Elements of Group Theory

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Groups are ubiquitous in modern mathematics.

We will primarily be interested in applications of groups to the theory of congruences.

The classical results of Wilson, Fermat and Euler can all be recast as statements about the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$.

The theory of groups is extensive, and we will only develop those tools that will be useful in the context of elementary number theory.

Binary Operations

Definition

Let S be a set. A *binary operation on* S is a function $\cdot : S \times S \to S$.

Remarks. Given a binary operation $\cdot : S \times S \to S$ and $x, y \in S$:

- We usually use infix notation and write $x \cdot y$ rather than $\cdot(x, y)$.
- Depending on the operation, it is also common to abbreviate $x \cdot y$ as xy.

Examples. Addition and multiplication are binary operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Groups

Definition

A *group* is a set G together with a binary operation which satisfies:

1. (Associativity) For all $a, b, c \in G$, $(ab)c = a(bc)$.
2. (Identity) There exists an $e \in G$ so that $ae = ea = a$ for all $a \in G$.
3. (Inverses) For each $a \in G$, there exists $b \in G$ so that $ab = ba = e$.

A group G is called *abelian* if it also satisfies:

4. (Commutativity) For all $a, b \in G$, $ab = ba$.

Examples

- $(\mathbb{Z}, +)$ is an abelian group. $(\mathbb{Z}, \times)$ is *not* a group.
- $(\mathbb{R} \setminus \{0\}, \times)$ and $(\mathbb{R}^+, \times)$ are abelian groups.
- For any $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z}, +)$ and $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ are (finite) abelian groups.
- The set

$$\mathrm{GL}_2)(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

  is a non-abelian group under matrix multiplication.
- For any nonempty set S, the set $\mathrm{Perm}(S)$ of bijections $S \to S$ is a group under function composition, non-abelian if $|S| \geq 3$.

Basic Properties of Groups

Let G be a group.

The identity element in G is unique. If $e, e' \in G$ are *both* identities, then

$$e = ee' = e'.$$

Note that we have used the "two-sided-ness" of the identity here.

Given $a \in G$, its inverse is also unique. If $b, c \in G$ are both inverses of a, then

$$b = be = b(ac) = (ba)c = ec = c.$$

Note that we have used associativity as well as the "two-sided-ness" of both inverses and the identity.

Let $a \in G$. We denote its inverse by a^{-1}.

We set $a^0 = e$ and for $n \in \mathbb{N}$ we define

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}},$$
$$a^{-n} = (a^{-1})^n.$$

With these definitions one can show that we have the familiar laws of exponents:

$$a^{m+n} = a^m a^n,$$
$$(a^m)^n = a^{mn},$$

for all $m, n \in \mathbb{Z}$.

Additive Groups

Sometimes it is convenient to describe a group using additive notation rather than multiplicative notation.

In this case we write $a + b$ for ab, 0 for e, and $-a$ for a^{-1}.

When using additive notation, we write

$$\underbrace{a + a + \cdots + a}_{n \text{ times}} = na$$

for $n \in \mathbb{N}$ and set $(-n)a = -(na)$. The laws of exponents become

$$(m + n)a = ma + na,$$
$$(mn)a = m(na),$$

for all $m, n \in \mathbb{Z}$.

Consider the additive group $\mathbb{Z}/n\mathbb{Z}$.

For any $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ we have

$$n(a + n\mathbb{Z}) = (na) + n\mathbb{Z} = 0 + n\mathbb{Z}.$$

Notice that $n = |\mathbb{Z}/n\mathbb{Z}|$.

This is no coincidence. It turns out that for any finite group G one has

$$a^{|G|} = e \quad \text{for all } a \in G.$$

The proof of this fact in general would take us too far afield.

However, when G is abelian we can give a very simple proof.

Translations

Let G be a group. For $a \in G$ define $L_a : G \to G$ by

$$L_a(x) = ax \quad \text{for all } x \in G.$$

L_a is called *left translation by* a.

Lemma 1

Let G be a group. For any $a \in G$, L_a is a bijection.

Proof. One can easily show that $(L_a)^{-1} = L_{a^{-1}}$ (HW). The result follows. □

Remark. The *right translation* $R_a(x) = xa$ also defines a bijection $G \to G$. However, if G is nonabelian, then $L_a \neq R_a$, in general.

Left translation will be the main tool in proving our main result.

Theorem 1

Let G be a finite abelian group. Then for any $a \in G$ one has

$$a^{|G|} = e.$$

Proof. Let

$$P = \prod_{x \in G} x,$$

the product of all of the elements in G.

Because G is abelian, the value of P is independent of how we choose to order the elements of G.

Let $a \in G$. Since $L_a : G \to G$ is a bijection,

$$P = \prod_{x \in G} x = \prod_{x \in G} L_a(x) = \prod_{x \in G} (ax).$$

Because G is abelian, in the final product we can factor out one copy of a for each $x \in G$. That is,

$$\prod_{x \in G} (ax) = a^{|G|} \prod_{x \in G} x = a^{|G|} P.$$

Hence, $P = a^{|G|} P$. Multiplication by P^{-1} on both sides finally yields

$$a^{|G|} = e.$$

Fermat's Little Theorem

Let $p \in \mathbb{N}$ be prime. Our first nontrivial application of Theorem 1 will be to the multiplicative group

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{a + p\mathbb{Z} : p \nmid a\} = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \ldots, (p-1) + p\mathbb{Z}\}.$$

Since $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1$, it follows that if $p \nmid a$, then

$$(a + p\mathbb{Z})^{p-1} = a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z} \quad \Leftrightarrow \quad a^{p-1} \equiv 1 \pmod{p}.$$

This proves:

Theorem 2 (Fermat's Little Theorem)

Let $p \in \mathbb{N}$ be prime and $a \in \mathbb{Z}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

There is an equivalent formulation of Fermat's theorem that doesn't require an additional hypothesis on a.

Corollary 1

Let $p \in \mathbb{N}$ be prime. For any $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

Proof. If $p|a$, then $p|a^p$, and hence

$$a \equiv 0 \equiv a^p \pmod{p}.$$

If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem.

Multiplying both sides of this congruence by a we immediately obtain $a^p \equiv a \pmod{p}$. □

Examples

Example 1

Find the remainder when 3^{298} is divided by 7.

Solution. Since $7 \nmid 3$, Fermat's theorem tells us that

$$3^6 \equiv 1 \pmod{7}.$$

So we reduce the exponent 298 modulo 6:

$$298 = 49 \cdot 6 + 4.$$

Thus

$$3^{298} = 3^{49 \cdot 6 + 4} = (3^6)^{49} \cdot 3^4 \equiv 1^{49} \cdot 3^4 \equiv (3^2)^2 \equiv 4 \pmod{7}.$$

Hence the remainder is $\boxed{4}$. □

Example 2

Let $a \in \mathbb{Z}$. Show that if $(a, 35) = 1$, then $a^{12} \equiv 1 \pmod{35}$.

