# 8. Cyclotomic polynomials



## 1. *Multiple factors in polynomials*

There is a simple device to detect repeated occurrence of a factor in a polynomial with coefficients in a field.

Let $k$ be a *field*. For a polynomial

$$f(x) = c_n x^n + \ldots + c_1 x + c_0$$

with coefficients $c_i$ in $k$, *define* the **(algebraic) derivative** [1] $Df(x)$ of $f(x)$ by

$$Df(x) = nc_n x^{n-1} + (n-1)c_{n-1}x^{n-2} + \ldots + 3c_3 x^2 + 2c_2 x + c_1$$

Better said, $D$ is by definition a $k$-linear map

$$D : k[x] \longrightarrow k[x]$$

defined on the $k$-basis $\{x^n\}$ by

$$D(x^n) = nx^{n-1}$$

[1.0.1] **Lemma:** For $f, g$ in $k[x]$,

$$D(fg) = Df \cdot g + f \cdot Dg$$

[1] Just as in the calculus of polynomials and rational functions one is able to evaluate all limits algebraically, one can readily prove (without reference to any limit-taking processes) that the notion of *derivative* given by this formula has the usual properties.

**[1.0.2] Remark:** Any $k$-linear map $T$ of a $k$-algebra $R$ to itself, with the property that

$$T(rs) = T(r) \cdot s + r \cdot T(s)$$

is a $k$-linear **derivation** on $R$.

*Proof:* Granting the $k$-linearity of $T$, to prove the derivation property of $D$ is suffices to consider basis elements $x^m$, $x^n$ of $k[x]$. On one hand,

$$D(x^m \cdot x^n) = Dx^{m+n} = (m+n)x^{m+n-1}$$

On the other hand,

$$Df \cdot g + f \cdot Dg = mx^{m-1} \cdot x^n + x^m \cdot nx^{n-1} = (m+n)x^{m+n-1}$$

yielding the product rule for monomials. ///

A field $k$ is **perfect** if either the characteristic of $k$ is 0 [2] or if, in characteristic $p > 0$, there is a $p^{th}$ root $a^{1/p}$ in $k$ for every $a \in k$. [3]

**[1.0.3] Proposition:** Let $f(x) \in k[x]$ with a field $k$, and $P$ an irreducible polynomial in $k[x]$. If $P^e$ divides $f$ then $P$ divides $\gcd(f, Df)$. If $k$ is *perfect* and $e - 1 \neq 0$ in $k$, there is a converse: [4] if $P^{e-1}$ divides both $f$ and $Df$ then $P^e$ divides $f$.

*Proof:* On one hand, suppose $f = P^e \cdot g$ with $\geq 2$. By the product rule,

$$Df = eP^{e-1}DP \cdot g + P^e \cdot Dg$$

is a multiple of $P^{e-1}$. [5] This was the easy half.

On the other hand, for the harder half of the assertion, suppose $P^{e-1}$ divides both $f$ and $Df$. Write

$$f/P^{e-1} = Q \cdot P + R$$

with $\deg R < \deg P$. Then $f = QP^e + RP^{e-1}$. Differentiating,

$$Df = DQ\, P^e + eQP^{e-1}DP + DR\, P^{e-1} + R(e-1)P^{e-2}\, DP$$

By hypothesis $P^{e-1}$ divides $Df$. All terms on the right-hand side except possibly $R(e-1)P^{e-2}\, DP$ are divisible by $P^{e-1}$, so $P$ divides $R(e-1)P^{e-2}\, DP$. Since $P$ is irreducible, either $e - 1 = 0$ in $k$, or $P$ divides $R$, or $P$ divides $DP$. If $P$ divides $R$, $P^e$ divides $f$, and we're done.

If $P$ does not divide $R$ then $P$ divides $DP$. Since $\deg DP < \deg P$, if $P$ divides $DP$ then $DP = 0$. This would require that all the exponents of $x$ occurring with non-zero coefficient are divisible by the characteristic $p$, which must be positive. So $P$ is of the form

$$P(x) = a_{pm}x^{pm} + a_{p(m-1)}x^{p(m-1)} + a_{p(m-2)}x^{p(m-2)} + \ldots + a_{2p}x^{2p} + a_p x^p + a_0$$

[2] as for $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$

[3] As is the case for finite fields such as $\mathbb{Z}/p$, by Fermat's Little Theorem.

[4] In particular, this converse holds if the characteristic of $k$ is 0.

[5] This half does not need the irreducibility of $P$.

Using the perfect-ness of the field $k$, each $a_i$ has a $p^{th}$ root $b_i$ in $k$. Because the characteristic is $p > 0$,

$$(A + B)^p = A^p + B^p$$

Thus, $P(x)$ is the $p^{th}$ power of

$$b_{pm}x^n + b_{p(m-1)}x^{(m-1)} + b_{p(m-2)}x^{(m-2)} + \ldots + b_{2p}x^2 + b_px + b_0$$

If $P$ is a $p^{th}$ power it is not irreducible. Therefore, for $P$ irreducible $DP$ is not the zero polynomial. Therefore, $R = 0$, which is to say that $P^e$ divides $f$, as claimed. ///

---

# 2. *Cyclotomic polynomials*

For $b \neq 0$ in a field $k$, the **exponent** of $b$ is the smallest positive integer $n$ (if it exists) such that $b^n = 1$. That is, $b$ is a root of $x^n - 1$ but not of $x^d - 1$ for any smaller $d$. We construct polynomials $\Phi_n(x) \in \mathbb{Z}[x]$ such that

$$\Phi_n(b) = 0 \text{ if and only if } b \text{ is of exponent } n$$

These polynomials $\Phi_n$ are **cyclotomic polynomials**.

