Fields and Cyclotomic Polynomials

These notes prove the existence of primitive elements in a very different way than the treatment in the textbook. Along the way we develop the theory of cyclotomic polynomials and prove some nice statements about quadratic residues.

Introduction to Fields

Here we briefly review the definition of a field, and we extend the notion of the order of an element to arbitrary fields.

Recall that a **binary operation** on a set S is a function $S \times S \to S$, i.e. a function that takes two elements of S as input and outputs an element of S. Some binary operations have certain special properties:

1. A binary operation $*$ is **associative** if
$$(x * y) * z \;=\; x * (y * z)$$
for all $x, y, z \in S$.

2. A binary operation $*$ is **commutative** if
$$x * y \;=\; y * x$$
for all $x, y \in S$.

3. An **identity element** for $*$ is an element e such that
$$x * e \;=\; e * x \;=\; x$$
for all $x \in S$.

4. If e is an identity element, an **inverse** for an element $x \in S$ with respect to $*$ is any element $y \in S$ such that
$$x * y = y * x = e.$$

5. Finally, if $+$ and $*$ are binary operations on a set S, we say that $*$ **distributes** over $+$ if
$$x * (y + z) = (x * y) + (x * z) \qquad \text{and} \qquad (x + y) * z = (x * z) + (y * z)$$
for all $x, y, z \in S$.

Definition: Field

A **field** is a set $\mathbb{F}$ with at least two elements having two binary operations:

1. An **addition** operation, usually denoted $x + y$ for $x, y \in \mathbb{F}$.
2. A **multiplication** operation, usually denoted xy for $x, y \in \mathbb{F}$.

These operations are required to satisfy the following conditions:

1. Addition is associative, commutative, has an identity element (usually denoted 0), and each element $x \in \mathbb{F}$ has an additive inverse (usually denoted $-x$).
2. Multiplication is associative, commutative, has an identity element (usually denoted 1), and each element $x \in \mathbb{F} - \{0\}$ has a multiplicative inverse (usually denoted x^{-1})
3. Multiplication distributes over addition.

For any field $\mathbb{F}$, we will let $\mathbb{F}^\times$ denote the set $\mathbb{F} - \{0\}$. Thus every element of $\mathbb{F}^\times$ has a multiplicative inverse.

For those familiar with group theory, axiom (1) says that a field forms an abelian group under addition, and axiom (2) implies that $\mathbb{F}^\times$ forms an abelian group under multiplication. Axiom (3) says that these two group structures are in a certain sense compatible with one another.

Some examples of fields include:

- The rational numbers $\mathbb{Q}$, under the usual operations of addition and multiplication.
- The real numbers $\mathbb{R}$, under the usual operations of addition and multiplication.
- The algebraic numbers $\mathbb{A}$, under the usual operations of addition and multiplication.

- The complex numbers $\mathbb{C}$, under the usual operations of addition and multiplication.
- For any prime p, the set $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, under the operations of addition and multiplication modulo p.

Of these examples, only $\mathbb{Z}_p$ is a **finite field**, meaning that it has a finite number of elements.

We now offer a few additional examples of fields.

EXAMPLE 1 Consider the set

$$\mathbb{Q}(\sqrt{2}) \;=\; \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

This set forms a field under the usual operations of addition and multiplication. In particular, $\mathbb{Q}(\sqrt{2})$ is clearly closed under addition, and it is also closed under multiplication:

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \;=\; (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}.$$

Every element of $\mathbb{Q}(\sqrt{2})$ has an additive inverse in $\mathbb{Q}(\sqrt{2})$, and similarly every element of $\mathbb{Q}(\sqrt{2})^\times$ has a multiplicative inverse in $\mathbb{Q}(\sqrt{2})$:

$$(a + b\sqrt{2})^{-1} \;=\; \frac{1}{a + b\sqrt{2}} \;=\; \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \;=\; \frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Note here that $a^2 - 2b^2$ can never be 0 if a and b are rational numbers. ■

EXAMPLE 2 Note that -1 $(= 2)$ has no square root in the field $\mathbb{Z}_3$. Consider the set

$$\mathbb{Z}_3(i) \;=\; \{a + bi \mid a, b \in \mathbb{Z}_3\} \;=\; \{0,\, 1, 2,\, i,\, 1+i,\, 2+i,\, 2i,\, 1+2i,\, 2+2i\}.$$

Here we have added a new element i to $\mathbb{Z}_3$ whose square is -1, in the same way that one adjoins a square root of -1 to $\mathbb{R}$ to obtain $\mathbb{C}$. The result is a set with exactly 9 elements (since there are three choices each for a and b).