Solution. It suffices to show that

$$a^{12} \equiv 1 \pmod{5} \quad \text{and} \quad a^{12} \equiv 1 \pmod{7}.$$

(Why?)

If $(a, 35) = 1$, then $5 \nmid a$ and $7 \nmid a$. By Fermat:

$$a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \pmod{5},$$
$$a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod{7},$$

which is what we needed to show. □

Euler's Theorem

Ryan C. Daileda

Trinity University

Number Theory

Recall

Theorem 1

Let G be a finite abelian group. For any $a \in G$, $a^{|G|} = e$.

Taking $G = (\mathbb{Z}/p\mathbb{Z})^\times$ for a prime p, we deduced Fermat's Little Theorem as a corollary.

The analogue of Fermat's Little Theorem for an arbitrary modulus $n \in \mathbb{N}$ is known as *Euler's Theorem*.

To state it, we first need a definition.

Definition

For $n \in \mathbb{N}$, *Euler's totient function* is defined by

$$\begin{aligned}\varphi(n) &= \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \left|\{a + n\mathbb{Z} \,|\, (a,n) = 1\}\right| \\ &= \left|\{1 \leq a < n \,|\, (a,n) = 1\}\right|.\end{aligned}$$

Examples

- For any prime p, $\varphi(p) = p - 1$.
- Since every integer is coprime to 1, we have $\varphi(1) = 1$.
- Direct computation gives:

$$\varphi(4) = 2, \quad \varphi(6) = 2, \quad \varphi(8) = 4, \quad \varphi(9) = 6,$$
$$\varphi(10) = 4, \quad \varphi(12) = 4, \quad \varphi(14) = 6, \quad \varphi(15) = 8.$$

- Because $(a, 2^n) = 1$ if and only if a is odd,

$$\varphi(2^n) = 2^n/2 = 2^{n-1}.$$

Euler's Theorem

We can now state and prove our main result.

Theorem 2

For any $n \in \mathbb{N}$, if $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. If $(a, n) = 1$, then $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Since $(\mathbb{Z}/n\mathbb{Z})^{\times}$ has order $\varphi(n)$ (by definition),

$$1 + n\mathbb{Z} = (a + n\mathbb{Z})^{\varphi(n)} = a^{\varphi(n)} + n\mathbb{Z},$$

according to Theorem 1.

But this is equivalent to $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

It follows, for instance, that if a is odd and not divisible by 7, then

$$a^6 \equiv 1 \pmod{14}.$$

And if $(a, 15) = 1$, then

$$a^8 \equiv 1 \pmod{15}.$$

And if $n \in \mathbb{N}$ and a is odd, then

$$a^{2^{n-1}} \equiv 1 \pmod{2^n}.$$

Remark. One can use induction to establish the stronger conclusion that, in fact,

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

for all $n \geq 3$, which has interesting consequences...

Properties

The function $\varphi(n)$ has a number of important properties.

Theorem 3

Let $p \in \mathbb{N}$ be prime. For any $n \in \mathbb{N}$, $\varphi(p^n) = p^n - p^{n-1}$.

Proof. A natural number $a < p^n$ is coprime to p^n iff $p \nmid a$.

Equivalently, $a < p^n$ is *not* coprime to p^n iff $a = pk$ for some k.

Since $kp < p^n$ iff $k < p^{n-1}$, there are exactly $p^{n-1} - 1$ choices for k, and hence for a.

So the number of $1 \leq a < p^n$ coprime to p^n is given by

$$(p^n - 1) - (p^{n-1} - 1) = p^n - p^{n-1}.$$

Isomorphisms

The totient function enjoys a useful property known as *multiplicativity*.

To understand the multiplicative nature of φ we need to take a slight detour.

Definition

Let R_1 and R_2 be rings. A *(ring) isomorphism* between R_1 and R_2 is a bijective function $f : R_1 \to R_2$ which satisfies:

1. $f(a+b) = f(a) + f(b)$;
2. $f(ab) = f(a)f(b)$,

for all $a, b \in R_1$.

Remarks

One can show that if $f : R_1 \to R_2$ is an isomorphism of rings, then $f(0_{R_1}) = 0_{R_2}$ and $f(1_{R_1}) = 1_{R_2}$.

The inverse of a ring isomorphism $f : R_1 \to R_2$ is a also an isomorphism (in the reverse direction).

If there is an isomorphism $f : R_1 \to R_2$, we say that R_1 and R_2 are *isomorphic*.

Isomorphic rings are "the same." Any ring-theoretic property satisfied by R_1 is automatically satisfied by R_2.

Products of Rings

We require one more purely ring-theoretic construction.

Definition

Let R_1 and R_2 be rings. Their *direct product* is the set $R_1 \times R_2$ endowed with the coordinate-wise operations

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2),$$

for all $a_1, a_2 \in R_1$ and $b_1, b_2 \in R_2$.

Theorem 4

If R_1 and R_2 are rings, then the direct product $R_1 \times R_2$ is also a ring.

Proof. Exercise. □

We have already encountered ring isomorphisms and product rings.

Suppose $m, n \in \mathbb{N}$ are relatively prime. The CRT asserts that that map

$$\begin{aligned} R : \mathbb{Z}/mn\mathbb{Z} &\to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}), \\ a + mn\mathbb{Z} &\mapsto (a + m\mathbb{Z}, a + n\mathbb{Z}), \end{aligned}$$

is a well-defined bijection.

The map R is also a ring isomorphism. For instance, if $a, b \in \mathbb{Z}$, then

$$\begin{aligned} R((a+mn\mathbb{Z})+(b+mn\mathbb{Z})) &= R((a+b)+mn\mathbb{Z}) \\ &= ((a+b)+m\mathbb{Z},(a+b)+n\mathbb{Z}) \\ &= ((a+m\mathbb{Z})+(b+m\mathbb{Z}),(a+n\mathbb{Z})+(b+n\mathbb{Z})) \\ &= (a+m\mathbb{Z},a+n\mathbb{Z})+(b+m\mathbb{Z},b+n\mathbb{Z}) \\ &= R(a+mn\mathbb{Z})+R(b+mn\mathbb{Z}), \end{aligned}$$

proving that R preserves addition.

It follows that R provides a ring isomorphism

$$\boxed{\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \quad \text{for} \quad (m,n)=1}.$$

The connection to Euler's totient function is provided by the pair of results.

Lemma 1

If R_1 and R_2 are rings, then $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$.