[2.0.1] **Corollary:** The polynomial $x^n - 1$ has no repeated factors in $k[x]$ if the field $k$ has characteristic *not* dividing $n$.

*Proof:* It suffices to check that $x^n - 1$ and its derivative $nx^{n-1}$ have no common factor. Since the characteristic of the field does not to divide $n$, $n \cdot 1_k \neq 0$ in $k$, so has a multiplicative inverse $t$ in $k$, and

$$(x^n - 1) - (tx) \cdot (nx^{n-1}) = -1$$

and $\gcd(x^n - 1, nx^{n-1}) = 1$. ///

Define the $n^{th}$ **cyclotomic polynomial** $\Phi_n(x)$ by

$$\Phi_1(x) = x - 1$$

and for $n > 1$, inductively,

$$\Phi_n(x) = \frac{x^n - 1}{lcm \text{ of all } x^d - 1 \text{ with } 0 < d < n,\ d \text{ dividing } n}$$

with the least common multiple *monic*.

[2.0.2] **Theorem:**

- $\Phi_n$ is a monic polynomial with integer coefficients. [6]
- For $\alpha$ in the field $k$, $\Phi_n(\alpha) = 0$ if and only if $\alpha^n = 1$ and $\alpha^t \neq 1$ for all $0 < t < n$.
- $\gcd(\Phi_m(x), \Phi_n(x)) = 1$ for $m < n$ with neither $m$ nor $n$ divisible by the characteristic of the field $k$.
- The degree of $\Phi_n(x)$ is $\varphi(n)$ (Euler's phi-function)
- Another description of $\Phi_n(x)$:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{1 \leq d < n, d|n} \Phi_d(x)}$$

[6] More properly, if the ambient field $k$ is of characteristic 0, then the coefficients lie in the copy of $\mathbb{Z}$ inside the prime field $\mathbb{Q}$ inside $k$. If the ambient field is of positive characteristic, then the coefficients lie inside the prime field (which is the natural image of $\mathbb{Z}$ in $k$). It would have been more elegant to consider the cyclotomic polynomials as polynomials in $\mathbb{Z}[x]$, but this would have required that we wait longer.

• $x^n - 1$ factors as

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

*Proof:* We know that $d|n$ (and $d > 0$) implies that $x^d - 1$ divides $x^n - 1$. Therefore, by unique factorization, the least common multiple of a collection of things each dividing $x^n - 1$ also divides $x^n - 1$. Thus, the indicated *lcm* does divide $x^n - 1$.

For $\alpha$ in $k$, $x - \alpha$ divides $\Phi_n(x)$ if and only if $\Phi_n(\alpha) = 0$. And $\alpha^t = 1$ if and only if $x - \alpha$ divides $x^t - 1$. The definition

$$\Phi_n(x) = \frac{x^n - 1}{\textit{lcm of all } x^d - 1 \text{ with } 0 < d < n,\ d \text{ dividing } n}$$

shows first that $\Phi_n(\alpha) = 0$ implies $\alpha^n = 1$. Second, if $\alpha^t = 1$ for any proper divisor $t$ of $n$ then $x - \alpha$ divides $x^t - 1$, and thus $x - \alpha$ divides the denominator. But $x^n - 1$ has no repeated factors, so $x - \alpha$ dividing the denominator would prevent $x - \alpha$ dividing $\Phi_n(x)$, contradiction. That is, $\Phi_n(\alpha) = 0$ if and only if $\alpha$ is of order $n$.

To determine the *gcd* of $\Phi_m$ and $\Phi_n$ for neither $m$ nor $n$ divisible by the characteristic of $k$, note that $\Phi_m$ divides $x^m - 1$ and $\Phi_n$ divides $x^n - 1$, so

$$\gcd(\Phi_m, \Phi_n) \quad \text{divides} \quad \gcd(x^m - 1, x^n - 1)$$

We claim that for $m$, $n$ two integers (divisible by the characteristic or not)

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

Prove this claim by induction on the maximum of $m$ and $n$. Reduce to the case $m > n$, wherein

$$x^m - 1 - x^{m-n} \cdot (x^n - 1) = x^{m-n} - 1$$

For $g$ a polynomial dividing both $x^m - 1$ and $x^n - 1$, $g$ divides $x^{m-n} - 1$. By induction,

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

But

$$\gcd(m, n) = \gcd(m - n, n)$$

and

$$x^m - 1 = x^{m-n} \cdot (x^n - 1) + x^{m-n} - 1$$

so

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

and induction works. Thus,

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

Since

$$d \le m < n$$

$d$ is a *proper* divisor of $n$. Thus, from

$$\Phi_n(x) = \frac{x^n - 1}{\textit{lcm of all } x^d - 1 \text{ with } 0 < d < n,\ d \text{ dividing } n}$$

we see that $\Phi_n(x)$ divides $(x^n - 1)/(x^d - 1)$. Since $x^n - 1$ has no repeated factors, $\Phi_n(x)$ has no factors in common with $x^d - 1$. Thus, $\gcd(\Phi_m, \Phi_n) = 1$.