We can define an addition operation on $\mathbb{Z}_3(i)$ by

$$(a_1 + b_1 i) + (a_2 + b_2 i) \;=\; (a_1 + a_2) + (b_1 + b_2)i$$

where $a_1 + a_2$ and $b_1 + b_2$ represent addition in $\mathbb{Z}_3$. Similarly, we can define multiplication on $\mathbb{Z}_3(i)$ by

$$(a_1 + b_1 i)(a_2 + b_2 i) \;=\; (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i.$$

It is easy to check that these operations are associative and commutative, and have identity elements. Each element $a + bi$ has an additive inverse $-a - bi$. It is less obvious that every element $\mathbb{Z}_3(i)^\times$ has a multiplicative inverse, but indeed

$$(1)(1) = (2)(2) = 1, \quad (i)(2i) = 1, \quad (1+i)(2+i) = 1, \quad \text{and} \quad (2+i)(1+2i) = 1.$$

Thus $\mathbb{Z}_3(i)$ is a finite field of order 9. ■

Though we will not be able to prove it here, finite fields have been completely classified.

Theorem 1 Classification of Finite Fields

If $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^n$ for some prime p and some $n \geq 1$. Moreover:

1. *For each prime p and each $n \geq 1$, there exists a finite field with exactly p^n elements.*

2. *Any two finite fields with the same number of elements are isomorphic.*

Here two fields are **isomorphic** if the only difference between them is the names of the elements, i.e. if there exists a bijection between them that preserves the algebraic operations. For example, let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, and let $\mathbb{F} = \{-2, -1, 0, 1, 2\}$ under the operations of addition and multiplication modulo 5. Then $\mathbb{F}$ is isomorphic to $\mathbb{Z}_5$, with the corresponding bijection being

$$0 \mapsto 0, \quad 1 \mapsto 1, \quad 2 \mapsto 2, \quad -2 \mapsto 3, \quad -1 \mapsto 4.$$

Indeed, according to the theorem above, any field with exactly 5 elements must be isomorphic to $\mathbb{Z}_5$.

Though the above theorem states that there is a finite field with p^n elements for any prime power p^n, the only finite fields we have seen so far are the fields $\mathbb{Z}_p$, which have a prime number of elements, and the field $\mathbb{Z}_3(i)$, which has 9 elements. In general, if p is prime and $a \in \mathbb{Z}_p$ is not a quadratic residue, then one can obtain a field with p^2 elements by adjoining a square root of a to $\mathbb{Z}_p$. For example:

- $\mathbb{Z}_7(i)$ is a field with $7^2 = 49$ elements, and $\mathbb{Z}_{11}(i)$ is a field with $11^2 = 121$ elements. However, the field with 25 elements cannot be described as $\mathbb{Z}_5(i)$, since -1 already has a square root in $\mathbb{Z}_5$.
- The field with 25 elements *can* be described as $\mathbb{Z}_5\big(\sqrt{2}\big)$, since 2 has no square root in $\mathbb{Z}_5$. Similarly, $\mathbb{Z}_{13}\big(\sqrt{2}\big)$ is a field with $13^2 = 169$ elements.

Finally, we will need some information about polynomials over fields. If $\mathbb{F}$ is a field and

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

is a polynomial with integer coefficients, then any element $a \in \mathbb{F}$ is said to be a **root** of p if

$$c_n a^n + c_{n-1}a^{n-1} + \cdots + a_1 x + a_0 = 0.$$

We will assume the following fact.

Theorem 2 Roots of Polynomials Over Fields

If $\mathbb{F}$ is a field and $p(x)$ is a polynomial of degree n with integer coefficients, then p has at most n different roots in $\mathbb{F}$.

Orders of Elements

The idea of the order of an element can be extended to any field.

Definition: Order of an Element
Let $\mathbb{F}$ be a field, and let $a \in \mathbb{F}^\times$. The **order** of a in $\mathbb{F}$, denoted $\mathrm{ord}_{\mathbb{F}}(a)$, is the smallest positive integer k for which $a^k = 1$. If no such k exists, then we say that a has **infinite order**.

For example, the only elements of $\mathbb{R}^\times$ that have finite order are 1 and -1, with $\mathrm{ord}_{\mathbb{R}}(1) = 1$ and $\mathrm{ord}_{\mathbb{R}}(-1) = 2$.

By the way, in the case of $\mathbb{Z}_p$, we use the same notation is the textbook and write $\mathrm{ord}_p(a)$ instead of $\mathrm{ord}_{\mathbb{Z}_p}(a)$ for the order of an element $a \in \mathbb{Z}_p^\times$.

EXAMPLE 3 The element $1 + i$ has order 8 in $\mathbb{Z}_3(i)^\times$, since

$$(1+i)^1 = 1+i, \qquad (1+i)^2 = 2i, \qquad (1+i)^3 = 1+2i, \qquad (1+i)^4 = 2,$$
$$(1+i)^5 = 2+2i, \qquad (1+i)^6 = i, \qquad (1+i)^7 = 2+i, \qquad (1+i)^8 = 1.$$

■

Proposition 3 Powers That Equal One

Let $\mathbb{F}$ be a field, let $a \in \mathbb{F}^\times$, and let $n \geq 1$. Then $a^n = 1$ if and only if $\mathrm{ord}_{\mathbb{F}}(a) \mid n$.