Proof (Sketch). Since the identity in $R_1 \times R_2$ is $(1_{R_1}, 1_{R_2})$, one can easily show that

$$(a, b)^{-1} = (a^{-1}, b^{-1}).$$

The result follows. □

Lemma 2

If $f : R_1 \to R_2$ is an isomorphism of rings, then $f| : (R_1)^\times \to (R_2)^\times$ is a multiplication preserving bijection (an isomorphism of groups*).*

Proof (Sketch). Every element of R_2 has the form $f(a)$ for some $a \in R_1$, and for every $a, b \in R_1$,

$$1_{R_2} = f(1_{R_1}) = f(ab) = f(a)f(b)$$

holds iff $a \in R_1^\times$ iff $f(a) \in R_2^\times$. □

A few remarks aside, we're ready to move on.

Remarks

One can form the direct product of any number (or indexed collection) of rings in an analogous manner, by simply performing addition and multiplication coordinate-wise.

Theorem 5 still holds in this more general setting: the unit group in the product is the product of the unit groups.

Applied in this setting, if $n_i \in \mathbb{N}$ are pairwise coprime, the CRT and Lemma 2 provide an isomorphism

$$(\mathbb{Z}/n_1 n_2 \cdots n_r\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times.$$

Let $p_1, p_2, \ldots, p_r \in \mathbb{N}$ be distinct primes and $e_1, e_2, \ldots, e_r \in \mathbb{N}$.

For $i \neq j$, the FTA implies that $(p_i^{e_i}, p_j^{e_j}) = 1$.

It follows that there is an isomorphism

$$(\mathbb{Z}/p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times.$$

This immediately implies that

$$\varphi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}).$$

This is what we mean when we say that φ is *multiplicative*.

We arrive at the following formula for φ.

Theorem 5

Let $n \in \mathbb{N}$. Then

$$\varphi(n) = \prod_{p|n}(p^{e_p} - p^{e_p-1}) = n\prod_{p|n}\left(1 - \frac{1}{p}\right),$$

where both products run over the prime divisors of n, and e_p denotes the exponent of p occurring in the canonical form of n.

Remarks.

- Remembering that the empty product equals 1 by caveat, both formulae are automatically valid for $n = 1$.
- It is often more convenient to use the equivalent form $p^{e_p} - p^{e_p-1} = p^{e_p-1}(p-1)$.

Proof of Theorem 5

Since $n = \prod_{p|n} p^{e_p}$, the multiplicativity of φ and Theorem 3 immediately imply that

$$\begin{aligned}\varphi(n) &= \varphi\left(\prod_{p|n} p^{e_p}\right) = \prod_{p|n} \varphi(p^{e_p}) \\ &= \prod_{p|n} (p^{e_p} - p^{e_p - 1}) = \prod_{p|n} p^{e_p}\left(1 - \frac{1}{p}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

Examples

We have

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$$

and

$$\varphi(98) = \varphi(2 \cdot 7^2) = \varphi(2)\varphi(7^2) = (2-1) \cdot 7(7-1) = 42$$

and

$$\begin{aligned}\varphi(18000000) &= \varphi(2 \cdot 9 \cdot 10^6) = \varphi(2^7)\varphi(3^2)\varphi(5^6) \\ &= 2^{7-1}(2-1) \cdot 3^{2-1}(3-1) \cdot 5^{6-1}(5-1) \\ &= 2^6 \cdot 3 \cdot 2 \cdot 5^5 \cdot 2^2 \\ &= 48 \cdot 10^5 = 4800000.\end{aligned}$$

Properties of Euler's Totient Function

Ryan C. Daileda

Trinity University

Number Theory

Recall

For $n \in \mathbb{N}$, Euler's *totient function* is defined to be

$$\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \left|\{1 \leq a \leq n \,|\, (a,n) = 1\}\right|.$$

Last time we proved that φ is *multiplicative*: given distinct primes p_i and $e_i \in \mathbb{N}$,

$$\varphi(p_1^{e_1} \cdots p_r^{e_r}) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r});$$

and we used this to deduce the formulae

$$\varphi(n) = \prod_{p|n}(p^{e_p} - p^{e_p - 1}) = n \prod_{p|n}\left(1 - \frac{1}{p}\right).$$

If we partition $\{1 \leq a \leq n\}$ according to (a, n), we can use φ to count the partitions and arrive at another useful identity.

Lemma 1

Let $n \in \mathbb{N}$ and suppose $d|n$. There is a bijection

$$\{1 \leq a \leq n \,|\, (a, n) = d\} \longleftrightarrow \left\{1 \leq b \leq \frac{n}{d} \,|\, \left(b, \frac{n}{d}\right) = 1\right\}.$$

Proof. If $1 \leq a \leq n$ and $(a, n) = d$, let $f(a) = \frac{a}{d}$.

We have

$$d = (a, n) = \left(d\frac{a}{d}, d\frac{n}{d}\right) = d\left(f(a), \frac{n}{d}\right) \quad \Rightarrow \quad \left(f(a), \frac{n}{d}\right) = 1.$$

Thus $f : \{1 \leq a \leq n \,|\, (a, n) = d\} \to \left\{1 \leq b \leq \frac{n}{d} \,|\, \left(b, \frac{n}{d}\right) = 1\right\}$.

On the other hand, if $1 \leq b \leq \frac{n}{d}$ and $(b, \frac{n}{d}) = 1$, define $g(b) = bd$.

Then

$$d = d\left(b, \frac{n}{d}\right) = (bd, n) = (g(b), n)$$

so that $g : \left\{1 \leq b \leq \frac{n}{d} \,|\, \left(b, \frac{n}{d}\right) = 1\right\} \to \{1 \leq a \leq n \,|\, (a, n) = d\}$.

Since $f(g(b)) = f(bd) = \frac{bd}{d} = b$ and $g(f(a)) = g(\frac{a}{d}) = d\frac{a}{d} = a$, f and g are inverses.

The result follows. □

Lemma 1 has the following immediate corollary.

Corollary 1

Let $n \in \mathbb{N}$ and suppose $d|n$. Then

$$\left|\{1 \leq a \leq n \,|\, (a,n) = d\}\right| = \varphi\left(\frac{n}{d}\right).$$

For $d|n$, the sets $\{1 \leq a \leq n \,|\, (a,n) = d\}$ partition $\{1 \leq a \leq n\}$.

Thus

$$n = \sum_{d|n} \left|\{1 \leq a \leq n \,|\, (a,n) = d\}\right| = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

But as d runs through the positive divisors of n, so does n/d. This proves:

Theorem 1

For $n \in \mathbb{N}$,

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

This identity will prove useful when we discuss *primitive roots*.

Before turning in that direction we prove one more identity involving φ.