Next, use induction to prove that

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

For $n = 1$ the assertion is true. From the definition of $\Phi_n$,

$$x^n - 1 = \Phi_n(x) \cdot \mathrm{lcm}\{x^d - 1 : d|n, 0 < d < n\}$$

By induction, for $d < n$

$$x^d - 1 = \prod_{0<e\le d, e|d} \Phi_e(x)$$

Since for $m < n$ the *gcd* of $\Phi_m$ and $\Phi_n$ is 1,

$$\mathrm{lcm}\{x^d - 1 : d|n, 0 < d < n\} = \prod_{d|n, d<n} \Phi_d(x)$$

Thus,

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

as claimed.

Inductively, since all lower-index cyclotomic polynomials have integer coefficients [7] and are monic, and $x^n - 1$ is monic with integer coefficients, the quotient of $x^n - 1$ by the product of the lower ones is monic with integer coefficients.

The assertion about the degree of $\Phi_n$ follows from the identity (see below) for Euler's phi-function

$$\sum_{d|n, d>0} \varphi(d) = n$$

This completes the proof of the theorem. ///

**[2.0.3] Proposition:** Let $\varphi(x)$ be Euler's phi-function

$$\varphi(x) = \sum_{1\le \ell\le x; \gcd(\ell,x)=1} 1$$

Then for $m$ and $n$ relatively prime

$$\varphi(mn) = \varphi(m) \cdot \varphi(n) \qquad \text{(weak multiplicativity)}$$

For $p$ prime and $\ell$ a positive integer

$$\varphi(p^\ell) = (p-1) \cdot p^{\ell-1}$$

And

$$\sum_{d|n, d>0} \varphi(d) = n$$

*Proof:* By unique factorization, for $\gcd(m, n) = 1$,

$$\gcd(t, mn) = \gcd(t, m) \cdot \gcd(t, n)$$

[7] Or, more properly, coefficients in the canonical image of $\mathbb{Z}$ in the field $k$.

so, $t$ is prime to $mn$ if and only if $t$ is prime to both $m$ and $n$. The gcd of $m$ and $n$ is the smallest positive integer of the form $rm + sn$. By Sun-Ze,

$$f : \mathbb{Z}/m \oplus \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$$

by

$$f : (x, y) \longrightarrow rmy + snx$$

is a *bijection*, since $m$ and $n$ are coprime. From $rm + yn = 1$, $rm = 1 \bmod n$ so $rm$ is prime to $n$, and $sn = 1 \bmod m$ so $sn$ is prime to $m$. Thus, $rmy + snx$ has a common factor with $m$ if and only if $x$ does, and $rmy + snx$ has a common factor with $n$ if and only if $y$ does. Thus, $f$ gives a bijection

$$\{x : 1 \le x < m, \gcd(x, m) = 1)\} \times \{y : 1 \le y < n, \gcd(y, n) = 1)\}$$

$$\longrightarrow \{z : 1 \le z < mn, \gcd(z, mn) = 1)\}$$

and $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. This reduces calculation of $\varphi()$ to calculation for prime powers $p^e$. An integer $x$ in $1 \le x < p^e$ is prime to $p^e$ if and only if it is not divisible by $p$, so there are

$$\varphi(p^e) = p^e - p^{e-1} = (p - 1)p^{e-1}$$

such $x$, as claimed.

To prove

$$\sum_{d|n, d>0} \varphi(d) = n$$

start with $n$ a prime power $p^e$, in which case

$$\sum_{d|p^e} \varphi(d) = \sum_{0 \le k \le e} \varphi(p^k) = 1 + \sum_{1 \le k \le e} (p - 1)p^{k-1} = 1 + (p - 1)(p^e - 1)/(p - 1) = p^e$$

Let $n = p_1^{e_1} \dots p_t^{e_t}$ with distinct primes $p_i$. Then

$$\sum_{d|n} \varphi(d) = \prod_{i=1,\dots,t} \left( \sum_{d|p_i^{e_i}} \varphi(d) \right) = \prod_{i=1,\dots,t} \varphi(p_i^{e_i}) = \varphi(\prod_i p_i^{e_i}) = \varphi(n)$$

This proves the desired identity for $\varphi$. ///

---

# 3. *Examples*

For prime $p$, the factorization of $x^p - 1$ into cyclotomic polynomials is boring

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$$

For $n = 2p$ with odd prime $p$

$$\Phi_{2p}(x) = \frac{x^{2p} - 1}{\Phi_1(x)\,\Phi_2(x)\,\Phi_p(x)} = \frac{x^{2p} - 1}{\Phi_2(x)\,(x^p - 1)} = \frac{x^p + 1}{x + 1}$$

$$= x^{p-1} - x^{p-2} + x^{p-3} - \dots + x^2 - x + 1$$

For $n = p^2$ with $p$ prime,

$$\Phi_{p^2}(x) = \frac{x^{p^2}-1}{\Phi_1(x)\,\Phi_p(x)} = \frac{x^{p^2}-1}{x^p-1} = x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1$$

Generally, one observes that for $n = p^e$ a prime power

$$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}}) = x^{p^{e-1}(p-1)} + x^{p^{e-1}(p-2)} + \ldots + x^{2p^{e-1}} + x^{2p^{e-1}} + 1$$