PROOF Let $k = \mathrm{ord}_{\mathbb{F}}(a)$. If $k \mid n$, then $n = mk$ for some $m \geq 1$, so

$$a^n \;=\; a^{mk} \;=\; (a^k)^m \;=\; 1^m \;=\; 1.$$

Conversely, suppose that $a^m = 1$, and let i and j be integers so that

$$im + jk \;=\; \gcd(m, k)$$

Then

$$a^{\gcd(m,k)} \;=\; a^{im+jk} \;=\; (a^m)^i (a^k)^j \;=\; 1^i 1^j \;=\; 1.$$

Then $\gcd(m, k)$ must be greater than or equal to k, so it follows that $\gcd(m, k) = k$, and hence $k \mid m$. ■

The following proposition determines the order of any power of an element.

Corollary 4 Orders of Powers

Let $\mathbb{F}$ be a field, let $a \in \mathbb{F}$, and suppose that $\mathrm{ord}_{\mathbb{F}}(a) = k$. *Then for any $n \geq 1$,*

$$\mathrm{ord}_{\mathbb{F}}(a^n) \;=\; \frac{k}{\gcd(n, k)}.$$

PROOF By the previous proposition, $(a^n)^m = 1$ if and only if $k \mid mn$. This occurs if and only if m is a multiple of $k/\gcd(n, k)$. ■

One of the most important properties of $\mathbb{Z}_p$ is Fermat's little theorem, which states that $a^{p-1} = 1$ for every $a \in \mathbb{Z}_p^\times$. By Proposition 3, the order of any element of $\mathbb{Z}_p^\times$ must be a divisor of $p - 1$.

The following proposition generalizes Fermat's little theorem to any finite field.

Theorem 5 Lagrange's Theorem for Finite Fields

Let $\mathbb{F}$ be a finite field with m elements. Then

$$a^{m-1} \;=\; 1$$

for every $a \in \mathbb{F}^\times$.

PROOF This follows from Lagrange's theorem in group theory. Specifically, the group $\mathbb{F}^\times$ has $|\mathbb{F}| - 1$ elements, so the multiplicative order of each element must be a divisor of $|\mathbb{F}| - 1$. ■

For example, recall that the field $\mathbb{Z}_7(i)$ has 49 elements. According to the above theorem,

$$(a + bi)^{48} = 1$$

for any element $a + bi \in \mathbb{Z}_7(i)$.

Corollary 6

If $\mathbb{F}$ is a finite field with m elements and $a \in \mathbb{F}^\times$, then $\operatorname{ord}_{\mathbb{F}}(a) \mid m - 1$.

Roots of Unity

Definition: Root of Unity
If n is a positive integer, an ***n*th root of unity** is a complex number ζ such that

$$\zeta^n = 1.$$

For example, 1 is the only first root of unity, and 1 and -1 are the only square roots of unity. It is easy to check that

$$1, \quad i, \quad -1, \quad \text{and} \quad -i$$

are fourth roots of unity, and indeed these are the only possibilities.

Proposition 7 Formula for the nth Roots of Unity

For any positive integer n, there are exactly n different nth roots of unity, namely the numbers

$$e^{2k\pi i/n} = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right)$$

for $0 \leq k < n$.

PROOF Note first that the n different numbers $e^{2k\pi i/n}$ for $0 \le k < n$ are all distinct, since they lie on the unit circle in the complex plane at angles of $2k\pi/n$ from the origin. Each of these numbers is an nt root of unity, since

$$\left(e^{2k\pi i/n}\right)^n = e^{2k\pi i} = 1$$

for all k. But since any nth root of unity is a root of the polynomial $z^n - 1$, which has degree n, there can be at most n different nth roots of unity, and therefore the numbers $e^{2k\pi i/n}$ for $0 \le k < n$ are the only possibilities. ■

According to this proposition, if we let

$$\omega = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right),$$

then the nth roots of unity are precisely the numbers

$$1, \quad \omega, \quad \omega^2, \quad \ldots, \quad \omega^{n-1},$$

since $\omega^k = e^{2k\pi i/n}$ for each k. For example, if $n = 4$ then $\omega = i$, and the fourth roots of unity are the powers of i:

$$i^0 = 1, \qquad i^1 = i, \qquad i^2 = -1, \qquad i^3 = -i.$$

EXAMPLE 1 The cube roots of unity consist of the number 1 together with

$$\omega = e^{2\pi i/3} = \frac{-1 + i\sqrt{3}}{2} \qquad \text{and} \qquad \omega^2 = e^{4\pi i/3} = \frac{-1 - i\sqrt{3}}{2}.$$

