# CYCLOTOMIC POLYNOMIALS

Contents



## 1. The derivative and repeated factors

The usual definition of the derivative in calculus involves the nonalgebraic notion of *limit* that requires a field such as $\mathbb{R}$ or $\mathbb{C}$ (or others) where limits are sensible for analytic reasons.

However, polynomial differentiation is an algebraic notion over any field. One can simply define the polynomial derivative to be as it is from calculus,

$$D\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n-1} (i+1)a_{i+1}X^i.$$

Alternatively (and working a bit casually here), one can introduce a second indeterminate $T$ and observe that the polynomial

$$f(X+T) - f(X) \in k[X][T]$$

is satisfied by $T = 0$, and so it takes the form

$$f(X+T) - f(X) = T\,g(X)(T), \quad g \in k[X][T].$$

The derivative of $f$ is then defined as the $T$-constant term of $g(X)(T)$,

$$f'(X) = g(X)(0) \in k[X].$$

The familiar facts that the derivative of $X^i$ is $iX^{i-1}$ for $i \geq 0$, that differentiation is linear, i.e., $(f+cg)' = f' + cg'$, and that differentiation satisfies the product rule, i.e., $(fg)' = fg' + f'g$, can be rederived from this purely algebraic definition of the derivative. In fact, yet a third approach to the polynomial derivative is to define $X' = 1$ and then stipulate that differentiation is the unique extension of this rule that is linear and satisfies the product rule. (For example, $1 = X' = (X \cdot 1)' = X \cdot 1' + X' \cdot 1 = X \cdot 1' + 1$, so $1' = 0$.)

**Proposition 1.1.** *Let $k$ be a field, and let $f \in k[X]$ be a polynomial. Then:*

$$\textit{If } \gcd(f, f') = 1 \textit{ then } f \textit{ has no repeated factors.}$$

*Proof.* To establish the contrapositive, suppose that $f = g^2 h$ in $k[X]$. The product rule gives

$$f' = 2gg'h + g^2 h' = g(2g'h + gh').$$

Thus $g \mid f'$, and so $g \mid \gcd(f, f')$, and so $\gcd(f, f') \neq 1$. □

## 2. Definition of the cyclotomic polynomials

Working in $\mathbb{Z}[X]$ we want to define *cyclotomic polynomials*

$$\Phi_n, \quad n \in \mathbb{Z}_{\geq 1}.$$

Provisionally, define

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}, \quad n \geq 1.$$

Here it is understood that for $n = 1$ the denominator is the empty product, i.e.,

$$\Phi_1(X) = X - 1.$$

Certainly each $\Phi_n$ lies in the quotient field $\mathbb{Z}(X)$ of $\mathbb{Z}[X]$ but we will show considerably more. In fact, always $\Phi_n$ lies in $\mathbb{Z}[X]$ and is irreducible. For example, repeatedly using the identity $X^n - 1 = \prod_{d|n} \Phi_d(X)$ in various ways,

$$\begin{aligned}
\Phi_2(X) &= \frac{X^2 - 1}{X - 1} = X + 1 = -\Phi_1(-X), \\
\Phi_p(X) &= \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1, && p \text{ prime}, \\
\Phi_{p^e}(X) &= \frac{X^{p^e} - 1}{X^{p^{e-1}} - 1} = \Phi_p(X^{p^{e-1}}), && p \text{ prime}, \\
\Phi_{2^d p}(X) &= \frac{X^{2^d p} - 1}{(X^{2^{d-1} p} - 1)\Phi_{2^d}(X)} = \frac{X^{2^{d-1} p} + 1}{X^{2^{d-1}} + 1} = \Phi_p(-X^{2^{d-1}}), && p > 2 \text{ prime}, \\
\Phi_{2^d p^e}(X) &= \frac{X^{2^d p^e} - 1}{(X^{2^{d-1} p^e} - 1)\Phi_{2^d}(X)\Phi_{2^d p}(X) \cdots \Phi_{2^d p^{e-1}}(X)} \\
&= \frac{X^{2^{d-1} p^e} + 1}{-\Phi_1(-X^{2^{d-1}})\Phi_p(-X^{2^{d-1}}) \cdots \Phi_{p^{e-1}}(-X^{2^{d-1}})} && \text{(induction on } e\text{)} \\
&= \frac{X^{2^{d-1} p^e} + 1}{X^{2^{d-1} p^{e-1}} + 1} = \Phi_p(-X^{2^{d-1} p^{e-1}}), && p > 2 \text{ prime}, \\
\Phi_{15}(X) &= \frac{(X^{15} - 1)}{(X^5 - 1)\Phi_3(X)} = \frac{X^{10} + X^5 + 1}{X^2 + X + 1} \\
&= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1, \\
\Phi_{2m}(X) &= \Phi_m(-X), && m \text{ odd}, \\
\Phi_{21}(X) &= \frac{X^{21} - 1}{(X^7 - 1)\Phi_3(X)} = \frac{X^{14} + X^7 + 1}{X^2 + X + 1} \\
&= X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1.
\end{aligned}$$