For $n = 2 \cdot m$ (with odd $m > 1$) we claim that

$$\backslash Phi_{2m}(x) = \Phi_m(-x)$$

Note that, anomalously, $\Phi_2(-x) = -x + 1 = -\Phi_1(x)$. Prove this by induction:

$$\Phi_{2m}(x) = \frac{x^{2m}-1}{\prod_{d|m}\ \Phi_d(x)\ \cdot \prod_{d|m,\ d<m}\ \Phi_{2d}(x)} = \frac{x^{2m}-1}{(x^m-1)\ \prod_{d|m,\ d<m}\ \Phi_d(-x)}$$

$$= \frac{x^m+1}{\prod_{d|m,\ d<m}\ \Phi_d(-x)} = \frac{(x^m+1)\,\Phi_m(-x)}{((-x)^m-1)\cdot(-1)} = \Phi_m(-x)$$

by induction, where the extra $-1$ in the denominator was for $\Phi_2(-x) = -\Phi_1(x)$, and $(-1)^m = -1$ because $m$ is odd.

Thus,

$$\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$$

$$\Phi_9(x) = \Phi_3(x^3) = x^6 + x^3 + 1$$

$$\Phi_{18}(x) = \Phi_9(-x) = x^6 - x^3 + 1$$

For $n = pq$ with distinct primes $p, q$ some unfamiliar examples appear.

$$\Phi_{15}(x) = \frac{x^{15}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = \frac{x^{15}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = \frac{x^{15}-1}{\Phi_3(x)(x^5-1)}$$

$$= \frac{x^{10}+x^5+1}{x^2+x+1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

by direct division [8] at the last step. And then

$$\Phi_{30}(x) = \Phi_{15}(-x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$$

[3.0.1] **Remark:** Based on a few hand calculations, one might speculate that all coefficients of all cyclotomic polynomials are either $+1$, $-1$, or 0, but this is not true. It *is* true for $n$ prime, and for $n$ having at most 2 distinct prime factors, but not generally. The smallest $n$ where $\Phi_n(x)$ has an exotic coefficient seems to be $n = 105 = 3 \cdot 5 \cdot 7$.

$$\Phi_{105}(x) = \frac{x^{105}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_7(x)\Phi_{15}(x)\Phi_{21}(x)\Phi_{35}(x)}$$

[8] Only mildly painful. Any lesson to be learned here?

$$= \frac{x^{105}-1}{\Phi_3(x)\Phi_{15}(x)\Phi_{21}(x)(x^{35}-1)} = \frac{x^{70}+x^{35}+1}{\Phi_3(x)\Phi_{15}(x)\Phi_{21}(x)} = \frac{(x^{70}+x^{35}+1)(x^7-1)}{\Phi_{15}(x)(x^{21}-1)}$$

$$= \frac{(x^{70}+x^{35}+1)(x^7-1)\Phi_1(x)\Phi_3(x)\Phi_5(x)}{(x^{15}-1)(x^{21}-1)}$$

$$= \frac{(x^{70}+x^{35}+1)(x^7-1)(x^5-1)\Phi_3(x)}{(x^{15}-1)(x^{21}-1)}$$

Instead of direct polynomial computations, we do *power series* [9] computations, imagining that $|x| < 1$, for example. Thus,

$$\frac{-1}{x^{21}-1} = \frac{1}{1-x^{21}} = 1 + x^{21} + x^{42} + x^{63} + \dots$$

We anticipate that the degree of $\Phi_{105}(x)$ is $(3-1)(5-1)(7-1) = 48$. We also observe that the coefficients of all cyclotomic polynomials are the same back-to-front as front-to-back (why?). Thus, we'll use power series in $x$ and ignore terms of degree above 24. Thus,

$$\Phi_{105}(x) = \frac{(x^{70}+x^{35}+1)(x^7-1)(x^5-1)(x^2+x+1)}{(x^{15}-1)(x^{21}-1)}$$

$$= (1+x+x^2)(1-x^7)(1-x^5)(1+x^{15})(1+x^{21})$$

$$= (1+x+x^2) \times (1 - x^5 - x^7 + x^{12} + x^{15} - x^{20} + x^{21} - x^{22})$$

$$= 1 + x + x^2 - x^5 - x^6 - x^7 - x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17}$$
$$- x^{20} - x^{21} - x^{22} + x^{21} + x^{22} + x^{23} - x^{22} - x^{23} - x^{24}$$

$$= 1 + x + x^2 - x^5 - x^6 - 2x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14}$$
$$+ x^{15} + x^{16} + x^{17} - x^{20} - x^{22} - x^{24}$$

Looking closely, we have a $-2x^7$.

Less well known are *Lucas-Aurifeullian-LeLasseur* factorizations such as

$$x^4 + 4 = (x^4 + 4x^2 + 4) - (2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

More exotic are

$$\frac{x^6+27}{x^2+3} = (x^2 + 3x + 3)(x^2 - 3x + 3)$$

$$\frac{x^{10}-5^5}{x^2-5} = (x^4 + 5x^3 + 15x^2 + 25x + 25) \times (x^4 - 5x^3 + 15x^2 - 25x + 25)$$

and

$$\frac{x^{12}+6^6}{x^4+36} = (x^4 + 6x^3 + 18x + 36x + 36) \times (x^4 - 6x^3 + 18x - 36x + 36)$$

and further

$$\frac{x^{14}+7^7}{x^2+7} = (x^6 + 7x^5 + 21x^4 + 49x^3 + 147x^2 + 343x + 343)$$
$$\times (x^6 - 7x^5 + 21x^4 - 49x^3 + 147x^2 - 343x + 343)$$

[9] In fact, one is not obliged to worry about convergence, since one can do computations in a *formal power series* ring. Just as polynomials can be precisely defined by their *finite* sequences of coefficients, with the obvious addition and multiplication mirroring our intent, formal power series are not-necessarily-finite sequences with the same addition and multiplication, noting that the multiplication does not require any infinite sums. The *formal* adjective here merely indicates that convergence is irrelevant.