Note that ω and ω^2 lie on the unit circle in the complex plane at angles of $2\pi/3 = 120°$ and $4\pi/3 = 240°$, respectively. ■

EXAMPLE 2 The fifth roots of unity are the numbers $1, \omega, \omega^2, \omega^3, \omega^4$, where

$$\omega = e^{2\pi i/5} = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right) = \frac{-1 + \sqrt{5} + i\sqrt{10 + \sqrt{5}}}{4}.$$

The five roots lie at equally spaced points on the unit circle, with angles of

$$0, \quad 2\pi/5 = 72°, \quad 4\pi/5 = 144°, \quad 6\pi/5 = 216°, \quad \text{and} \quad 8\pi/5 = 288°.$$ ■

EXAMPLE 3 The sixth roots of unity are the numbers $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5$, where

$$\omega = e^{i\pi/3} = \cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = \frac{1 + i\sqrt{3}}{2}.$$

Note that $\omega^3 = -1$ is a square root of unity, and that

$$\omega^2 \;=\; \frac{-1+i\sqrt{3}}{2} \qquad \text{and} \qquad \omega^4 \;=\; \frac{-1-i\sqrt{3}}{2}$$

are cube roots of unity. The last root is ω^5, which is the complex conjugate of ω. ■

We saw in the last example that the sixth roots of unity include elements of orders 1, 2, 3, and 6. The following proposition generalizes this observation.

Proposition 8 Orders of Roots of Unity

Let $\zeta \in \mathbb{C}$ and let $n \geq 1$. Then ζ is an nth root of unity if and only if $\mathrm{ord}_{\mathbb{C}}(\zeta) \mid n$.

PROOF This follows immediately from Proposition 3. ■

Definition: Primitive Roots of Unity
A **primitive nth root of unity** is any nth root of unity ζ for which $\mathrm{ord}_{\mathbb{C}}(\zeta) = n$. We will let $P(n)$ denote the set of all primitive nth roots of unity.

That is, $\zeta \in \mathbb{C}^\times$ is a primitive nth root of unity if $\zeta^n = 1$ but $\zeta^k \neq 1$ for any $k < n$. Applying Proposition 3, we obtain the following characterization of the nth roots in terms of primitive roots.

Corollary 9 Structure of the Set of nth Roots

The set of all nth roots of unity is the union

$$\bigcup_{d \mid n} P(d),$$

For example, the fourth roots of unity are the union

$$P(1) \cup P(2) \cup P(4) \;=\; \{1\} \cup \{-1\} \cup \{i, -i\}$$

and the sixth roots of unity are the union

$$P(1) \cup P(2) \cup P(3) \cup P(6) \;=\; \{1\} \cup \{-1\} \cup \left\{\tfrac{-1+i\sqrt{3}}{2}, \tfrac{-1-i\sqrt{3}}{2}\right\} \cup \left\{\tfrac{1+i\sqrt{3}}{2}, \tfrac{1-i\sqrt{3}}{2}\right\}.$$

Proposition 10 Characterization of Primitive nth Roots

Let n be a positive integer, let $\omega = e^{2\pi i/n}$, and let

$$\zeta = \omega^k$$

be an nth root of unity. Then ζ is a primitive nth root of unity if and only if

$$\gcd(k, n) = 1.$$

PROOF Clearly $\mathrm{ord}_{\mathbb{C}}(\omega) = n$. Then $\mathrm{ord}_{\mathbb{C}}(\omega^k) = n/\gcd(n,k)$ by Corollary 4. In particular, $\mathrm{ord}_{\mathbb{C}}(\omega^k) = n$ if and only if $\gcd(n,k) = 1$. ■

Corollary 11 Number of Primitive Roots

For each $n \geq 1$, there are exactly $\phi(n)$ primitive nth roots of unity.

Combining this with Corollary 9, we obtain the following interesting formula involving the totient function.

Corollary 12 Sum of the Totient Function

If n is a positive integer, then

$$\sum_{d\,|\,n} \phi(d) = n.$$

For example,

$$\phi(1) + \phi(2) + \phi(4) = 1 + 1 + 2 = 4$$

and

$$\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6.$$

Cyclotomic Polynomials

> **Definition: Cyclotomic Polynomial**
> The ***n*th cyclotomic polynomial** Φ_n is defined by
> $$\Phi_n(x) \;=\; \prod_{\zeta\in P(n)} (x-\zeta)$$
> where $P(n)$ denotes the set of all primitive nth roots of unity.