Theorem 2

Let $n \in \mathbb{N}$. If $n > 1$, then

$$\sum_{\substack{1 \le a < n \\ (a,n)=1}} a = \frac{1}{2} n\varphi(n).$$

Proof. If $1 \le a \le n$ and $(a, n) = 1$, then

$$1 \le n - a < n \quad \text{and} \quad (n - a, n) = (-a, n) = (a, n) = 1.$$

Thus

$$\sum_{\substack{1 \le a < n \\ (a,n)=1}} a = \sum_{\substack{1 \le a < n \\ (a,n)=1}} (n - a) = n \sum_{\substack{1 \le a < n \\ (a,n)=1}} 1 - \sum_{\substack{1 \le a < n \\ (a,n)=1}} a = n\varphi(n) - \sum_{\substack{1 \le a < n \\ (a,n)=1}} a.$$

The result follows. □

The Order of an Element

Definition

Let G be a group and $a \in G$. The *order (or period)* of a, denoted $|a|$, is the least $n \in \mathbb{N}$ so that $a^n = e$. If no such n exists, we say that $|a|$ is infinite.

Examples.

- If G is a group and $a \in G$, then $|a| = 1$ iff $a = e$.
- Every nonzero element of $\mathbb{Z}$ has infinite order, since if $a \in \mathbb{Z}$ and $a \neq 0$, then $an \neq 0$ for all $n \in \mathbb{N}$.
- $2 + 6\mathbb{Z}$ has (additive) order 3 since $2(2 + 6\mathbb{Z}) = 4 + 6\mathbb{Z}$ and $3(2 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 0 + 6\mathbb{Z}$.
- $2 + 5\mathbb{Z}$ has (multiplicative) order 4 since

$$(2 + 5\mathbb{Z})^2 = 4 + 5\mathbb{Z}, (2 + 5\mathbb{Z})^3 = 3 + 5\mathbb{Z}, (2 + 5\mathbb{Z})^4 = 1 + 5\mathbb{Z}.$$

Properties of the Order

Theorem 3

Let G be a group and $a \in G$. If a has finite order $n \in \mathbb{N}$, then $a^m = e$ if and only if $n|m$.

Proof. Suppose $a^m = e$. Use the Division Algorithm to write $m = qn + r$ with $0 \leq r < n$.
Then

$$e = a^m = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r.$$

If $r > 0$, this contradicts the fact that $n = |a|$. So we must have $r = 0$ and hence $n|m$.
The converse is immediate. If $m = nq$, then

$$a^m = a^{nq} = (a^n)^q = e^q = e.$$

Corollary 2

Let G be a group and $a \in G$. If a has finite order $n \in \mathbb{N}$, then $a^i = a^j$ iff $i \equiv j \pmod{n}$.

Proof. We have

$$a^i = a^j \iff a^i(a^j)^{-1} = e \iff a^{i-j} = e.$$

The result now follows from Theorem 1. □

This immediately implies:

Corollary 3

Let G be a group and $a \in G$. If a has finite order $n \in \mathbb{N}$, then the distinct powers of a are $e, a, a^2, a^3, \ldots, a^{n-1}$.

It remains to address the powers of an element with infinite order.

Theorem 4

Let G be a group and $a \in G$. If $|a|$ is infinite, then $a^i = a^j$ iff $i = j$. That is, the powers of a are all distinct.

Proof. Suppose $a^i = a^j$ and $i \neq j$. Without loss of generality, suppose $i > j$.

Then, as above, we have $a^{i-j} = e$. Since $i - j > 0$, this implies $|a|$ is finite, which is a contradiction.

Thus we must have $i = j$. □

Corollary 4

Let G be a group. If G contains an element of infinite order, then G is infinite. Conversely, if G is finite, every element of G has finite order.

Proof. If $a \in G$ has infinite order, then the subset $\{a^i \mid i \in \mathbb{Z}\}$ is infinite, by Theorem 2.

Hence G is infinite as well. □

Corollary 5

Let G be a finite group and $a \in G$. Then $|a| \leq |G|$.

Proof. Let $n = |a|$. Then G contains the elements $e, a, a^2, \ldots, a^{n-1}$, which are distinct by Corollary 2. Thus $|G| \geq n$. □

When G is a finite abelian group, we can give a more precise relationship between $|a|$ and $|G|$.

Theorem 5

Let G be a finite abelian group. For any $a \in G$, $|a|$ divides $|G|$.

Proof. For $a \in G$, we know that $a^{|G|} = e$.

The result now follows from Theorem 3. □

Remark. The conclusion of Theorem 5 holds for arbitrary finite groups, but the proof would take us too far afield.

Orders of Powers of Elements

Let G be a group, let $a \in G$, and suppose that $|a| = n \in \mathbb{N}$.
Let $m \in \mathbb{Z}$ and set $b = a^m$. Since

$$b^n = (a^m)^n = a^{mn} = (a^n)^m = e^m = e,$$

b necessarily has finite order.
Let's compute $|b|$. We have

$$b^k = e \;\Leftrightarrow\; (a^m)^k = e \;\Leftrightarrow\; a^{mk} = e \;\Leftrightarrow\; n|mk,$$

by Theorem 3.
Write $m = (m,n)m'$ and $n = (m,n)n'$, so that $(m',n') = 1$. Then

$$n|mk \;\Leftrightarrow\; (m,n)n'|(m,n)m'k \;\Leftrightarrow\; n'|m'k \;\Leftrightarrow\; n'|k,$$

by Euclid's lemma.

The smallest positive k so that $n'|k$ is n'. Thus:

Theorem 6

Let G be a group and let $a \in G$ have finite order n. Then for any $m \in \mathbb{Z}$,

$$|a^m| = \frac{n}{(m,n)}.$$

Corollary 6

Let G be a group and let $a \in G$ have finite order n. If $(m,n) = 1$ and $b = a^m$, then

$$\{e, a, a^2, \ldots, a^{n-1}\} = \{e, b, b^2, \ldots, b^{n-1}\}.$$

Proof. If $(m,n) = 1$, then $|b| = |a^m| = \frac{n}{(m,n)} = n$. Thus b has exactly n distinct powers.
But so does a, and every power of b is a power of a.
The result follows. □

Additive Orders Modulo n

We will primarily be interested in the orders of elements in the groups $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^\times$.

We can very easily determine the orders of elements in $\mathbb{Z}/n\mathbb{Z}$.

We first notice that $|1 + n\mathbb{Z}| = n$, since

$$k(1 + n\mathbb{Z}) = k + n\mathbb{Z} = 0 + n\mathbb{Z} \quad \Leftrightarrow \quad n|k.$$

Let $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. Then $a + n\mathbb{Z} = a(1 + n\mathbb{Z})$. By Theorem 6 we have:

Theorem 7

The additive order of $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ is $\dfrac{n}{(a, n)}$.