The possibility and nature of these factorizations are best explained by Galois theory.

# 4. *Finite subgroups of fields*

Now we can prove that the multiplicative group $k^\times$ of a finite field $k$ is a *cyclic group*. When $k$ is *finite*, a generator of $k^\times$ is a **primitive root** for $k$.

[4.0.1] **Theorem:** Let $G$ be a finite subgroup of $k^\times$ for a field $k$. Then $G$ is cyclic.

[4.0.2] **Corollary:** For a finite field $k$, the multiplicative group $k^\times$ is cyclic. ///

*Proof:* Let $n$ be the order of $G$. Then [10] any element of $G$ is a root of the polynomial $f(x) = x^n - 1$. We know that a polynomial with coefficients in a field $k$ has at most as many roots (in $k$) as its degree, so this polynomial has at most $n$ roots in $k$. Therefore, it has *exactly* $n$ roots in $k$, namely the elements of the subgroup $G$.

The characteristic $p$ of $k$ cannot divide $n$, since if it did then the derivative of $f(x) = x^n - 1$ would be zero, and $\gcd(f, f') = f$ and $f$ would have multiple roots. Thus,

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

Since $x^n - 1$ has $n$ roots in $k$, and since the $\Phi_d$'s here are relatively prime to each other, each $\Phi_d$ with $d|n$ must have a number of roots (in $k$) equal to its degree. Thus, $\Phi_d$ for $d|q-1$ has $\varphi(d) > 0$ roots in $k$ (Euler's phi-function).

The roots of $\Phi_n(x)$ are $b \in k^\times$ such that $b^n = 1$ and no smaller positive power than $n$ has this property.

Any root of $\Phi_n(x) = 0$ in $k^\times$ would be a generator of the (therefore cyclic) group $G$. The cyclotomic polynomial $\Phi_n$ has $\varphi(n) > 0$ zeros, so $G$ has a generator, and is cyclic. ///

# 5. *Infinitude of primes* $p = 1 \bmod n$

This is a very special case of Dirichlet's theorem that, given a modulus $n$ and a fixed integer $a$ relatively prime to $n$, there are infinitely-many primes $p = a \bmod n$. We only treat the case $a = 1$.

[5.0.1] **Corollary:** Fix $1 < n \in \mathbb{Z}$. There are infinitely many primes $p = 1 \bmod n$.

*Proof:* Recall that the $n^{th}$ cyclotomic polynomial $\Phi_n(x)$ is monic (by definition), has integer coefficients, and has constant coefficient $\pm 1$. [11] And $\Phi_n(x)$ is not constant. Suppose there were only finitely-many primes $p_1, \ldots, p_t$ equal to 1 mod $n$. Then for large-enough positive integer $\ell$,

$$N = \Phi_n(\ell \cdot np_1 \ldots p_t) > 1$$

and $N$ is an integer. Since $\Phi_n(x)$ has integer coefficients and has constant term $\pm 1$, for each $p_i$ we have $N = \pm 1 \bmod p_i$, so in particular no $p_i$ divides $N$. But since $N > 1$ it does have some prime factor $p$. Further, since the constant term is $\pm 1$, $N = \pm 1 \bmod n$, so $p$ is relatively prime to $n$. Then

$$\Phi_n(\ell \cdot np_1 \ldots p_t) = N = 0 \bmod p$$

[10] Lagrange, again.

[11] The assertion about the constant coefficient follows from the fact that $\Phi_n(x)$ is monic, together with the fact that $\Phi(x^{-1}) = \pm\Phi(x)$, which is readily proven by induction.

Thus, $\ell \cdot np_1 \dots p_t$ has order $n$ in $\mathbb{F}_p^\times$. By Lagrange, $n$ divides $|\mathbb{F}_p^\times| = p-1$, so $p = 1 \bmod n$. Contradiction to the finiteness assumption, [12] so there are infinitely-many primes $p = 1 \bmod n$. ///

# 6. *Worked examples*

[8.1] Gracefully verify that the octic $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ factors properly in $\mathbb{Q}[x]$.

This octic is

$$\frac{x^9 - 1}{x - 1} = \frac{x^3 - 1)(x^6 + x^3 + 1)}{x - 1} = (x^2 + x + 1)\,(x^6 + x^3 + 1)$$

for example. We might anticipate this reducibility by realizing that

$$x^9 - 1 = \Phi_1(x)\,\Phi_3(x)\,\Phi_9(x)$$

where $\Phi_n$ is the $n^{th}$ cyclotomic polynomial, and the given octic is just $(x^9-1)/\Phi_1(x)$, so what is left *at least* factors as $\Phi_3(x)\,\Phi_9(x)$.