For example:

- Since $P(1) = \{1\}$ and $P(2) = \{-1\}$, the first and second cyclotomic polynomials are respectively
$$\Phi_1(x) \;=\; x-1 \qquad \text{and} \qquad \Phi_2(x) \;=\; x+1.$$
- Recall that $P(3) = \{\omega, \omega^2\}$, where $\omega = \big(-1+i\sqrt{3}\big)/2$. Thus the third cyclotomic polynomial is
$$\Phi_3(x) \;=\; (x-\omega)\big(x-\omega^2\big) \;=\; x^2+x+1$$
- Since $P(4) = \{i, -i\}$, the fourth cyclotomic polynomial is
$$\Phi_4(x) \;=\; (x-i)(x+i) \;=\; x^2+1.$$

In general, since there are exactly $\phi(n)$ primitive nth roots of unity, the nth cyclotomic polynomial always has degree $\phi(n)$. Table 1.1 shows the first ten cyclotomic polynomials.

The following proposition is fundamental to the theory of cyclotomic polynomials.

n	$\Phi_n(x)$	n	$\Phi_n(x)$
1	$x-1$	6	x^2-x+1
2	$x+1$	7	$x^6+x^5+x^4+x^3+x^2+x+1$
3	x^2+x+1	8	x^4+1
4	x^2+1	9	x^6+x^3+1
5	$x^4+x^3+x^2+x+1$	10	$x^4-x^3+x^2-x+1$

Table 1.1: The first ten cyclotomic polynomials.

Proposition 13 Fundamental Relation

For any positive integer n,

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

PROOF The roots of $x^n - 1$ are precisely the nth roots of unity. But every nth root of unity is a primitive dth root of unity for some divisor d of n, and these are precisely the roots of the product on the right. ■

For example,

- $x^2 - 1 \;=\; \Phi_1(x)\,\Phi_2(x) \;=\; (x-1)(x+1)$.
- $x^3 - 1 \;=\; \Phi_1(x)\,\Phi_3(x) \;=\; (x-1)\big(x^2+x+1\big)$.
- $x^4 - 1 \;=\; \Phi_1(x)\,\Phi_2(x)\,\Phi_4(x) \;=\; (x-1)(x+1)\big(x^2+1\big)$.
- $x^5 - 1 \;=\; \Phi_1(x)\,\Phi_5(x) \;=\; (x-1)\big(x^4+x^3+x^2+x+1\big)$.
- $x^6 - 1 \;=\; \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x) \;=\; (x-1)(x+1)\big(x^2+x+1\big)\big(x^2-x+1\big)$.

We can use the fundamental relation to compute the cyclotomic polynomials inductively. The following example illustrates this technique.

EXAMPLE 4 Compute the fifteenth cyclotomic polynomial $\Phi_{15}(x)$.

SOLUTION By the fundamental relation,

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

and hence

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

Multiplying out the denominator gives

$$\Phi_{15}(x) \;=\; \frac{x^{15}-1}{x^7+x^6+x^5-x^2-x-1}.$$

This fraction can be simplified using polynomial long division, which is tedious but straightforward. The result is

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

In addition to being useful for computation, the fundamental relation also allows us to prove things about the cyclotomic polynomials inductively. The following proposition illustrates this technique.

Proposition 14 Integer Coefficients

Every cyclotomic polynomial $\Phi_n(x)$ has integer coefficients.

PROOF This follows by induction on n. For $n = 1$, we have that $\Phi_1(x) = x - 1$ has integer coefficients. For $n > 1$, we can write

$$x^n - 1 \;=\; \Phi_{d_1}(x)\,\Phi_{d_2}(x)\,\cdots\,\Phi_{d_k}(x)\,\Phi_n(x)$$

where $d_1, \ldots, d_k$ are the proper divisors of n. By our induction hypothesis, each $\Phi_{d_i}(x)$ has integer coefficients, and since each Φ_{d_i} is monic it follows that $\Phi_n(x)$ has integer coefficients.[1] ■

Since the cyclotomic polynomials are monic and have integer coefficients, it follows immediately that their roots (i.e. the roots of unity) are algebraic integers.

Regarding the coefficients, you may have noticed that each of the cyclotomic polynomials in Table 1.1 has the property that all of its coefficients are either 0, 1, or -1. It turns out that this pattern holds for $\Phi_n(x)$ whenever n has at most two odd prime factors, but in general the coefficients of $\Phi_n(x)$ can be arbitrary integers. Since $3 \times 5 \times 7 = 105$, the first such example is $\Phi_{105}(x)$, which has two coefficients of -2.

Incidentally, it is a theorem of Gauss that every cyclotomic polynomial is actually irreducible over $\mathbb{Q}$, meaning that it cannot be factored into polynomials of smaller degree that have rational coefficients. It follows that the fundamental relation

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

is the complete factorization of the polynomial $x^n - 1$ over the rational numbers.

[1] We are using here the fact that if $p(x)$ and $q(x)$ are monic polynomials with integer coefficients and $q(x)$ is a factor of $p(x)$, then the quotient $p(x)/q(x)$ also has integer coefficients. This is because no non-integers can arise during the long division of $p(x)$ by $q(x)$.

Proposition 15 $\Phi_p(x)$ and $\Phi_{2p}(x)$.

