means $p \equiv 1 \pmod{q}$, and thus **every** divisor of $\Phi_q(x)$ is $\equiv 1 \pmod{q}$. This idea will come up handy many times.

Problem 6.0

Let a, b be positive integers, such that $\Phi_a(x)$ and $\Phi_b(x)$ share a common factor greater than 1. Then, there exists an integer k and a prime p for which $a/b = p^k$.

Proof. Take some prime $p \mid \Phi_a(x), \Phi_b(x)$. It turns out that there can be at most one such prime, and furthermore a/b must be a power of p.

Let $a = p^\alpha A$ and $b = p^\beta B$ for some integers A, B, α, β for which $p \nmid A, B$. Then, by the corollary of Problem 5.2, we obtain

$$0 \equiv \Phi_a(x) = \Phi_{p^\alpha A}(x) = \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} \implies p \mid \Phi_A(x^{p^\alpha}).$$

However, we have $p \mid x^{p-1} - 1 \mid x^{(p-1)(p^{\alpha-1}+\cdots+p+1)} - 1 = p^{p^\alpha - 1} - 1$, and thus

$$\Phi_A(x^{p^\alpha}) = \Phi_A(x^{p^\alpha - 1} \cdot x) \equiv \Phi_A(x) \implies p \mid \Phi_A(x).$$

Similarly, we have $p \mid \Phi_B(x)$ as well. Thus, we have $p \mid \Phi_A(x) \mid x^A - 1$ and similarly $p \mid \Phi_B(x) \mid x^B - 1$, and hence

$$p \mid \gcd(x^A - 1, x^B - 1) = x^{\gcd(A,B)} - 1.$$

Thus, there exists some $\ell \mid \gcd(A, B)$ for which $p \mid \Phi_\ell(x)$, and $\ell \mid \gcd(A, B) \mid A$.

However, by Lemma 6.0.1, we have that since p is a common prime divisor between $\Phi_A(x)$ and $\Phi_\ell(x)$ for some $\ell \mid A$, it follows that $p \mid A$. This contradicts the assumption that $p \nmid A$, and thus it follows that $A = B$. It follows that $a/b = p^k$ for some integer k. $\square$

6.1 Bounding $\Phi_n(X)$ and Zsigmondy's Theorem

Due to the somewhat irregularity of the coefficients of $\Phi_n(X)$, it looks like bounding $\Phi_n(X)$ would be a difficult task. However, the following method obtains a very sharp bound for $\Phi_n(X)$:

Lemma 6.1.1

Let $n \geqslant 1$. Then, for each $X > 1$, the following bound holds:

$$(X-1)^{\varphi(n)} \leqslant \Phi_n(X) \leqslant (X+1)^{\varphi(n)}.$$

Proof. Instead of bounding by coefficients, we instead bound by the roots of $\Phi_n(X)$. We have

$$\Phi_n(X) = |\Phi_n(X)| = \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(n,k)=1}} \left|X - \zeta^k\right| \leqslant |X+1|^{\varphi(n)},$$

since the roots of unity ζ^k lie on the unit circle and thus every such distance $|X - \zeta^k|$ must be at most $b + 1$. Similarly, it can also be shown that $\Phi_n(X) \geqslant (X-1)^{\varphi(n)}$, since each such distance $|X - \zeta^k|$ must be at least $X - 1$ for each $X > 1$. $\square$

Lemma 6.1.2

Let $a, n > 1$ be positive integers, and let $q \mid \Phi_n(a)$. We define q to be a **Zsigmondy Prime** $q \mid a^n - 1$, but does **not** divide $a^k - 1$ for each $k < n$. Then:

(a) q is a non-Zsigmondy prime if and only if $q \mid n$.

(b) q must be the largest prime factor of n, with $n = q^a \cdot R$ where $R \mid q - 1$. Furthermore, $q^2 \nmid \Phi_a(x)$ unless $q = n = 2$.

(c) If no Zsigmondy primes exist, then $\Phi_n(a) = q^\ell$ for some ℓ; if $n \geqslant 3$, then $\ell = 1$.

Proof. For **(a)**, we first prove the 'if' direction. If $q \mid n$, then we have

$$1 \equiv a^n = a^{q \cdot (n/q)} \equiv a^{n/q} \pmod{q}$$

since we have $q \mid \Phi_n(a) \mid a^n - 1$.