[8.2] Gracefully verify that the quartic $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

Use the recursive definition of cyclotomic polynomials

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

Thus, the given quartic is $\Phi_5(x)$. And use the fact that for the characteristic of the field $k$ not dividing $n$, $\Phi_n(\alpha) = 0$ if and only if $\alpha$ is of order $n$ in $k^\times$. If it had a linear factor $x - \alpha$ with $\alpha \in \mathbb{F}_2$, then $\Phi_4(\alpha) = 0$, and $\alpha$ would be of order 5 in $\mathbb{F}_2^\times$. But $\mathbb{F}_2^\times$ is of order 1, so has no elements of order 5 (by Lagrange). (We saw earlier that) existence of an irreducible quadratic factor of $\Phi_4(x)$ in $\mathbb{F}_2[x]$ is equivalent to existence of an element $\alpha$ of order 5 in $\mathbb{F}_{2^2}^\times$, but $|\mathbb{F}_{2^2}^\times| = 2^2 - 1 = 3$, which is not divisible by 5, so (Lagrange) has no element of order 5. The same sort of argument would show that there is no irreducible cubic factor, but we already know this since if there were any proper factorization then there would be a proper factor of at most half the degree of the quartic. But there is no linear or quadratic factor, so the quartic is irreducible.

[8.3] Gracefully verify that the sextic $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_3[x]$.

Use the recursive definition of cyclotomic polynomials

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

Thus, the given sextic is $\Phi_7(x)$. And use the fact that for the characteristic of the field $k$ not dividing $n$, $\Phi_n(\alpha) = 0$ if and only if $\alpha$ is of order $n$ in $k^\times$. If it had a linear factor $x - \alpha$ with $\alpha \in \mathbb{F}_3$, then $\Phi_7(\alpha) = 0$, and $\alpha$ would be of order 7 in $\mathbb{F}_2^\times$. But $\mathbb{F}_3^\times$ is of order 2, so has no elements of order 7 (Lagrange). Existence of an (irreducible) quadratic factor of $\Phi_7(x)$ in $\mathbb{F}_3[x]$ is equivalent to existence of an element $\alpha$ of order 7 in $\mathbb{F}_{3^2}^\times$, but $|\mathbb{F}_{3^2}^\times| = 3^2 - 1 = 8$, which is not divisible by 7, so (Lagrange) has no element of order 5. Similarly, if there were an (irreducible) cubic factor, then there would be a root in a cubic extension $\mathbb{F}_{3^3}$ of $\mathbb{F}_3$, but $\mathbb{F}_{3^3}^\times$ has order $3^3 - 1 = 26$ which is not divisible by 7, so there is no such element. If there were any proper

[12] Mildly ironic that we have a contradiction, considering that we seem to have just succeeded in proving that there is one more prime of the type that we want. Perhaps this suggests that it is needlessly inefficient to couch this argument as proof by contradiction.

factorization then there would be a proper factor of at most half the degree of the sextic. But there is no linear, quadratic, or cubic factor, so the sextic is irreducible.

[8.4] Gracefully verify that the quartic $x^4+x^3+x^2+x+1$ in factors into two irreducible quadratics in $\mathbb{F}_{19}[x]$.

As above, we see that the quartic is the $5^{th}$ cyclotomic polynomial. If it had a linear factor in $\mathbb{F}_{19}[x]$ then (since the characteristic 19 does not divide the index 5) there would be an element of order 5 in $\mathbb{F}_{19}^\times$, but the latter group has order $19-1$ not divisible by 5, so (Lagrange) there is no such element. But the quadratic extension $\mathbb{F}_{19^2}$ of $\mathbb{F}_{19}$ has multiplicative group with order $19^2-1=360$ which is divisible by 5, so there is an element $\alpha$ of order 5 there.

Since $\alpha\in\mathbb{F}_{19^2}-\mathbb{F}_{19}$, the minimal polynomial $M(x)$ of $\alpha$ over $\mathbb{F}_{19}$ is quadratic. We have shown that in this circumstance the polynomial $M$ divides the quartic. (Again, the proof is as follows: Let

$$x^4+x^3+x^2+x+1=Q(x)\cdot M(x)+R(x)$$

with $Q,R\in\mathbb{F}_{19}[x]$ and $\deg R<\deg M$. Evaluating at $\alpha$ gives $R(\alpha)=0$, which (by minimality of $M$) implies $R$ is the 0 polynomial. Thus, $M$ divides the quartic.) The quotient of the quartic by $M$ is quadratic, and (as we've already seen) has no linear factor in $\mathbb{F}_{19}[x]$, so is irreducible.

[8.5] Let $f(x)=x^6-x^3+1$. Find primes $p$ with each of the following behaviors: $f$ is irreducible in $\mathbb{F}_p[x]$, $f$ factors into irreducible quadratic factors in $\mathbb{F}_p[x]$, $f$ factors into irreducible cubic factors in $\mathbb{F}_p[x]$, $f$ factors into linear factors in $\mathbb{F}_p[x]$.

By the recursive definition and properties of cyclotomic polynomials, we recognize $f(x)$ as the $18^{th}$ cyclotomic polynomial $\Phi_{18}(x)$. For a prime $p$ not dividing 18, zeros of $\Phi_{18}$ are exactly elements of order 18. Thus, if $p^d-1=0 \bmod 18$ but no smaller exponent than $d$ achieves this effect, then $\mathbb{F}_{p^d}^\times$ (proven *cyclic* by now) has an element of order 18, whose minimal polynomial divides $\Phi_{18}(x)$.