If $p > 2$ is prime, then

$$\Phi_p(x) \;=\; x^{p-1} + x^{p-2} + \cdots + x + 1$$

and

$$\Phi_{2p}(x) \;=\; x^{p-1} - x^{p-2} + \cdots - x + 1.$$

PROOF Since p is prime, we have $x^p - 1 = \Phi_1(x)\,\Phi_p(x)$, so

$$\Phi_p(x) \;=\; \frac{x^p - 1}{\Phi_1(x)} \;=\; \frac{x^p - 1}{x - 1} \;=\; x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Moreover,

$$\begin{aligned}\Phi_{2p}(x) \;&=\; \frac{x^{2p} - 1}{\Phi_1(x)\,\Phi_2(x)\,\Phi_p(x)} \;=\; \frac{x^{2p} - 1}{(x^p - 1)\,\Phi_2(x)} \\ &=\; \frac{x^{2p} - 1}{(x^p - 1)\,(x + 1)} \;=\; \frac{x^p + 1}{x + 1} \;=\; x^{p-1} - x^{p-2} + \cdots - x + 1.\end{aligned}$$ ■

For example,

$$\Phi_{11}(x) \;=\; x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

and

$$\Phi_{14}(x) \;=\; x^6 - x^5 + x^4 - x^3 + x^2 - x + 1.$$

Lemma 16 Orders of Roots

Let $\mathbb{F}$ be a field, and let k and n be positive integers with $k \mid n$. Then for each $a \in \mathbb{F}^\times$,

$$\mathrm{ord}_{\mathbb{F}}(a) \;=\; nk \qquad \textit{if and only if} \qquad \mathrm{ord}_{\mathbb{F}}(a^k) = n.$$

PROOF If $\mathrm{ord}_{\mathbb{F}}(a) = nk$, then by Corollary 4, it follows that

$$\mathrm{ord}_{\mathbb{F}}(a^k) \;=\; \frac{nk}{\gcd(k, nk)} \;=\; \frac{nk}{k} \;=\; n.$$

For the converse, suppose that $\operatorname{ord}_{\mathbb{F}}(a^k) = n$, and let $m = \operatorname{ord}_{\mathbb{F}}(a)$. By Corollary 4, we know that

$$\operatorname{ord}_{\mathbb{F}}(a^k) = \frac{m}{\gcd(m,k)}$$

so

$$\frac{m}{\gcd(m,k)} = n.$$

Since $k \mid n$ and $m = n\gcd(m,k)$, we know that $k \mid m$, and therefore $\gcd(m,k) = k$. It follows that $m = nk$. ■

Proposition 17 A Formula for $\Phi_{nk}(x)$

Let n and k be positive integers with $k \mid n$. Then

$$\Phi_{nk}(x) = \Phi_n(x^k).$$

PROOF Let $\zeta \in \mathbb{C}^\times$. By the lemma, $\zeta \in P(nk)$ if and only if $\zeta^k \in P(n)$. Thus ζ is a root of $\Phi_{nk}(x)$ if and only if ζ^k is a root of $\Phi_n(x^k)$. Then $\Phi_{nk}(x)$ and $\Phi_n(x^k)$ are monic polynomials with the same roots, so they must be equal. ■

For example, it follows from this proposition that

$$\Phi_{18}(x) = \Phi_6(x^3) = (x^3)^2 - (x^3) + 1 = x^6 - x^3 + 1$$

and

$$\Phi_{64}(x) = \Phi_8(x^8) = (x^8)^4 + 1 = x^{32} + 1.$$

Primitive Elements

The notion of a primitive element makes perfect sense over any finite field.

Definition: Primitive Element
Let $\mathbb{F}$ be a finite field with m elements. An element $a \in \mathbb{F}^\times$ is called a **primitive element** of $\mathbb{F}$ if $\operatorname{ord}_{\mathbb{F}}(a) = m - 1$.

We shall now use cyclotomic polynomials to prove the existence of primitive elements. We begin with the following theorem.

Theorem 18 Order and Cyclotomic Polynomials

Let $\mathbb{F}$ be a field, let $a \in \mathbb{F}^\times$, and suppose that $\mathrm{ord}_{\mathbb{F}}(a) = n$. *Then* $\Phi_n(a) = 0$.

