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 $|a| = \big|\langle a \rangle\big|$, if G is finite we find that

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

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:

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

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:

$(\mathbb{Z}/15\mathbb{Z})^\times$

Order	Elements
1	$1 + 15\mathbb{Z}$
2	$4 + 15\mathbb{Z}, 11 + 15\mathbb{Z}, 14 + 15\mathbb{Z}$
4	$2 + 15\mathbb{Z}, 7 + 15\mathbb{Z}, 8 + 15\mathbb{Z}, 13 + 15\mathbb{Z}$

$(\mathbb{Z}/5\mathbb{Z})^\times$

Order	Elements
1	$1 + 5\mathbb{Z}$
2	$4 + 5\mathbb{Z}$
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. $\square$

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 $f(X) = a_1 X + a_0$, and

$$f(X) \equiv 0 \pmod{p} \;\Leftrightarrow\; a_1 X \equiv -a_0 \pmod{p}.$$

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

Therefore the linear congruence $a_1 X \equiv -a_0 \pmod{p}$ 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. $\square$

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

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

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. $\square$

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 $a \neq \Box, -1$, 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.