For the 'only-if' direction, suppose q is not a Zsigmondy prime: then there exists some prime factor $p \mid n$ for which $a^{n/p} \equiv 1 \pmod{q}$. Since $\Phi_n(X) \mid \dfrac{X^n-1}{X^{n/p}-1}$, after placing $c = a^{n/p}$, we obtain

$$q \mid \Phi_n(a) \mid \frac{a^n-1}{a^{n/p}-1} = \frac{c^p-1}{c-1} = c^{p-1} + c^{p-2} + \cdots + c + 1 \equiv p \pmod{q}$$

whence $q = p \mid n$, and hence $q \mid n$. This proves **(a)**.

For **(b)**, notice that the proof from **(a)** shows that if $p \mid n$ and $a^{n/p} \equiv 1 \pmod{q}$, then p necessarily needs to equal q. In particular, this means that the smallest integer K for which $a^K \equiv 1 \pmod{q}$ must be of the form n/q^j for some integer j. However, we also have $a^{q-1} \equiv 1 \pmod{q}$, and hence $n/q^j = K \mid q-1$. It follows that q must be the largest prime factor of n (as otherwise n/q^j has a prime factor larger than $q-1$, meaning it cannot divide $q-1$), and consequently if $n = q^j \cdot R$ for some integer term R, we have $R \mid q-1$.

To show $q^2 \nmid \Phi_a(x)$ for $q > 2$, it suffices to show $q^2 \nmid \dfrac{a^n-1}{a^{n/p}-1} = \dfrac{c^p-1}{c-1}$. If we put $d = c-1 = a^{n/p}-1$, then clearly $q \mid d$, and we have

$$\frac{c^q-1}{c-1} = \frac{(d+1)^q-1}{d} = \sum_{k=1}^{q} \binom{q}{k} d^{k-1} \equiv q \not\equiv 0 \pmod{q^2}$$

and thus $q^2 \nmid \Phi_a(x)$.

In the case $q = 2$ and $n > 2$, it must be that $n = 2^k$ for some k (since $n = 2^a \cdot R$ where $R \mid q-1 = 1$, and so $R = 1$) and thus $n \geqslant 4$. It suffices to show $4 \nmid \Phi_n(a)$, or $4 \nmid \frac{a^n-1}{a^{n/2}-1} = a^{n/2}+1 = (a^{n/4})^2+1$. However, it is well known $4 \nmid x^2+1$ for any integer x, and hence we have proven **(b)**.

It turns out that **(c)** is a simple consequence of **(a)** and **(b)**; every prime $p \mid \Phi_n(a)$ must satisfy $p = q$, and so it must be of the form q^ℓ. For $n \geqslant 3$, we must have $\ell = 1$ since $q^2 \nmid \Phi_a(x)$. $\square$

Now, we use this lemma to prove a very powerful theorem, called **Zsigmondy's Theorem**. This theorem, whilst usually acceptable in an Olympiad proof, has its use often looked down on as it is extremely powerful and is often an overkill of an otherwise elementary problem. However, using the theory of Cyclotomic Polynomials, we can actually prove this theorem:

Problem 6.1: Zsigmondy's Theorem for $b = 1$.

Let $a, n > 1$ be integers. Then, there exists a prime divisor $q \mid a^n - 1$ such that $q \nmid a^k - 1$ for each $1 \leqslant k \leqslant n$, except in the following cases:

(a) $n = 2$ and $a = 2^T - 1$, for some $T \geqslant 2$;

(b) $n = 6$ and $a = 2$.

Proof. Well obviously if either condition **(a)** or **(b)** holds then there are no primes q satisfying the conditions (thus being the special cases). Hence, we shall prove there are no more counterexamples to the statement.

For $n = 2$, the Lemma 6.1.2 shows that $a+1 = \Phi_2(a) = q^\ell$, and furthermore $2 = n = q^a \cdot R$ which implies $q = 2$. This means $a = 2^\ell - 1$ for some ℓ, which works (and thus satisfies **(a)**).