We might observe that $(\mathbb{Z}/18)^\times$ is itself *cyclic*, of order $\varphi(18)=\varphi(2)\varphi(3^2)=(3-1)3=6$, so has elements of all possible orders, namely $1,2,3,6$.

For $p=1 \bmod 18$, for example $p=19$, already $p-1=0 \bmod 18$, so $f(x)$ has a *linear* factor in $\mathbb{F}_{19}[x]$. This is the case of order 1 element in $(\mathbb{Z}/18)^\times$.

A moment's thought might allow a person to realize that $17=-1$ is an element (and the only element) of order 2 in $(\mathbb{Z}/18)^\times$. So any prime $p=17 \bmod 18$ (for example $p=17$ itself, by coincidence prime) will have the property that $\mathbb{F}_{p^2}^\times$ has elements of order 18. Indeed, by properties of cyclic groups, it will have $\varphi(18)=6$ elements of order 18 there, each of whose minimal polynomial is quadratic. Thus (since a quadratic has at most two zeros) there are at least 3 irreducible quadratics dividing the sextic $\Phi_{18}(x)$ in $\mathbb{F}_p[x]$. Thus, since degrees add in products, these three quadratics are *all* the factors of the sextic.

After a bit of trial and error, one will find an element of order 3 in $(\mathbb{Z}/18)^\times$, such as 7. Thus, for $p=7 \bmod 18$ (such as 7 itself, which by coincidence is prime), there is no element of order 18 in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$, but there *is* one in $\mathbb{F}_{p^3}$, whose minimal polynomial over $\mathbb{F}_p$ is therefore cubic and divides $\Phi_{18}$. Again, by properties of cyclic groups, there are exactly $\varphi(18)=6$ such elements in $\mathbb{F}_{p^3}$, with cubic minimal polynomials, so there are at least (and, thus, exactly) two different irreducible cubics in $\mathbb{F}_p[x]$ dividing $\Phi_{18}(x)$ for such $p$.

After a bit more trial and error, one finds an element of order 6 in $(\mathbb{Z}/18)^\times$, such as 5. (The other is 11.) Thus, for $p=5 \bmod 18$ (such as 5 itself, which by coincidence is prime), there is no element of order 18 in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$, or $\mathbb{F}_{p^3}$, but there is one in $\mathbb{F}_{p^6}$. (By Lagrange, the only possible orders of $p$ in $(\mathbb{Z}/18)^\times$ are $1,2,3,6$, so we need not worry about $p^4$ or $p^5$). The minimal polynomial of such an element is $\Phi_{18}(x)$, which is (thus, necessarily) irreducible in $\mathbb{F}_p[x]$.

[8.6] Explain why $x^4+1$ properly factors in $\mathbb{F}_p[x]$ for any prime $p$.

As in the previous problems, we observe that $x^4+1$ is the $8^{th}$ cyclotomic polynomial. If $p|8$, namely $p=2$, then this factors as $(x-1)^4$. For odd $p$, if $p=1 \bmod 8$ then $\mathbb{F}_p^\times$, which we now know to be *cyclic*, has an element of order 8, so $x^4+1$ has a linear factor. If $p \neq 1 \bmod 8$, write $p=2m+1$, and note that

$$p^2-1=(2m+1)^2-1=4m^2+4m=m(m+1)\cdot 4$$

so, if $m$ is odd, $m+1$ is even and $p^2-1=0 \bmod 8$, and if $m$ is even, the same conclusion holds. That is, for odd $p$, $p^2-1$ is invariably divisible by 8. That is, (using the cyclicness of any finite field) there is an element of order 8 in $\mathbb{F}_{p^2}$. The minimal polynomial of this element, which is quadratic, divides $x^4+1$ (as proven in class, with argument recalled above in another example).

[8.7] Explain why $x^8-x^7+x^5-x^4+x^3-x+1$ properly factors in $\mathbb{F}_p[x]$ for any prime $p$. (*Hint:* It factors either into linear factors, irreducible quadratics, or irreducible quartics.)

The well-read person will recognize this octic as $\Phi_{15}(x)$, the fifteenth cyclotomic polynomial. For a prime $p$ not dividing 15, zeros of $\Phi_15$ in a field $\mathbb{F}_{p^d}$ are elements of order 15, which happens if and only if $p^d-1=0 \bmod 15$, since we have shown that $\mathbb{F}_{p^d}^\times$ is cyclic. The smallest $d$ such that $p^d=1 \bmod 15$ is the order of $p$ in $(\mathbb{Z}/15)^\times$. After some experimentation, one may realize that $(\mathbb{Z}/15)^\times$ is *not* cyclic. In particular, every element is of order 1, 2, or 4. (How to see this?) Granting this, for any $p$ other than 3 or 5, the minimal polynomial of an order 15 element is linear, quadratic, or quartic, and divides $\Phi_{15}$.