Example. Consider $a = 4$ modulo 10. Since $\frac{10}{(10,4)} = \frac{10}{2} = 5$, 4 should have additive order 5 modulo 10. Indeed:

$$2{\cdot}4 = 8, \;\; 3{\cdot}4 \equiv 2 \pmod{10}, \;\; 4{\cdot}4 \equiv 6 \pmod{10}, \;\; 5{\cdot}4 \equiv 0 \pmod{10}.$$

Similar computations produce the following table.

Order	Elements
1	$0 + 10\mathbb{Z}$
2	$5 + 10\mathbb{Z}$
5	$2 + 10\mathbb{Z}$, $4 + 10\mathbb{Z}$, $6 + 10\mathbb{Z}$, $8 + 10\mathbb{Z}$
10	$1 + 10\mathbb{Z}$, $3 + 10\mathbb{Z}$, $7 + 10\mathbb{Z}$, $9 + 10\mathbb{Z}$

By Corollary 6, it follows, for instance, that every element of $\mathbb{Z}/10\mathbb{Z}$ is a multiple of $7 + 10\mathbb{Z}$.

This is equivalent to the statement that for any $a \in \mathbb{Z}$, the linear congruence $7x \equiv a \pmod{10}$ has a solution.

We can explain the preceding table by counting how many elements of $\mathbb{Z}/n\mathbb{Z}$ have a given order.

Let d divide $\left|\mathbb{Z}/n\mathbb{Z}\right| = n$. Then $a + n\mathbb{Z}$ has order d iff $d = \frac{n}{(a,n)}$ iff $(a, n) = \frac{n}{d}$.

Thus, the number of elements in $\mathbb{Z}/n\mathbb{Z}$ with order d is equal to

$$\left|\{1 \leq a \leq n \,|\, (a, n) = n/d\}\right| = \varphi\left(\frac{n}{n/d}\right) = \varphi(d),$$

by Corollary 1. These computations prove the next result.

Theorem 8

Let $n \in \mathbb{N}$ and suppose $d|n$. There are exactly $\varphi(d)$ elements in $\mathbb{Z}/n\mathbb{Z}$ of order d.

Cyclic Groups and Primitive Roots

Ryan C. Daileda

Trinity University

Number Theory

Cyclic Subgroups

Let G be a group and let $a \in G$. The set

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

is clearly closed under multiplication and inversion in G.
$\langle a \rangle$ is therefore a group in its own right, the *cyclic subgroup generated by* a.
Our work last time immediately proves:

Theorem 1

Let G be a group and let $a \in G$. If $|a|$ is infinite, so is $\langle a \rangle$. If $|a| = n \in \mathbb{N}$, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\},$$

and these elements are all distinct.

Examples

The (additive) subgroup of $\mathbb{Z}/20\mathbb{Z}$ generated by $12 + 20\mathbb{Z}$ is

$$\{12 + 20\mathbb{Z}, 4 + 20\mathbb{Z}, 16 + 20\mathbb{Z}, 8 + 20\mathbb{Z}, 0 + 20\mathbb{Z}\},$$

which has $5 = \frac{20}{(12,20)}$ elements, as expected.

The (multiplicative) subgroup of $(\mathbb{Z}/16\mathbb{Z})^\times$ generated by $3 + 16\mathbb{Z}$ is

$$\{3 + 16\mathbb{Z}, 9 + 16\mathbb{Z}, 11 + 16\mathbb{Z}, 1 + 16\mathbb{Z}\},$$

which has $4 = |3 + 16\mathbb{Z}|$ elements.

Cyclic Groups

Definition

A group G is called *cyclic* if there is an $a \in G$ so that $G = \langle a \rangle$. In this case we say that G is *generated* by a.

Since $|a| = \left|\langle a \rangle\right|$, if G is finite we find that

$$G \text{ is cyclic } \Leftrightarrow \quad G \text{ has an element of order } |G|.$$

Since the additive order of $1 + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ is exactly n, we conclude that

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ (under addition) is always cyclic.}}$$

Recall that the additive order of $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ is $\frac{n}{(a,n)}$. Thus:

The (additive) generators of $\mathbb{Z}/n\mathbb{Z}$ are the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$.

The multiplicative structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ is a bit more subtle than the additive structure of $\mathbb{Z}/n\mathbb{Z}$.

For instance, we have:

$(\mathbb{Z}/15\mathbb{Z})^\times$		$(\mathbb{Z}/5\mathbb{Z})^\times$	
Order	Elements	Order	Elements
1	$1 + 15\mathbb{Z}$	1	$1 + 5\mathbb{Z}$
2	$4 + 15\mathbb{Z}, 11 + 15\mathbb{Z}, 14 + 15\mathbb{Z}$	2	$4 + 5\mathbb{Z}$
4	$2 + 15\mathbb{Z}, 7 + 15\mathbb{Z},$ $8 + 15\mathbb{Z}, 13 + 15\mathbb{Z}$	4	$2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}$

This implies that $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic, while $(\mathbb{Z}/15\mathbb{Z})^\times$ *is not*.

Primitive Roots

Goal: Precisely determine those $n \in \mathbb{N}$ for which $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

Definition

An integer $a \in \mathbb{Z}$ for which $\langle a + n\mathbb{Z} \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$ is called a *primitive root modulo n*.

Example. Based on the previous slide, 2 and 3 are primitive roots modulo 5, whereas there are no primitive roots modulo 15.

Note that $a \in \mathbb{Z}$ is a primitive root modulo n iff $(a, n) = 1$ and either:

1. For every $b \in \mathbb{Z}$ with $(b, n) = 1$, there is a $k \in \mathbb{N}$ so that $a^k \equiv b \pmod{n}$; OR
2. The multiplicative order of $a + n\mathbb{Z}$ is $\varphi(n)$.

Primitive Roots Modulo 2^n

Our first general result concerns moduli that are powers of 2.

Theorem 2

Let $n \geq 3$. Then there are no primitive roots modulo 2^n.

Remark. 3 is a primitive root modulo $2^2 = 4$.

Proof. Suppose that $(a, 2^n) = 1$. Then a is odd, and in the HW you proved (exercise 4.2.15) that

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

This means that the multiplicative order of $a + 2^n\mathbb{Z}$ cannot exceed 2^{n-2}.

But $\varphi(2^n) = 2^{n-1}$, so a cannot be a primitive root modulo 2^n. □

Primitive Roots Modulo p^n in General

We will see that 2 is the only "deficient" prime. Specifically, we will (eventually) prove:

Theorem 3

Let p be an odd prime and let $n \in \mathbb{N}$. There exists a primitive root modulo p^n.