Otherwise, we assume $n \geqslant 3$. Assume there are no Zsigmondy Primes: then Lemma 6.1.2 shows that $\Phi_n(a) = q$ must be a prime number. However, letting $n = q^j \cdot R$, we have

$$\Phi_n(a) = \Phi_{q^j \cdot R}(a) = \frac{\Phi_R(a^{q^j})}{\Phi_R(a^{q^{j-1}})} = \frac{\Phi_R(b^q)}{\Phi_R(b)} \geqslant \left(\frac{b^q-1}{b+1}\right)^{\varphi(R)} \geqslant \left(b^{q-2}(b-1)\right)^{\varphi(R)}$$

where we have let $b = a^{q^{j-1}}$ and also used the inequality from Lemma 6.1.1, alongside $b^q - 1 \geqslant b^{q-2}(b^2-1)$. Since we have $q = \Phi_n(a)$, we have

$$q > \left(b^{q-2}(b-1)\right)^{\varphi(R)}.$$

However, for $p \geqslant 5$, this inequality fails since $b^{q-2} > q$ for any positive integer $b \geqslant 2$; thus, we must have $q = 3$. However, then we have

$$3 > (b(b-1))^{\varphi(R)},$$

which yields $\varphi(R) = 1$ (hence $R = 1, 2$), and $b = 2$ for which $b = a^{q^{j-1}}$ forces $j = 1$ and $a = 2$ as well. Since we had $n = q^j \cdot R$, it follows that either $n = 3$ or $n = 6$. For $n = 3$, the statement holds for the required $q = 3$ and $a = 2$, since $a^n - 1 = 7$ has a Zsigmondy prime 7 which does not divide any $a^k - 1$ for each $k < n$. On the other hand, $n = 6$ corresponds to the other exception as per **(b)**.

Hence, with all cases resolved, we have proven Zsigmondy's Theorem. □

7 Other Examples of Cyclotomic Polynomials in Olympiad NT

7.1 Infinitude of Primes of Certain Types

We all know Euclid's proof of the infinitude of primes: suppose there are only finitely many of them, call them $p_1 < p_2 < \cdots < p_n$: the the number $N = p_1 p_2 \ldots p_n + 1$ must have a prime factorisation, but none of these prime factors can be p_i, which is a contradiction.

In the same way, we could attempt to prove some cases of Dirichlet's Theorem, a generalisation that there are infinitely many prime numbers of the form $an + b$, where $\gcd(a, b) = 1$.[1] It turns out that for the case $b = 1$, we can imitate Euclid's proof to derive a similar result.

Problem 7.1

Let $a \geqslant 2$ be an integer. Then, there are infinitely many primes of the form $an + 1$ for integer n.

Proof. Suppose otherwise, that there are at most finitely many primes of the form $an + 1$, and let these primes be $p_1 < p_2 < \cdots < p_N$. Consider an integer k large enough such that

$$\Phi_a\left((a \cdot p_1 p_2 \ldots p_N)^k\right) > 1.$$

Clearly, such a k must exist since $\Phi_a(x)$ is monic and thus has positive leading coefficient. Now, consider any prime $q \mid \Phi_a\left((a \cdot p_1 p_2 \ldots p_N)^k\right)$: it follows from earlier properties that $q \equiv 1 \pmod{a}$ or $q \mid a$. The first case fails, because that would imply $q = p_i$ for some i, but $p_i \mid \Phi_a\left((a \cdot p_1 p_2 \ldots p_N)^k\right) \mid \left((a \cdot p_1 p_2 \ldots p_N)^k\right)^a - 1$ is a contradiction as this implies $p_i \mid 1$.

If instead we have $q \mid a$, then this also fails since we have $q \mid \Phi_a\left((a \cdot p_1 p_2 \ldots p_N)^k\right) \mid \left((a \cdot p_1 p_2 \ldots p_N)^k\right)^a - 1$ which contradicts the assumed $q \mid a$. □

Fun fact. For a given (a, b), define a **Euclidean Polynomial** $h(T) \in \mathbb{Z}[T]$ to be a nonconstant polynomial for which any factor $p \mid h(n)$ satisfies, with at most finitely many exceptions, either $p \equiv 1 \pmod{m}$ or $p \equiv b \pmod{m}$, and **infinitely many primes of the latter type occur.** For instance, the Cyclotomic Polynomial $\Phi_d(n)$ is a Euclidean Polynomial for $(a, 1)$, $a \geqslant 3$, since any $p \mid \Phi_n(T)$ implies $p \equiv 1 \pmod{a}$, or $p \mid a$. Other examples of Euclidean Polynomials are as follows:

- $5n + 4$: $p \mid h(T) = 2T^2 - 5$ satisfies either $p \equiv 1, 4 \pmod{5}$, or $p = 2, 5$.
- $8n + 7$: $p \mid h(T) = T^2 - 2$ satisfies either $p = 1, 7 \pmod{8}$ or $p = 2, 3$

[1] The stronger form of Dirichlet states that if $\pi_{a,b}(x)$ is the number of such primes at most x, then $\pi_{a,b}(x) \sim \frac{x}{\log x \cdot \varphi(a)}$.