These identities give $\Phi_n$ for all $n \leq 32$. They also suggest that all cyclotomic polynomials $\Phi_n$ for $n > 1$ have constant term 1, and this is readily shown by induction on $n$.

As an aside, invoking some ideas from outside this course, the relation

$$X^n - 1 = \prod_{d|n} \Phi_d(X), \quad n \in \mathbb{Z}_{\geq 1}$$

gives in consequence a closed form expression for the cyclotomic polynomials,

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}, \quad n \in \mathbb{Z}_{\geq 1},$$

in which $\mu$ is the Möbius function of elementary number theory,

$$\mu(\prod_{i=1}^{g} p_i^{e_i}) = \begin{cases} (-1)^g & \text{if } e_i = 1 \text{ for each } i, \\ 0 & \text{if } e_i \geq 2 \text{ for some } i. \end{cases}$$

Here it is understood that terms $p^0$ are omitted from the product in the previous display, and that we view 1 as the empty product of prime powers, so that the formula gives $\mu(1) = (-1)^0 = 1$. The formula for the cyclotomic polynomial $\Phi_n(X)$ as a product of polynomials $X^d - 1$ and their reciprocals, in consequence of the formula for the polynomial $X^n - 1$ as a product of cyclotomic polynomials $\Phi_d(X)$, is an instance of *Möbius inversion*. For more on these matters, see

`http://people.reed.edu/~jerry/361/lectures/lec03.pdf`.

We make two observations about the polynomial $X^n - 1$ where $n \in \mathbb{Z}_{\geq 1}$.

- $X^n - 1$ has no repeated factors in $\mathbb{Z}[X]$ for any $n \in \mathbb{Z}_{\geq 1}$. Indeed, working in the larger ring $\mathbb{Q}[X]$ we have

$$(X^n - 1) - (1/n)X \cdot (X^n - 1)' = (X^n - 1) - (1/n)X \cdot nX^{n-1} = -1 \in \mathbb{Q}^\times,$$

  so that $\gcd(X^n - 1, (X^n - 1)') = 1$. As explained above, $X^n - 1$ therefore has no repeated factors in $\mathbb{Q}[X]$, much less in $\mathbb{Z}[X]$. For future reference, we note that this argument also works in $(\mathbb{Z}/p\mathbb{Z})[X]$ where $p$ is prime, so long as $p \nmid n$.
- For any $n, m \in \mathbb{Z}_{\geq 1}$,

$$\gcd(X^n - 1, X^m - 1) = X^{\gcd(n,m)} - 1.$$

  Indeed, taking $n > m$, the calculation

$$X^n - 1 - X^{n-m}(X^m - 1) = X^{n-m} - 1$$

  shows that

$$\langle X^n - 1, X^m - 1 \rangle = \langle X^{n-m} - 1, X^m - 1 \rangle,$$

  and, letting $n = qm + r$ where $0 \leq r < n$ and repeating the calculation $q$ times,

$$\langle X^n - 1, X^m - 1 \rangle = \langle X^r - 1, X^m - 1 \rangle.$$

  That is, carrying out the Euclidean algorithm on $X^n - 1$ and $X^m - 1$ in $\mathbb{Q}(X)$ slowly carries out the Euclidean algorithm on $n$ and $m$ in $\mathbb{Z}$. (If the Euclidean algorithm on $n$ and $m$ takes $k$ division-steps, with quotients $q_1$ through $q_k$, then the Euclidean algorithm on $X^n - 1$ and $X^m - 1$ takes $q_1 + \cdots + q_k$ steps.) The result follows.