PROOF By Proposition 13, we know that

$$\prod_{d|n} \Phi_d(a) \;=\; a^n - 1 \;=\; 0.$$

But for $d < n$, the polynomial $\Phi_d(x)$ is also a factor of $x^d - 1$. Since a is not a root of $x^d - 1$ for any $d < n$, it follows that $\Phi_d(a) \neq 0$ for any $d < n$, and therefore $\Phi_n(a) = 0$. ■

For example, observe that 2 has order 3 modulo 7, since

$$2^1 \equiv 2 \pmod 7, \qquad 2^2 \equiv 4 \pmod 7 \qquad \text{and} \qquad 2^3 \equiv 1 \pmod 7.$$

Then 2 must be a root of $\Phi_3(x) = x^2 + x + 1$ modulo 7. This is easy to check:

$$\Phi_3(2) \;=\; 2^2 + 2 + 1 \;\equiv\; 0 \pmod 7.$$

Similarly, 4 also has order 3 modulo 7, so

$$\Phi_3(4) \;=\; 4^2 + 4 + 1 \;\equiv\; 0 \pmod 7$$

as well. Indeed,

$$x^2 + x + 1 \;\equiv\; (x-2)(x-4) \pmod 7.$$

By the way, the converse of the previous theorem does *not* hold in general. For example,

$$\Phi_2(1) \equiv 0 \pmod 2,$$

but 1 does not have order two in $\mathbb{Z}_2$. Similarly,

$$\Phi_6(2) \equiv 0 \pmod 3,$$

but 2 does not have order six in $\mathbb{Z}_3$.

Theorem 19 Orders of Elements in Finite Fields

Let $\mathbb{F}$ be a finite field with m elements, and let d be a divisor of $m-1$. Then the polynomial $\Phi_d(x)$ has exactly $\phi(d)$ roots in $\mathbb{F}$, and these are precisely the elements of $\mathbb{F}^\times$ that have order d.

PROOF For each divisor d of $m-1$, let $R(d)$ be the set of all roots of $\Phi_d(x)$ in $\mathbb{F}^\times$. By the previous proposition, if $a \in \mathbb{F}^\times$ has order d, then $d \in R(d)$. By Lagrange's theorem for finite fields, we know that the order of a divides $m-1$ for all $a \in \mathbb{F}^\times$, and hence

$$\bigcup_{d \,|\, m-1} R(d) \;=\; \mathbb{F}^\times.$$

But since each $\Phi_d(x)$ has degree $\phi(d)$, we know that $|R(d)| \leq \phi(d)$ for each d. By Corollary 12, we have

$$\sum_{d \,|\, m-1} \phi(d) \;=\; m-1 \;=\; |\mathbb{F}^\times|,$$

so indeed $|R(d)| = \phi(d)$ for each $d \mid m-1$, Moreover, these sets must all be disjoint, so each element $a \in \mathbb{F}^\times$ of order d lies *only* in $R(d)$, and therefore each element of $R(d)$ must have order d. ■

Corollary 20 Existence of Primitive Elements

Let $\mathbb{F}$ be a finite field with m elements. Then $\mathbb{F}$ has exactly $\phi(m-1)$ primitive elements.

Indeed, these primitive elements are precisely the roots of $\Phi_{m-1}(x)$ in $\mathbb{F}$. For example, the primitive elements of $\mathbb{Z}_7$ are 3 and 5, and these are precisely the roots of the polynomial $\Phi_6(x) = x^2 - x + 1$ in $\mathbb{Z}_7$. Indeed, it is easy to check that

$$x^2 - x + 1 \;\equiv\; (x-3)(x-5) \pmod{7}.$$

We can state this sort of factorization of $\Phi_k(x)$ in general.

Corollary 21 Factorization of $\Phi_d(x)$ Modulo p

Let p be a prime and let d be a divisor of $p-1$. Then

$$\Phi_d(x) \;\equiv\; \prod_{\zeta \in O(d)} (x-\zeta) \pmod{p}$$

where $O(d)$ denotes the set of elements of $\mathbb{Z}_p^\times$ of order d.

Application to Quadratic Residues

Recall that a number $k \in \mathbb{Z}$ is called a **quadratic residue** modulo n if the congruence

$$x^2 \equiv k \pmod{n}$$

has at least one solution. That is, k is a quadratic residue modulo n if k has a square root modulo n.

Theorem 22 Square Roots of -1

Let $p > 2$ be a prime. Then -1 is a quadratic residue modulo p if and only if

$$p \equiv 1 \ (\mathrm{mod}\ 4).$$

PROOF Observe that -1 is the only root of $\Phi_2(x) = x+1$, so it is the only element of $\mathbb{Z}_p$ of order 2. Then -1 has a square root in $\mathbb{Z}_p$ if and only if $\mathbb{Z}_p$ has elements of order 4, i.e. if and only if $4 \mid p-1$. This is equivalent to the condition that $p \equiv 1 \ (\mathrm{mod}\ 4)$. ■

For example, -1 has a square root modulo 5, 13, or 17:

$$2^2 \equiv -1 \ (\mathrm{mod}\ 5), \qquad 5^2 \equiv -1 \ (\mathrm{mod}\ 13), \qquad 4^2 \equiv -1 \ (\mathrm{mod}\ 17)$$

but -1 has no square root modulo 3, 7, or 11.

Of course, the reasoning used in the proof of this theorem can also be applied to any finite field. That is, if $\mathbb{F}$ is a finite field with m elements, then -1 has a square root in $\mathbb{F}$ if and only if $m \equiv 1 \ (\mathrm{mod}\ 4)$.