- $12n+7$: $p \mid h(T) = T^2+3$ satisfies either $p \equiv 1, 7 \pmod{12}$ or $p = 2, 3, 5, 13$
- $12n+11$: $p \mid h(T) = 3T^2-4$ satisfies either $p \equiv 1, 11 \pmod{12}$, or $p = 2$.

Now, why is this called a Euclidean polynomial? Simply because, having such a polynomial for a given (a, b) gives us a proof that there are infinitely many primes of the form $an+b$ using a method very similar to that utilised by Euclid's proof of the infinitude of primes, and is basically the minimum requirement for a polynomial for which this can be achieved. As Dirichlet's theorem is not elementary to prove, it may be of interest to see for which pairs (a, b) does a Euclidean polynomial $h(T)$ exist.

In **1912**, Schur proved that if $b^2 \equiv 1 \pmod{a}$ for some $a, b \geqslant 1$, a Euclidean polynomial exists for (a, b).

In **1988**, Murty proved that if a Euclidean polynomial exists for (a, b), then we must have $b^2 \equiv 1 \pmod{a}$.

In particular, this means that it is not possible to prove that there are infinitely many primes of the form $5n+2$ using a method akin to that of Euclid (!!)

7.2 Other problems

Problem 7.2: IMO Shortlist 2002 N3 Generalisation

Let $p_1, p_2, \ldots, p_n >\!\!\geqslant 5$ be **distinct** prime numbers. Show that

$$2^{p_1 p_2 \cdots p_n} + 1$$

has at least $2^{2^{n-1}}$ distinct divisors.

Proof. It suffices to show that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 2^{n-1} **distinct** pairwise coprime divisors, which would suffices since any subset of them will multiply to a different divisor.

We have

$$2^P + 1 = \frac{2^{2P}-1}{2^P-1} = \frac{\prod_{D \mid 2P} \Phi_D(2)}{\prod_{d \mid P} \Phi_d(2)} = \frac{\left(\prod_{D \mid P} \Phi_{2D}(2)\right)\left(\prod_{D \mid P} \Phi_D(2)\right)}{\prod_{d \mid P} \Phi_d(2)} = \prod_{d \mid P} \Phi_{2d}(2)$$

where P is the product $p_1 \ldots p_n$, since P is odd (and hence we can split 2 off the product without causing trouble). Now, we know that if $\gcd(\Phi_a(x), \Phi_b(x)) > 1$ for some integers a, b, x, then a/b must be a power of a prime. Hence, it suffices to find 2^{p-1} factors of the product which are coprime to each other.

However, this is obvious since we can simply take each term $\Phi_{2A}(2)$ where A is composed of an **odd** number of primes $p_1, \ldots, p_n$, and thus these numbers will have no common factor. There are also 2^{n-1} of them available to choose, and thus we have 2^{n-1} prime factors of $2^P - 1$ which are pairwise coprime. □

Problem 7.2: IMO Shortlist 2006 N5

Show that there are no integer solutions (x, y) to the equation

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

Proof. Notice that $\dfrac{x^7-1}{x-1}$ is the 7-th cyclotomic polynomial $\Phi_7(x)$. It follows that any $p \mid \Phi_7(x)$ satisfies either $p \equiv 1 \pmod{7}$ or $p = 7$, and thus **all its factors are** $\equiv 0, 1 \pmod{7}$. Since we have the factorisation $y^5 - 1 = (y-1)(y^4+y^3+y^2+y+1)$, it follows $y - 1 \mid \Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1$, which implies $y - 1 \equiv 0, 1 \pmod{7}$, and hence $y \equiv 1, 2 \pmod{7}$.

Since $y^4 + \cdots + y + 1$ is also a factor of $\Phi_7(x)$, it follows it must also be $\equiv 0, 1 \pmod 7$. However, for $y \equiv 1$ we get $y^4 + \cdots + y + 1 \equiv 5 \not\equiv 0, 1 \pmod 7$. A similar contradiction arises with $y \equiv 2$ which gives $y^4 + \cdots + y + 1 \equiv 3 \not\equiv 0, 1 \pmod 7$. It follows there are no integer solutions to the equation. $\square$

Problem 7.2: Existence of Generators modulo p

Let $p \geqslant 3$ be prime. Show that there exists an integer g for which the set

$$1, g, g^2, \ldots, g^{p-2}$$

forms a **complete residue set modulo** p.