Recall the definition

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}, \quad n \geq 1.$$

Note that

- $\Phi_1 \in \mathbb{Z}[X]$, and
- (vacuously) no $\Phi_k$ and $\Phi_m$ for distinct $k, m < 1$ share a factor.

The two bullets are the base case of an induction argument. Fix some $n \geq 1$ and assume that

- all $\Phi_m$ for $m \leq n$ lie in $\mathbb{Z}[X]$, and
- no $\Phi_k$ and $\Phi_m$ for distinct $k, m < n$ share a factor.

Let $m < n$, and let $k = \gcd(m, n) \leq m < n$. Any common factor of $\Phi_m$ and $\Phi_n$ is a common factor of $X^m - 1$ and $X^n - 1$, hence a factor of $X^k - 1$. However, the calculation

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)} \left| \frac{X^n - 1}{\prod_{\substack{d|n \\ d\leq k}} \Phi_d(X)} = \frac{X^n - 1}{X^k - 1} \right.$$

shows that no factor of $\Phi_n$ is a factor of $X^k - 1$. In sum, the strict inequality in the second bullet weakens: no $\Phi_k$ and $\Phi_m$ for distinct $k, m \leq n$ share a factor. Equivalently, no $\Phi_k$ and $\Phi_m$ for distinct $k, m < n + 1$ share a factor.

Now, for each proper divisor $d$ of $n + 1$, each factor of $\Phi_d$ is a factor of $X^d - 1$ in $\mathbb{Z}[X]$, hence a factor of $X^{n+1} - 1$ in $\mathbb{Z}[X]$. And the product

$$\prod_{\substack{d|n+1 \\ d<n+1}} \Phi_d(X)$$

contains no repeat factors of $X^{n+1} - 1$. Thus $\Phi_{n+1} \in \mathbb{Z}[X]$. This completes the induction step:

- all $\Phi_m$ for $m \leq n + 1$ lie in $\mathbb{Z}[X]$, and
- no $\Phi_k$ and $\Phi_m$ for distinct $k, m < n + 1$ share a factor.

By induction, $\Phi_n \in \mathbb{Z}[X]$ for all $n \in \mathbb{Z}_{\geq 1}$, and no two $\Phi_n$ share a factor.

The totient function identity $\sum_{d|n} \phi(d) = n$ quickly combines with the formula $\prod_{d|n} \Phi_d(X) = X^n - 1$ and a little induction to show that the degree of the cyclotomic polynomial is the totient function of its index,

$$\boxed{\deg(\Phi_n) = \phi(n), \quad n \geq 1.}$$

If we view the integers $\mathbb{Z}$ as a subring of the complex number field $\mathbb{C}$ then the $n$th cyclotomic polynomial factors as

$$\Phi_n(X) = \prod_{\substack{0\leq e<n \\ \gcd(e,n)=1}} (X - \zeta_n^e), \quad \text{where } \zeta_n = e^{2\pi i/n}.$$

Indeed, the formula produces the monic polynomial in $\mathbb{C}[X]$ whose roots are the complex numbers $z$ such that $z^n = 1$ but $z^m \neq 1$ for all $1 \leq m < n$. Indeed, the word *cyclotomic* literally refers to dividing the circle.

The previous paragraph notwithstanding, we do not want to think of the cyclotomic polynomials innately in complex terms, because the integers are also compatible with other algebraic structures that are incompatible with the complex numbers

in turn. Rather, we want to think of the roots of $\Phi_n$ as the elements having order exactly $n$ in whatever environment is suitable. In the next example, the environment is $\mathbb{Z}/p\mathbb{Z}$ where $p$ is a prime that does not divide $n$. Earlier we observed that our arguments apply in this setting as well.