Theorem 23 Primes Congruent to $1 \ (\mathrm{mod}\ 4)$

There are infinitely many primes congruent to $1 \ (\mathrm{mod}\ 4)$.

PROOF Observe that if n is any even integer, then every prime divisor of n^2+1 must be congruent to 1 modulo 4. For if p is a prime divisor of n^2+1, then $p \neq 2$ since n is even, and since $n^2 \equiv -1 \ (\mathrm{mod}\ p)$ it follows that $p \equiv 1 \ (\mathrm{mod}\ 4)$.

Now suppose there are only finitely many primes $p_1, \ldots, p_m$ congruent to 1 modulo 4, and let $n = 2p_1 \cdots p_m$. Then n^2+1 is not divisible by any of the p_i, but every prime factor of n^2+1 is congruent to 1 modulo 4, a contradiction. ■

The following theorem is based on an interesting trick. Recall that the primitive cube roots of unity are the numbers

$$\omega = \frac{-1 + i\sqrt{3}}{2} \qquad \text{and} \qquad \omega^2 = \frac{-1 - i\sqrt{3}}{2}.$$

Then

$$\omega - \omega^2 = i\sqrt{3}$$

is a square root of -3. This suggests a possible way of making square roots of -3 in any field: if we can find an element a in the field of order 3, then perhaps $a - a^2$ will be a square root of -3.

Theorem 24 Square Roots of -3

Let $p > 3$ be a prime. Then -3 is a quadratic residue modulo p if and only if

$$p \equiv 1 \pmod 3.$$

PROOF Suppose first that $p \equiv 1 \pmod 3$. Then 3 is a divisor of $p - 1$, so there exists an element $a \in \mathbb{Z}_p$ of order 3. Note then that a is a root of the cyclotomic polynomial $\Phi_3(x) = x^2 + x + 1$, so $a^2 + a = -1$. Then

$$\left(a - a^2\right)^2 = a^2 - 2a^3 + a^4 = a^2 - 2 + a = -3,$$

so -3 is a quadratic residue modulo p.

Conversely, suppose that -3 is a quadratic residue modulo p, and let $b \in \mathbb{Z}_p$ so that $b^2 = -3$. Let $c = 2^{-1}(-1 + b)$, and note that $c \neq 1$ since $b \neq 3$. But

$$(-1 + b)^3 = -1 + 3b - 3b^2 + b^3 = -1 + 3b - 3(-3) + b(-3) = 8$$

so $c^3 = \left(2^{-1}\right)^3(-1 + b)^3 = \left(2^{-1}\right)^3(8) = 1$. Then c has order 3 in $\mathbb{Z}_p$, which implies that $3 \mid p - 1$, and hence $p \equiv 1 \pmod 3$. ■

For example, -3 has a square root modulo 7, 13, or 19:

$$2^2 \equiv -3 \pmod 7, \qquad 6^2 \equiv -3 \pmod{13}, \qquad 4^2 \equiv -3 \pmod{19}$$

but -3 has no square root modulo 5, 11, or 17.

Corollary 25 Primes Congruent to $1 \pmod 3$

There are infinitely many primes congruent to $1 \pmod 3$.

PROOF Observe that if n is any even integer and n is not a multiple of 3, then every prime factor of n^2+3 is congruent to 1 modulo 3. For neither 2 nor 3 can be a prime factor of n^2+3, and if $p>3$ is a prime factor of n^2+3 then $n^2 \equiv -3 \pmod{p}$ and hence $p \equiv 1 \pmod{3}$.

Now suppose that there are only finitely many primes $p_1, \ldots, p_m$ congruent to 1 modulo 3, and let $n = 2p_1 \cdots p_m$. Then n is even and is not a multiple of 3, so every prime factor of n^2+3 is congruent to 1 modulo 3. But none of the primes $p_1, \ldots, p_m$ divide n^2+3, a contradiction. ■

Corollary 26 Square Roots of 3

Let p be prime. If $p \equiv 1 \pmod{12}$, then 3 is a quadratic residue modulo p

PROOF Since $p \equiv 1 \pmod{4}$, there exists an element $a \in \mathbb{Z}_p$ so that $a^2 = -1$. Since $p \equiv 1 \pmod{3}$, there exists an element $b \in \mathbb{Z}_p$ so that $b^2 = -3$. Then

$$(ab)^2 = a^2b^2 = (-1)(-3) = 3,$$

so 3 is a quadratic residue. ■

Note that the converse of this last corollary is false. That is, there exist prime numbers p with $p \not\equiv 1 \pmod{12}$ for which 3 is a quadratic residue. A simple example is 11, for which

$$5^2 \equiv 3 \pmod{11}.$$

Indeed, it is a consequence of quadratic reciprocity that 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$.