Our proof will, of necessity, be nonconstructive.

We will first establish the existence of a primitive root modulo p using a pigeonhole argument.

We will then successively "lift" this element to a primitive root modulo p^n for $n \geq 2$.

Lagrange's Theorem

We begin our hunt for primitive roots with a result on polynomial congruences modulo p.

Theorem 4 (Lagrange)

Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots a_1 X + a_0$ be a polynomial with integer coefficients and let p be prime. If $p \nmid a_n$, then the congruence $f(X) \equiv 0 \pmod{p}$ has at most n distinct solutions modulo p.

Remarks.

- This says that a polynomial congruence modulo p never has more solutions that the degree of the polynomial.
- Compare this to the analogous result on roots of polynomials with real (or complex) coefficients.

Proof. Let $\mathbb{Z}[X]$ denote the set of all polynomials with integer coefficients.

For any $r \in \mathbb{Z}$ define

$$\begin{aligned} T_r : \mathbb{Z}[X] &\to \mathbb{Z}[X], \\ g(X) &\mapsto g(X - r). \end{aligned}$$

Since $T_r^{-1} = T_{-r}$, this is a bijection.

This means that for any $g(X) \in \mathbb{Z}[X]$ there is a unique $h(X) \in \mathbb{Z}[X]$ so that $T_r(h) = g$, i.e.

$$g(X) = h(X - r).$$

The polynomial $h(X)$ is called the *Taylor expansion of* $g(X)$ *at* r.

Write $h(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots b_1 X + b_0$ with $b_i \in \mathbb{Z}$.

Then

$$\begin{aligned} g(X) &= h(X - r) \\ &= b_m (X - r)^m + b_{m-1} (X - r)^{m-1} + \cdots + b_1 (X - r) + b_0 \\ &= (X - r)\widetilde{g}(X) + b_0, \end{aligned}$$

for some $\widetilde{g}(X) \in \mathbb{Z}[X]$.

In particular

$$g(r) = (r - r)\widetilde{g}(r) + b_0 = b_0.$$

We conclude that for any $g(X) \in \mathbb{Z}[X]$ and any $r \in \mathbb{Z}$, there exists a $\widetilde{g}(X) \in \mathbb{Z}[X]$ so that

$$g(X) = (X - r)\widetilde{g}(X) + g(r).$$

We now induct on the degree $n \geq 1$ of $f(X)$.

If $n = 1$, then $f(X) = a_1X + a_0$, and

$$f(X) \equiv 0 \pmod{p} \iff a_1X \equiv -a_0 \pmod{p}.$$

Since $p \nmid a_1$ and p is prime, $(a_1, p) = 1$.

Therefore the linear congruence $a_1X \equiv -a_0 \pmod{p}$ has exactly 1 solution modulo p.

Now fix $n \geq 2$ and suppose we have proven the result for all polynomials in $\mathbb{Z}[X]$ of degree $< n$.

If $f(X) \equiv 0 \pmod{p}$ has no solutions modulo p, then we're finished.

So we may assume there is an $r \in \mathbb{Z}$ so that $f(r) \equiv 0 \pmod{p}$.

Write $f(X) = (X - r)\widetilde{f}(X) + f(r)$ for some $\widetilde{f}(X) \in \mathbb{Z}[X]$.

Suppose $s \not\equiv r \pmod{p}$ satisfies $f(s) \equiv 0 \pmod{p}$.

Then

$$0 \equiv f(s) \equiv (s - r)\widetilde{f}(s) + f(r) \equiv (s - r)\widetilde{f}(s) \pmod{p}.$$

Since $p \nmid (s - r)$ and p is prime, by Euclid's lemma we must have $p|\widetilde{f}(s)$. That is, $\widetilde{f}(s) \equiv 0 \pmod{p}$.

So every solution to $f(X) \equiv 0 \pmod{p}$ that is *different* from r modulo p is actually a solution to $\widetilde{f}(X) \equiv 0 \pmod{p}$.

Since $\deg f(X) \geq 2$ and $f(r)$ is a constant, we must have

$$\begin{aligned} n = \deg f(X) &= \deg((X-r)\widetilde{f}(X) + f(r)) \\ &= \deg((X-r)\widetilde{f}(X)) = 1 + \deg \widetilde{f}(X), \end{aligned}$$

which implies that $\deg \widetilde{f}(X) = n - 1 < n$.

Since $f(X)$ and $\widetilde{f}(X)$ have the same leading coefficient, we find that the inductive hypothesis applies to $\widetilde{f}(X)$.

Therefore the congruence $\widetilde{f}(X) \equiv 0 \pmod{p}$ has at most $n-1$ incongruent solutions modulo p.

Together with our earlier observation, this means that $f(X) \equiv 0 \pmod{p}$ has no more than n incongruent solutions modulo p, which completes our induction. □

Example

Consider $f(X) = X^2 + 1$. Since $5 \equiv 1 \pmod 4$, we know that the congruence $X^2 + 1 \equiv 0 \pmod 5$ has at least one solution modulo 5.

In particular, $f(2) = 5 \equiv 0 \pmod 5$, so we must have

$$X^2 + 1 = (X - 2)\widetilde{f}(X) + 5$$

for some integral polynomial $\widetilde{f}(X)$. Indeed, one can easily check that

$$X^2 + 1 = (X - 2)(X + 2) + 5.$$

It follows immediately that the only other solution to $X^2 + 1 \equiv 0 \pmod 5$ is $X \equiv -2 \equiv 3 \pmod 5$.

Now fix an odd prime p and let $d|\varphi(p) = p - 1$.

Suppose that $a + p\mathbb{Z}$ has multiplicative order d in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Then the first d powers

$$1 + p\mathbb{Z}, a + p\mathbb{Z}, a^2 + p\mathbb{Z}, \ldots, a^{d-1} + p\mathbb{Z}$$

are all distinct, and satisfy

$$(a^k + p\mathbb{Z})^d = a^{kd} + p\mathbb{Z} = (a^d + p\mathbb{Z})^k = (1 + p\mathbb{Z})^k = 1 + p\mathbb{Z}.$$

That is, $1, a, a^2, \ldots, a^{d-1}$ are incongruent modulo p and solve the polynomial congruence

$$X^d - 1 \equiv 0 \pmod{p}.$$

By Lagrange's Theorem, there can be *no other solutions* modulo p.

Therefore if $b + p\mathbb{Z}$ also has order d, then $b \equiv a^k \pmod{p}$ for some k, which means

$$d = |b + p\mathbb{Z}| = |(a + p\mathbb{Z})^k| = \frac{d}{(k, d)} \quad \Rightarrow \quad (k, d) = 1.$$

Thus, the powers $a^k + p\mathbb{Z}$ with $0 \leq k \leq d - 1$ and $(k, d) = 1$ yield *all* elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ with order d.