## 3. Application: an infinite congruence class of primes

**Theorem 3.1.** *Let $n > 1$ be a positive integer. There exist infinitely many primes $p$ such that $p = 1 \bmod n$.*

*Proof.* Suppose that the only primes equal to 1 mod $n$ are $p_1, \ldots, p_t$. The idea is to find some other prime $p$ and some integer $a$ such that the multiplicative order of $a$ modulo $p$ is $n$; this holds if $\Phi_n(a) = 0 \bmod p$ and $p \nmid n$. Because $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, we thus have $n \mid p-1$, i.e., $p = 1 \bmod n$. So the original list of such primes was not exhaustive after all, and hence there is no such finite list.

To carry out the idea, introduce an unbounded family of positive integers,

$$a_\ell = \ell \cdot n \cdot p_1 \cdots p_t, \quad \ell = 1, 2, 3, \ldots .$$

Then $\Phi_n(a_\ell) > 1$ for all large enough $\ell$. Take such $\ell$, and with $\ell$ chosen, simply write $a$ for $a_\ell$. The condition $\Phi_n(a) = 1 \bmod a$ makes $\Phi_n(a)$ coprime to $a$. Take any prime divisor $p$ of $\Phi_n(a)$. Thus $p \notin \{p_1, \ldots, p_t\}$, and

$$\Phi_n(a) = 0 \bmod p \quad \text{and} \quad p \nmid n.$$

As noted above, the display says that the multiplicative order of $a$ modulo $p$ is $n$ and consequently the proof is complete. □

## 4. Application: Wedderburn's theorem

The cyclotomic polynomials combine with the counting formulas of group actions to provide a lovely proof of the following result.

**Theorem 4.1.** *Let $D$ be a finite division ring, i.e., a field except that multiplication might not commute. Then $D$ is a field.*

*Proof.* The center of $D$ is a finite field $k$; let $q$ denote its order. Since $D$ is a vector space over $k$, the order of $D$ is therefore $q^n$ for some $n$. We want to show that $n = 1$.

For any $x \in D$, the centralizer

$$D_x = \{y \in D : yx = xy\}$$

is again a division ring containing $k$, and its multiplicative group $D_x^\times$ is a subgroup of $D^\times$. Hence $|D_x| = q^{n_x}$ where $q^{n_x} - 1$ divides $q^n - 1$, so that $n_x$ divides $n$. And if $x \notin k$ then the divisibilities are proper. Let $D^\times$ act on $D$ by conjugation. The class formula gives

$$|D| = |k| + \sum_x |D^\times|/|D_x^\times|$$

where the sum adds the sizes of the nontrivial orbits, or

$$q^n = q + \sum_x \frac{q^n - 1}{q^{n_x} - 1}$$

summing over representatives of nontrivial orbits.

Recall that each $n_x$ arising from the sum is a proper divisor of $n$. The formulas

$$\Phi_n(q) \Big| \prod_{d|n} \Phi_d(q) = q^n - 1,$$
$$\Phi_n(q) \Big| \prod_{\substack{d|n \\ d\nmid n_x}} \Phi_d(q) = \frac{q^n-1}{q^{n_x}-1},$$

(in which all $\Phi_*(q)$-values are integers) show that $\Phi_n(q)$ divides the left side and each summand in the formula

$$q^n - 1 = q - 1 + \sum_x \frac{q^n-1}{q^{n_x}-1}.$$

Consequently $\Phi_n(q)$ divides $q-1$.

But viewing $\mathbb{Z}$ as a subring of the complex number system $\mathbb{C}$ lets us show that $\Phi_n(q)$ can not divide $q-1$ unless $n=1$,

$$|\Phi_n(q)|^2 = \prod_{\substack{0\le k<n \\ \gcd(k,n)=1}} \big((q-\cos(2\pi k/n))^2 + (\sin(2\pi k/n))^2\big)$$

If $n>1$ then each term of the product is greater than $(q-1)^2$, and so $|\Phi_n(q)| > q-1$. This completes the proof. □

## 5. Irreducibility of prime-power cyclotomic polynomials

The irreducibility of prime-power cyclotomic polynomials $\Phi_{p^e}(X)$ in $\mathbb{Z}[X]$ (and hence in $\mathbb{Q}[X]$) can be established by an argument set entirely in $\mathbb{Z}[X]$ and its quotient-structures.