For $p=3$, there is some degeneration, namely $x^3-1=(x-1)^3$. Thus, in the (universal) expression

$$\Phi_{15}(x)=\frac{x^{15}-1}{\Phi_1(x)\,\Phi_3(x)\,\Phi_5(x)}$$

we actually have

$$\Phi_{15}(x)=\frac{(x^5-1)^3}{(x-1)^2\,(x^5-1)}=\frac{(x^5-1)^2}{(x-1)^2}=(x^4+x^3+x^2+1)^2$$

For $p=5$, similarly, $x^5-1=(x-1)^5$, and

$$\Phi_{15}(x)=\frac{x^{15}-1}{\Phi_1(x)\,\Phi_3(x)\,\Phi_5(x)}=\frac{(x^3-1)^5}{(x^3-1)\,(x-1)^4}=\frac{(x^3-1)^4}{(x-1)^4}=(x^2+x+1)^4$$

[8.8] Why is $x^4-2$ irreducible in $\mathbb{F}_5[x]$?

A zero of this polynomial would be a fourth root of 2. In $\mathbb{F}_5^\times$, one verifies by brute force that 2 is of order 4, so is a generator for that (cyclic) group, so is not a square in $\mathbb{F}_5^\times$, much less a fourth power. Thus, there is no linear factor of $x^4-2$ in $\mathbb{F}_5[x]$.

The group $\mathbb{F}_{5^2}^\times$ is cyclic of order 24. If 2 were a fourth power in $\mathbb{F}_{5^2}$, then $2=\alpha^4$, and $2^4=1$ gives $\alpha^{16}=1$. Also, $\alpha^{24}=1$ (Lagrange). Claim that $\alpha^8=1$: let $r,s\in\mathbb{Z}$ be such that $r\cdot 16+s\cdot 24=8$, since 8 is the greatest common divisor. Then

$$\alpha^8=\alpha^{16r+24s}=(\alpha^{16})^r\cdot(\alpha^{24})^s=1$$

This would imply

$$2^2=(\alpha^4)^2=\alpha^8=1$$

which is false. Thus, 2 is not a fourth power in $\mathbb{F}_{5^2}$, so the polynomial $x^4-2$ has no quadratic factors.

A quartic with no linear or quadratic factors is irreducible (since any proper factorization of a polynomial $P$ must involve a factor of degree at most half the degree of $P$). Thus, $x^4-2$ is irreducible in $\mathbb{F}_5[x]$.

[8.9] Why is $x^5-2$ irreducible in $\mathbb{F}_{11}[x]$?

As usual, to prove irreducibility of a quintic it suffices to show that there are no linear or quadratic factors. To show the latter it suffices to show that there is no zero in the underlying field (for linear factors) or in a quadratic extension (for irreducible quadratic factors).

First determine the order of 2 in $\mathbb{F}_{11}$: since $|\mathbb{F}_{11}^\times| = 10$, it is either $1, 2, 5$, or 10. Since $2 \neq 1 \bmod 11$, and $2^2 - 1 = 3 \neq 0 \bmod 11$, and $2^5 - 1 = 31 \neq 0 \bmod 11$, the order is 10. Thus, in $\mathbb{F}_{11}$ it cannot be that 2 is a fifth power.

The order of $\mathbb{F}_{11^2}^\times$ is $11^2 - 1 = 120$. If there were a fifth root $\alpha$ of 2 there, then $\alpha^5 = 2$ and $2^{10} = 1$ imply $\alpha^{50} = 1$. Also, (Lagrange) $\alpha^{120} = 1$. Thus, (as in the previous problem) $\alpha$ has order dividing the *gcd* of 50 and 120, namely 10. Thus, if there were such $\alpha$, then

$$2^2 = (\alpha^5)^2 = \alpha^{10} = 1$$

But $2^2 \neq 1$, so there is no such $\alpha$.

# Exercises

**8.**[6.0.1] Determine the coefficients of the $12^{th}$ cyclotomic polynomial.

**8.**[6.0.2] Gracefully verify that $(x^{15} - 1)/(x^5 - 1)$ factors properly in $\mathbb{Q}[x]$.

**8.**[6.0.3] Find a prime $p$ such that the $35^{th}$ cyclotomic polynomial has an irreducible $12^{th}$-degree factor in $\mathbb{F}_p[x]$.

**8.**[6.0.4] Determine the factorization into irreducibles of $(x^7 - 1)/(x - 1)$ in $\mathbb{F}_2[x]$.

**8.**[6.0.5] Explain why the $12^{th}$ cyclotomic polynomial factors properly in $\mathbb{F}_p[x]$ for any prime $p$.

**8.**[6.0.6] Explain why the thirty-fifth cyclotomic polynomial factors properly in $\mathbb{F}_p[x]$ for any prime $p$.

**8.**[6.0.7] Show that a finite field extension of $\mathbb{Q}$ contains only finitely-many roots of unity.

**8.**[6.0.8] Let $p$ be a prime and $n \geq 1$. Let $\varphi_m$ be the $m^{th}$ cyclotomic polynomial. Show that

$$\varphi_{pn}(x) = \begin{cases} \varphi_n(x^p) & (\text{for } p|n) \\ \dfrac{\varphi_n(x^p)}{\varphi_n(x)} & (\text{otherwise}) \end{cases}$$

**8.**[6.0.9] Let $n = 2^a\, p^b\, q^c$ for primes $p, q$. Show that the coefficients of the cyclotomic polynomial $\varphi_n$ are in the set $\{-1, 0, 1\}$.

**8.**[6.0.10] Suppose $n$ is divisible by $p^2$ for some prime $p$. Show that the sum of the primitive $n^{th}$ roots of unity is 0.