This proves:

Lemma 1

Let p be an odd prime and let $d|p - 1$. If there is one element in $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d, then there are exactly $\varphi(d)$ of them.

Now let $\psi(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order exactly d.

Lemma 1 implies that $0 \leq \psi(d) \leq \varphi(d)$.

Since every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ has *some* order dividing $p-1$, we have

$$p - 1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d) = p - 1,$$

by Gauss' Theorem.

Therefore

$$\psi(d) = \varphi(d) \quad \text{for all } d|p-1.$$

Primitive Roots Modulo p Exist

This proves our main result of the day.

Theorem 5

Let p be an odd prime and let $d|p-1$. Then there are exactly $\varphi(d)$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d.

Corollary 1

For any odd prime p, there exist exactly $\varphi(p-1)$ (incongruent modulo p) primitive roots modulo p.

Proof. Take $d = p - 1$ in the theorem. □

And, as we have seen in the course of our proof, given one primitive root a modulo p, all the others are given by $a^k \pmod{p}$, for $1 \leq k \leq p-1$ with $(k, p-1) = 1$.

Examples

The following table lists the all the incongruent primitive roots modulo p, for small values of p.

p	Primitive Roots
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27

Remarks

Although one can explicitly compute a primitive root modulo a given prime p, there is no known simple general formula that will produce one for a *generic* (or even infinitely many) p.

Artin's primitive root conjecture asserts that if $a \neq \square, -1$, then a is a primitive root modulo infinitely many primes.

In 1967 Hooley proved that Artin's conjecture is true under the assumption of the *Generalized Riemann Hypothesis* for Dedekind zeta functions.

While Artin's conjecture is unresolved for any specific value of a, Heath-Brown has shown that at least one of 2, 3, or 5 is a primitive root modulo infinitely many primes, and that there are at most two primes for which Artin's conjecture fails.

Primitive Roots Modulo Prime Powers

Ryan C. Daileda

Trinity University

Number Theory

Recall

Given $n \in \mathbb{N}$, a *primitive root modulo n* is an integer a so that

$$(\mathbb{Z}/n\mathbb{Z})^\times = \langle a + n\mathbb{Z} \rangle.$$

Equivalently, for any $b \in \mathbb{Z}$ with $(b, n) = 1$, there exists a $k \in \mathbb{N}$ so that $a^k \equiv b \pmod{n}$.

Last time we used a counting argument to prove that primitive roots modulo primes exist.

Theorem 1

Let $p \in \mathbb{N}$ be prime. Then there are exactly $\varphi(p-1)$ (incongruent modulo p) primitive roots modulo p.

Order Lifting

Today we will treat the case of primitive roots modulo p^n, where p is an *odd* prime.

(Remember that there are *no* primitive roots modulo 2^n for $n \geq 3$).

We will produce primitive roots modulo p^n by "lifting" primitive roots modulo p.

Recall that if $m|n$, then there is a well-defined map

$$r : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$$
$$a + n\mathbb{Z} \mapsto a + m\mathbb{Z}.$$

Lemma 1

If $m|n$ and $(a, n) = 1$, then the order of $a + m\mathbb{Z}$ divides the order of $a + n\mathbb{Z}$.

Proof. Let d denote the order of $a + n\mathbb{Z}$. Then $a^d \equiv 1 \pmod{n}$.

Since $m|n$, this implies $a^d \equiv 1 \pmod{m}$. Thus, $(a + m\mathbb{Z})^d = 1 + m\mathbb{Z}$.

This implies that the order of $a + m\mathbb{Z}$ divides d. □

Corollary 1

Let p be a prime. If a is a primitive root modulo p,then $a + p^2\mathbb{Z}$ has order $p - 1$ or $p(p - 1)$.

Proof. Let d be the order of $a + p^2\mathbb{Z}$. Since

$$\left|(\mathbb{Z}/p^2\mathbb{Z})^\times\right| = \varphi(p^2) = p(p-1),$$

we have $d|p(p - 1)$.

Since $a + p\mathbb{Z}$ has order $p - 1$, by Lemma 1 $p - 1|d$.

Primitive Roots Modulo p^2

So we have $p-1|d|p(p-1)$, which implies $\frac{d}{p-1}$ divides p.

Since p is prime, this means $\frac{d}{p-1}$ is either 1 or p.

That is, $d = p-1$ or $d = p(p-1)$. □

Theorem 2

Let p be an odd prime. If $a \in \mathbb{Z}$ is a primitive root modulo p, then either a or $a+p$ is a primitive root modulo p^2.

Proof. By Corollary 1, $a + p^2\mathbb{Z}$ has either order $p-1$ or $p(p-1)$.

In the second case we are finished.

So we may assume that $a + p^2\mathbb{Z}$ has order $p - 1$.

That is, $a^{p-1} \equiv 1 \pmod{p^2}$.

Since $a \equiv a + p \pmod{p}$, $(a + p) + p\mathbb{Z}$ also has order $p - 1$.

So $(a + p) + p^2\mathbb{Z}$ has order $p - 1$ or $p(p - 1)$, by Corollary 1.

Thus, if we can show that $(a + p)^{p-1} \not\equiv 1 \pmod{p^2}$, we will be finished.

By the Binomial Theorem and our assumption on a we have

$$\begin{aligned}(a+p)^{p-1} &\equiv a^{p-1} + (p-1)a^{p-2}p \pmod{p^2} \\ &\equiv 1 - a^{p-2}p \pmod{p^2}.\end{aligned}$$

If this is $\equiv 1 \pmod{p^2}$, then $a^{p-2}p \equiv 0 \pmod{p^2}$ iff $a^{p-2} \equiv 0 \pmod{p}$ iff $a \equiv 0 \pmod{p}$ (by Euclid's lemma), which contradicts the fact that $(a, p) = 1$.

Thus $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, and the result is proven. □

Theorem 2 gives us an explicit algorithm for constructing primitive roots modulo p^2 from primitive roots modulo p.

Examples

2 is a primitive root modulo 3, which means that 2 or $2 + 3 = 5$ is a primitive root modulo $3^2 = 9$.

Since $2^{3-1} = 4 \not\equiv 1 \pmod 9$, it must be that 2 is a primitive root modulo 9.

The smallest "exception" occurs when $p = 29$. In this case 14 is a primitive root modulo 29.

But $14^{28} \equiv 1 \pmod{29^2}$, so that 14 is *not* a primitive root modulo 29^2.

Instead, $14 + 29 = 43$ is a primitive root modulo 29^2.