To avoid interrupting the pending argument, we establish a small preliminary result.

**Lemma 5.1.** *Let $p$ be prime. For all $\varepsilon \in \mathbb{Z}_{\ge 0}$, $(X-1)^{p^\varepsilon} = X^{p^\varepsilon} - 1$ in $(\mathbb{Z}/p\mathbb{Z})[X]$.*

*Proof.* The result is immediate if $\varepsilon = 0$. And for the induction step, working in $(\mathbb{Z}/p\mathbb{Z})[X]$,

$$(X-1)^{p^{\varepsilon+1}} = ((X-1)^{p^\varepsilon})^p = (X^{p^\varepsilon}-1)^p = \sum_{i=0}^{p} \binom{p}{i} X^{ip^\varepsilon}(-1)^{p-i} = X^{p^{\varepsilon+1}} - 1,$$

because the binomial coefficients for $1 \le i \le p-1$ vanish modulo $p$ and because $(-1)^p = -1 \bmod p$ for all $p$, including $p=2$. □

The result $(A+B)^p = A^p + B^p$ in characteristic $p$ is sometimes given names such as *the freshman's dream*. Such names are, in this author's opinion, pejorative distractions from the point that raising to the $p$th power is a homomorphism in characteristic $p$; this has enormous consequences with no counterpart in characteristic 0.

Again let $p$ be prime, and let $e \ge 1$. We show that the cyclotomic polynomial $\Phi_{p^e}$ is irreducible in $\mathbb{Z}[X]$, thereby making it irreducible in $\mathbb{Q}[X]$ by Gauss's Lemma. From the relation $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}) = (X^{p^e}-1)/(X^{p^{e-1}}-1)$ we have

$$(X^{p^{e-1}}-1)\Phi_{p^e}(X) = X^{p^e} - 1 \quad \text{in } \mathbb{Z}[X],$$

from which, by the lemma,

$$(X-1)^{p^{e-1}}\Phi_{p^e}(X) = (X-1)^{p^e} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X],$$

and therefore, recalling that $p^e - p^{e-1} = \phi(p^e)$,

$$\Phi_{p^e}(X) = (X-1)^{\phi(p^e)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

Also,

$$\Phi_{p^e}(1) = \Phi_p(1^{p^{e-1}}) = \Phi_p(1) = p \neq 0 \quad \text{in } \mathbb{Z}/p^2\mathbb{Z}.$$

The previous two displays show precisely that $\Phi_{p^e}(X)$ is irreducible in $\mathbb{Z}[X]$ by Schönemann's Criterion (below). Hence $\Phi_{p^e}(X)$ is irreducible in $\mathbb{Q}[X]$ by Gauss's Lemma.

**Proposition 5.2** (Schönemann's Criterion, special case)**.** *Let $f(X) \in \mathbb{Z}[X]$ be monic of positive degree $n$. Suppose that for some element $a$ of $\mathbb{Z}$ and some prime $p$ in $\mathbb{Z}$,*

$$f(X) = (X-a)^n \bmod p\mathbb{Z}[X] \qquad \textit{and} \qquad f(a) \neq 0 \bmod p^2.$$

*Then $f(X)$ is irreducible modulo $p^2\mathbb{Z}[X]$ and hence $f(X)$ is irreducible in $\mathbb{Z}[X]$.*