Proof. Recall the well-known identity $X^p - x \equiv X(X-1)(X-2)\ldots(X-(p-1)) \pmod p$ (as a consequence of Fermat's Little Theorem and Lagrange's Theorem in $\mathbb{Z}_p$). However, we also have the factorisation

$$X^p - X = X(X-1)(X-\zeta)(X-\zeta^2)\ldots(X-\zeta^{p-2})$$

where ζ is a primitive root of unity. Hence, treating the ζ's as elements of $\mathbb{Z}_p$, it follows that $1, \zeta, \ldots, \zeta^{p-2}$ form a complete residue set modulo p. Then simply take $g = \zeta$. $\square$

8 Other Interesting Facts about Cyclotomic Polynomials

- **Gauss' Cyclotomic Formula.** Let n be an odd, squarefree integer. Then, there exists polynomials $R(X), S(X) \in \mathbb{Z}[X]$ for which

$$4 \cdot \Phi_n(x) = R(x)^2 - (-1)^{\frac{n-1}{2}} n \cdot S(x)^2$$

- **Lucas' Cyclotomic Formula.** Let n be an odd, squarefree integer. Then, there exists polynomials $R_1(X), S_1(X) \in \mathbb{Z}[X]$ for which

$$\Phi_n(x) = R_1(x)^2 - (-1)^{\frac{p-1}{2}} px \cdot S_1(x)^2.$$

8.1 Special Values of $\Phi_n(x)$

- Define the **Von Mangoldt Function** $\Lambda(n)$ as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \\ 0 & \text{otherwise.} \end{cases}$$

  Then, we have $\log(\Phi_n(1)) = \Lambda(n)$ for each $n \geqslant 1$.

- We have $\Phi_1(-1) = -2$ and $\Phi_2(-1) = 0$ (well duh obviously). For each $n = 2 \cdot p^k$, we have $\Phi_n(-1) = p$, and $\Phi_n(-1) = 1$ in every other case ($n \neq 1, 2, 2 \cdot p^k$).

- For each integer $n \geqslant 3$, we have $\Phi_n'(1) = \frac{\varphi(n)}{2}\Phi_n(1)$ and $\Phi_n'(-1) = -\frac{\varphi(n)}{2}\Phi_n(-1)$.

- The coefficient of $x^{\varphi(n)-1}$ in the polynomial $\Phi_n(x)$ is $-\mu(n)$. In general, there does not exist simple formulas for coefficients of $\Phi_n(x)$ other than this one, the leading coefficient (1), constant coefficient (1) and the coefficient of x ($-\mu(n)$).

- The derivative of $\Phi_n(x)$ as a holomorphic function in $\mathbb{C}[x]$ is never zero on the unit circle.

- **(Kronecker's Polynomial Theorem.)** Let P be a monic polynomial with integer coefficients, all of whose roots lie on the unit circle. Then P is expressible as the product of cyclotomic polynomials.