Primitive Roots Modulo p^n

For $n \geq 3$, we have the following result concerning primitive roots modulo p^n.

Theorem 3

Let p be an odd prime and $n \geq 3$. If $a \in \mathbb{Z}$ is a primitive root modulo p^{n-1}, then a is a primitive root modulo p^n.

Proof. Let d be the multiplicative order of $a + p^n\mathbb{Z}$. Then $d|\varphi(p^n) = p^{n-1}(p-1)$.

By Lemma 1, the order of $a + p^{n-1}\mathbb{Z}$ divides d as well. Thus

$$\varphi(p^{n-1}) = p^{n-2}(p-1)|d|p^{n-1}(p-1) \quad \Rightarrow \quad \frac{d}{p^{n-2}(p-1)}\Bigg|p.$$

Since p is prime, this implies that $\frac{d}{p^{n-2}(p-1)} \in \{1, p\}$ or

$$d = p^{n-2}(p-1) \text{ or } p^{n-1}(p-1).$$

It therefore suffices to show that $a^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$.

Now Euler's Theorem implies

$$a^{p^{n-3}(p-1)} \equiv 1 \pmod{p^{n-2}} \;\Rightarrow\; a^{p^{n-3}(p-1)} = 1 + kp^{n-2}.$$

However, since a is a primitive root modulo p^{n-1}, $a^{p^{n-3}(p-1)} \not\equiv 1 \pmod{p^{n-1}}$.

It follows that $p \nmid k$.

By the Binomial Theorem we therefore have

$$\begin{aligned} a^{p^{n-2}(p-1)} &= \left(a^{p^{n-3}(p-1)}\right)^p = (1+kp^{n-2})^p \\ &= 1 + \binom{p}{1} kp^{n-2} + \binom{p}{2} k^2 p^{2(n-2)} + \cdots \\ &\qquad \cdots + \binom{p}{p-1} k^{p-1} p^{(p-1)(n-2)} + k^p p^{p(n-2)} \\ &\equiv 1 + kp^{n-1} \not\equiv 1 \pmod{p^n} \end{aligned}$$

since $\binom{p}{m} \equiv 0 \pmod{p}$ for $1 \leq m \leq p-1$, $p, n \geq 3$ and $p \nmid k$.

This is what we needed to show. □

Corollary 2

Let p an odd prime and let $a \in \mathbb{Z}$ be a primitive root modulo p. Then either a or $a + p$ is a primitive modulo p^n for all $n \geq 2$.

Proof. By Theorem 2, either a or $a + p$ is a primitive root modulo p^2. The result follows from Theorem 3 and a quick induction. □

Examples.

- Since 2 is a primitive root modulo 3 and 9, it is a primitive root modulo 3^n for all $n \geq 1$.
- Since 14 is a primitive root modulo 29 and $14 + 29 = 43$ is a primitive root modulo 29^2, 43 is a primitive root modulo 29^n for all $n \geq 2$.

Primitive Roots Modulo Composite Integers in General

We are almost ready completely classify the natural numbers n for which there exist primitive roots.

Lemma 2

Let $m, n \in \mathbb{N}$. Suppose that $(m, n) = 1$ and $m, n \geq 3$. Then there is no primitive root modulo mn.

Proof. Suppose that $(a, mn) = 1$. Then $(a, m) = (a, n) = 1$.

Since $\varphi(m)$ and $\varphi(n)$ are both even, Euler's Theorem implies

$$a^{\frac{\varphi(m)\varphi(n)}{2}} = (a^{\varphi(m)})^{\frac{\varphi(n)}{2}} \equiv 1^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{m},$$
$$a^{\frac{\varphi(m)\varphi(n)}{2}} = (a^{\varphi(n)})^{\frac{\varphi(m)}{2}} \equiv 1^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{n}.$$

Thus $a^{\frac{\varphi(m)\varphi(n)}{2}} \equiv 1 \pmod{mn}$, by the CRT.

So the order of a modulo mn cannot exceed $\frac{\varphi(m)\varphi(n)}{2}$.

But $\frac{\varphi(m)\varphi(n)}{2} = \frac{\varphi(mn)}{2} < \varphi(mn)$.

So a cannot be a primitive root modulo mn. □

We can now eliminate "most" composite numbers from consideration.

Corollary 3

Let $n \in \mathbb{N}$. Then n fails to have a primitive root if either:

1. *n is divisible by two odd primes.*
2. *$n = 2^k p^\ell$, where $k \geq 2$ and p is an odd prime.*

Proof (Sketch). In both cases we can write $n = ab$ with $(a, b) = 1$ and $a, b \geq 3$. □

We now find that the only candidates for moduli for which primitive roots exist are 2, 4, p^k and $2p^k$, where p is an odd prime.

We've seen that primitive roots do, indeed, exist in the first three cases.

It remains to address integers of the form $2p^k$, where p is an odd prime.

Lemma 3

Let p be an odd prime. For any $k \in \mathbb{N}$, there is a primitive root modulo $2p^k$.

Proof. Let a be a primitive root modulo p^k.

Since $a \equiv a + p^k \pmod{p^k}$, $a + p^k$ is also a primitive root modulo p^k.

Since either a or $a + p^k$ is even, we can assume WLOG that a is odd.

Since $(a, p^k) = 1$ by assumption, it follows that $(a, 2p^k) = 1$.

We will show that a is a primitive root modulo $2p^k$.

Let $r = |a + 2p^k\mathbb{Z}|$. By Lemma 1, $\varphi(p^k) = |a + p^k\mathbb{Z}|$ must divide r.

But then we have $\varphi(p^k)|r|\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$.

Hence $r = \varphi(p^k) = \varphi(2p^k)$, and we're finished. □

We have achieved our complete classification!

Theorem 4

Let $n \in \mathbb{N}$. There is a primitive root modulo n if and only if

$$n = 2, 4, p^k, \text{ or } 2p^k,$$

where p is an odd prime.

Remark. Euler, Lagarange, Legendre and Gauss all had a hand in originally proving Theorem 4.

Legendre gave the first complete proof of the existence of primitive roots modulo primes in 1785, and Gauss first proved Theorem 4 in 1801.

Example

Let's find a primitive root modulo $338 = 2 \cdot 13^2$.

Since $\varphi(13) = 12$ and

$$2^2 = 4, 2^3 = 8, 2^4 \equiv 3 \pmod{13}, 2^6 \equiv -1 \pmod{13}$$

2 must be a primitive root modulo 13. And since

$$2^{12} \equiv 40 \not\equiv 1 \pmod{169},$$

2 must also be a primitive root modulo 169.

Since 2 is even, the proof of Lemma 3 tells us that $2 + 169 = 171$ must be a primitive root modulo 338 (or modulo $2 \cdot 13^k$).