*Proof.* We show the contrapositive statement, arguing that if $f(X)$ is reducible mod $p^2\mathbb{Z}[X]$ then its reduction looks enough like $(X-a)^n$ to force $f(a) = 0 \bmod p^2$. Specifically, suppose that

$$f(X) = f_1(X)f_2(X) \bmod p^2\mathbb{Z}[X].$$

The reduction modulo $p^2$ agrees modulo $p$ with the reduction modulo $p$,

$$f_1(X)f_2(X) = (X-a)^n \bmod p\mathbb{Z}[X],$$

and so, because we may take $f_1(X)$ and $f_2(X)$ to be monic, we have for $i = 1, 2$,

$$f_i(X) = (X-a)^{n_i} \bmod p\mathbb{Z}[X], \quad n_i \in \mathbb{Z}^+;$$

specifically, we have the equality $f_1(X)f_2(X) = (X-a)^n$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ where the polynomials now have their coefficients reduced modulo $p$, and because $(\mathbb{Z}/p\mathbb{Z})[X]$ is a UFD, $f_i(X) = (X-a)^{n_i}$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ for $i = 1, 2$, giving the previous display. In consequence of the display $f_i(a) = 0 \bmod p$ for $i = 1, 2$, and so the first display in the proof gives $f(a) = 0 \bmod p^2$ as desired. □

## 6. Irreducibility of general cyclotomic polynomials

In contrast to the previous section, quickly showing the irreducibility of the general cyclotomic polynomial $\Phi_n(X)$ in $\mathbb{Z}[X]$ requires an argument that extends beyond $\mathbb{Z}$ and $\mathbb{Q}$. Again we establish a preliminary result.

**Lemma 6.1.** *Let $n > 1$ be an integer and let $p \nmid n$ be prime. Then the cyclotomic polynomial $\Phi_n(X)$ has no repeated factors modulo $p$.*

*Proof.* Indeed, $\Phi_n(X)$ divides $X^n - 1$, which is coprime to its derivative $nX^{n-1}$ modulo $p$ because $p \nmid n$. Hence $X^n - 1$ has no repeated factors modulo $p$, and so neither does $\Phi_n(X)$. □

Let $n > 1$, let $\zeta_n = e^{2\pi i/n}$, and let $f(X) \in \mathbb{Z}[X]$ be the monic irreducible polynomial of $\zeta_n$. We have $\Phi_n(X) = f(X)g(X)$ for some $g(X) \in \mathbb{Z}[X]$, and we want to show that $f(X) = \Phi_n(X)$. The complex roots of $\Phi_n(X)$ are the values $\zeta_n^e$ such that $\gcd(e, n) = 1$, and every such root can be obtained from $\zeta_n$ by repeatedly raising to various primes $p \nmid n$. Thus it suffices to show that:

For any root $\rho$ of $f$ and for any prime $p \nmid n$, also $\rho^p$ is a root of $f$.

So, let $\rho$ be a root of $f$ and let $p \nmid n$ be prime. We show that $f(\rho^p) = 0$ by showing that $g(\rho^p) \neq 0$. For, if instead $g(\rho^p) = 0$ then $\rho$ is a root of $g(X^p)$, and so $f(X)$ divides $g(X^p)$ in $\mathbb{Z}[X]$. Letting an overbar denote reduction modulo $p$, $\overline{f}(X)$ divides $\overline{g}(X)^p$ in the UFD $(\mathbb{Z}/p\mathbb{Z})[X]$, and so $\overline{f}(X)$ and $\overline{g}(X)$ share a nontrivial factor $h(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. Thus $h(X)^2$ divides $\Phi_N(X)$ modulo $p$. But this contradicts the lemma, showing that the condition $g(\rho^p) = 0$ is impossible. The argument is complete.

## 7. Factorization of cyclotomic polynomials modulo $p$

**Proposition 7.1.** *Let $p$ be prime. Let $n$ be a positive integer, which takes the form $n = p^\epsilon m$ with $\epsilon \geq 0$ and $p \nmid m$. Let $f$ be the order of $p$ modulo $m$, i.e., $p^f = 1 \bmod m$ but $p^i \neq 1 \bmod m$ for $i = 1, \dots, f-1$, and let $g = \phi(m)/f$ where $\phi$ is Euler's totient function. Then there exist distinct monic irreducible polynomials $\varphi_{1,m}(X), \dots, \varphi_{g,m}(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$, all of degree $f$, such that*

$$\Phi_n(X) = \prod_{i=1}^{g} \varphi_{i,m}(X)^{\phi(p^e)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X], \quad \deg(\varphi_{i,m}) = f \text{ for each } i.$$