9 Problem Section

1. Prove that none of the numbers in the sequence $1001, 1001001, 1001001, \ldots$ are prime numbers.
2. **(Korea 2010.)** Prove that $7^{2^{20}} + 7^{2^{19}} + 1$ has at least 21 distinct prime divisors.
3. Show that if $4^n + 2^n + 1$ is a prime, then $n = 3^k$ for some positive integer k.
4. Show that if p is an odd prime number, then $\Phi_{2p}(X) = \Phi_p(-X)$.
5. **(2nd OAO.)** Given a positive integer $n \geqslant 2$, define $P(x) = \prod_{i=1}^{n} \frac{x^{n+i} - 1}{x^i - 1}$. Prove that $P(x) \in \mathbb{Z}[x]$.
6. **(Vietnam TST 1997.)** The function $\mathbb{Z}^+ \to \mathbb{Z}$ is defined recursively by $f(0) = 2$, $f(1) = 503$ and for each $n \geqslant 1$,
$$f(n+2) = 503f(n+1) - 1996f(n).$$
Furthermore, let $s_1, s_2, \ldots, s_k \geqslant k$ be arbitrary integers, and let $p(s_i)$ denote an arbitrary prime divisor of $f(2^{s_i})$ for each $i \leqslant k$. Prove that, for any $T \leqslant k$, we have $2^T \mid \sum_{j=1}^{k} p(s_j)$ if and only if $2^T \mid k$.
7. Show that every integer appears as the coefficient of some Cyclotomic Polynomial.
8. **(Belarus TST 2017.)** Prove (**without Dirichlet's Theorem**) that for any positive integers a and b, there exist infinitely many prime numbers p for which $ap + b$ is composite.
9. **(USA TST 2012.)** Find all positive integers $a, n \geq 1$ such that for all primes p dividing $a^n - 1$, there exists a positive integer $m < n$ such that $p \mid a^m - 1$.
10. **(Romania TST 2014.)** Let p be an odd prime number. Determine all pairs of polynomials f and g from $\mathbb{Z}[X]$ such that
$$f(g(X)) = \sum_{k=0}^{p-1} X^k = \Phi_p(X).$$
11. **(Iran TST 2013.)** Do there exist natural numbers a, b and c such that $a^2 + b^2 + c^2$ is divisible by $2013(ab + bc + ca)$?
12. **(IMO Shortlist 1992.)** Show that the number $\frac{5^{125} - 1}{5^{25} - 1}$ is **not** a prime number.
13. **(USAMO 2007.)** Prove that for every nonnegative integer n, the number $7^{7^n} + 1$ is the product of at least $2n + 3$ (**not necessarily distinct**) primes.
14. Prove that there exist infinitely many integers N for which all prime factors of $N^2 + N + 1$ does not exceed $N^{1/2019}$.
15. Let $a \geqslant 2$ be an integer. Prove that there are infinitely many integers n for which $a + n \mid a^n + 1$.
16. **(Romania TST 2009.)** Show that there are infinitely many pairs of prime numbers (p, q) such that $p \mid 2^{q-1} - 1$ and $q \mid 2^{p-1} - 1$.
17. **(Croatia TST 2013.)** Prove that there exist infinitely many $n \in \mathbb{N}$ that have more than two distinct prime divisors, such that $n \mid 2^n - 8$.

18. **(All–Russian Olympiad 2006.)** Let $P(x) = x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_1x + c_0$ be an integer polynomial whose coefficients are odd. Suppose $P(x) \mid (x+1)^n - 1$ for some integer n.

    Show that $k+1 \mid n$.

19. **(IMO Shortlist 2017 N5.)** Find all pairs (p, q) of prime numbers which $p > q$ and

$$\frac{(p+q)^{p+q}(p-q)^{p-q} - 1}{(p+q)^{p-q}(p-q)^{p+q} - 1}$$

    is an integer.

20. **(Iran 2011.)** Let n be a positive integer not divisible by 3. Prove that the number

$$(n^{2n} + n^n + n + 1)^{2n} + (n^{2n} + n^n + n + 1)^n + 1$$

    has at least $2 \cdot \sigma(n)$ distinct prime factors, where $\sigma(n)$ is the number of positive divisors of n.

21. **(China TST 2004.)** Let u be a fixed positive integer. Prove that the equation $n! = u^\alpha - u^\beta$ has a finite number of solutions (n, α, β).

22. **(China TST 2009.)** Let $f(x)$ denote a polynomial of degree n, all of whose coefficients are ± 1 and satisfying $(x-1)^m \mid f(x)$, but $(x-1)^{m+1} \nmid f(x)$.

    Show that if $m \geqslant 2^k$ for some integer $k \geqslant 2$, then $n \geqslant 2^{k+1} - 1$.

23. **(China TST 2009.)** Find all the pairs of integers (a, b) satisfying $ab(a-b) \neq 0$ such that there exists a subset $Z_0 \subseteq Z$, for any integer n, exactly one among three integers $n, n+a, n+b$ belongs to Z_0.

24. **(Challenge!!)** Let $\Phi_n(x)$ denote the nth cyclotomic polynomial in x, and $\varphi(n)$ and $\mu(n)$ defined conventionally. Denote $P(n) = \prod_{p \in \mathbb{P}} \frac{p^{\varphi(n)}}{\Phi_n(p)}$. Prove that:

    - $\mu(n) = 1$ iff $P(n)$ diverges.
    - $\mu(n) = 0$ iff $P(n)$ converges to a positive finite real.
    - $\mu(n) = -1$ iff $P(n)$ converges to 0.