*Here $f$ is independent of $i$, and $f$ and $g$ depend only on the reduction of $p$ modulo $m$ rather than fully on $p$.*

In algebraic number theory, this proposition describes how a prime $p$ decomposes in the cyclotomic integer ring $\mathbb{Z}[\zeta_n]$. As two particular instances of the proposition, we have already seen the prime power case,

$$\Phi_{p^e}(X) = (X-1)^{\phi(p^e)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X],$$

and in the case $p = 1 \bmod m$ there exist integers $\alpha_1, \dots, \alpha_{\phi(m)}$, distinct modulo $p$, such that

$$\Phi_m(X) = \prod_{i=1}^{\phi(m)} (X - \alpha_i) \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X] \quad \text{if } p = 1 \bmod m.$$

This last result does not require the full strength of Proposition 7.1. Indeed, the polynomial $X^{p-1} - 1$ has a full contingent of roots in $\mathbb{Z}/p\mathbb{Z}$ (this is Fermat's Little Theorem), and because $\Phi_m(X) \mid X^m - 1 \mid X^{p-1} - 1$ (using the condition $m \mid p-1$ and the finite geometric sum formula for the second divisibility), so does $\Phi_m(X)$. Similarly, if $p \neq 1 \bmod m$ then $\Phi_m(X)$ has no roots in $\mathbb{Z}/p\mathbb{Z}$, because its roots have order $m$ and $m \nmid p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$. Another thing to note here is that section 3 has shown that there exist infinitely many primes $p$ such that $p = 1 \mod m$, without requiring the full strength of Dirichlet's theorem on primes in an arithmetic progression.

*Proof.* Recall that $n = p^\epsilon m$. First we show that

$$\Phi_n(X) = \Phi_m(X)^{\phi(p^\epsilon)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

We have this result for $m = 1$. Also, it is trivial for $\epsilon = 0$. For $\epsilon \geq 1$, work modulo $p$ and note that the identity $\Phi_p(X^{p^{\epsilon-1}m}) = \Phi_{p^\epsilon}(X^m) = (X^m - 1)^{\phi(p^\epsilon)}$ is

$$\frac{X^{p^\epsilon m} - 1}{X^{p^{\epsilon-1}m} - 1} = (X^m - 1)^{\phi(p^\epsilon)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

Break the proper divisors of $p^\epsilon m$ into two sets to get

$$\Phi_{p^\epsilon m}(X) = \frac{X^{p^\epsilon m} - 1}{(X^{p^{\epsilon-1}m} - 1)\prod_{\substack{d|m \\ d<m}} \Phi_{p^\epsilon d}(X)} = \frac{(X^m - 1)^{\phi(p^\epsilon)}}{\prod_{\substack{d|m \\ d<m}} \Phi_{p^\epsilon d}(X)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

We are taking $m > 1$, and we may assume inductively on $m$ that each $\Phi_{p^\epsilon d}(X)$ in the denominator is $\Phi_d(X)^{\phi(p^\epsilon)}$, so indeed

$$\Phi_{p^\epsilon m}(X) = \frac{(X^m - 1)^{\phi(p^\epsilon)}}{\prod_{\substack{d|m \\ d<m}} \Phi_d(X)^{\phi(p^\epsilon)}} = \Phi_m(X)^{\phi(p^\epsilon)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

Now we show how $\Phi_m(X)$ factors in $(\mathbb{Z}/p\mathbb{Z})[X]$, where $p \nmid m$ and $p + m\mathbb{Z}$ has order $f$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. The argument relies on standard facts about finite fields. In the finite field of order $p^f$, the multiplicative group $\mathbb{F}_{p^f}^\times$ is cyclic of order $p^f - 1$ and so the $m$th power map on $\mathbb{F}_{p^f}^\times$ has a cyclic kernel of size $m$ because $m \mid p^f - 1$, with $\phi(m)$ kernel elements having order exactly $m$. In any proper subfield $\mathbb{F}_{p^i}$ where $i \mid f$, the $m$th power map on $\mathbb{F}_{p^i}^\times$ is an automorphism because $m \nmid p^i - 1$, and so the only $m$th root of unity in $\mathbb{F}_{p^i}$ is 1. Thus $\mathbb{F}_{p^f}$ is the splitting field of $\Phi_m(X)$ over $\mathbb{Z}/p\mathbb{Z}$. Its Galois group is cyclic of order $f$, generated by the Frobenius automorphism $x \mapsto x^p$. The $\phi(m)$ roots of $\Phi_m(X)$ form $g$ disjoint Galois orbits $[r] = \{r, r^p, r^{p^2}, \ldots, r^{p^{f-1}}\}$ of length $f$, and the corresponding Galois-symmetrized polynomials

$$\varphi_{[r]}(X) = \prod_{j=0}^{f-1} (X - r^{p^j})$$

are irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$. The proposition follows, with each $\varphi_{i,m}$ in its statement being $\varphi_{[r_i]}$ for a Galois orbit $[r_i]$. □

For example, taking $p^\epsilon m = 20$,

$$\Phi_{20}(X) = 1 - X^2 + X^4 - X^6 + X^8.$$

For $p = 5$, we first have $\Phi_{20}(X) = \Phi_4(X)^4 \bmod 5$, and then $\Phi_4(X) = X^2 + 1$ factors into linear terms modulo 5 because $5^1 = 1 \bmod 4$. Similarly $\Phi_{20}(X)$ factors into quartic terms modulo 7 because $7^4 = 2401 = 1 \bmod 20$, and 4 is the lowest such

exponent of 7. Computer algebra confirms these factorizations and others,

$$\Phi_{20}(X) = (1 + X + X^2 + X^3 + X^4)^2 \bmod 2,$$
$$\Phi_{20}(X) = (1 - X + X^3 + X^4)(1 + X - X^3 + X^4) \bmod 3,$$
$$\Phi_{20}(X) = (2 + X)^4(-2 + X)^4 \bmod 5,$$
$$\Phi_{20}(X) = (1 - 3X - 3X^2 + 3X^3 + X^4)(1 + 3X - 3X^2 - 3X^3 + X^4) \bmod 7,$$
$$\Phi_{20}(X) = (3 + X^2)(4 + X^2)(5 + X^2)(9 + X^2) \bmod 11,$$
$$\Phi_{20}(X) = (1 - 5X - X^2 + 5X^3 + X^4)(1 + 5X - X^2 - 5X^3 + X^4) \bmod 13,$$
$$\Phi_{20}(X) = (1 - 4X - X^2 + 4X^3 + X^4)(1 + 4X - X^2 - 4X^3 + X^4) \bmod 17,$$
$$\Phi_{20}(X) = (1 + 6X + X^2)(1 - 6X + X^2)(1 + 8X + X^2)(1 - 8X + X^2) \bmod 19,$$
$$\Phi_{20}(X) = (1 - 8X - 3X^2 + 8X^3 + X^4)(1 + 8X - 3X^2 - 8X^3 + X^4) \bmod 23,$$
$$\Phi_{20}(X) = (1 - 9X - 3X^2 + 9X^3 + X^4)(1 + 9X - 3X^2 - 9X^3 + X^4) \bmod 43,$$
$$\Phi_{20}(X) = (1 - 24X - 3X^2 + 24X^3 + X^4)(1 + 24X - 3X^2 - 24X^3 + X^4) \bmod 83.$$

Here the $10k + 3$ primes $3, 13, 23, 43, 83$ all have order 4 modulo 20 because they have order 4 modulo 5 and order 1 or 2 modulo 4, and so the factorizations modulo $3, 13, 23, 43, 83$ match as they must, with $f = 4$ and $g = 2$. Only the factorizations modulo prime divisors of 20 have repeat factors, their powers being $\phi(2^2) = 2$ and $\phi(5) = 4$.