Recall: Last time we proved

- $n = \sum_{d \mid n}' \phi(d)$

- For any polynomial $f(x) \in \mathbb{F}[x]$ of degree $n \geq 1$ with coefficients in a field $\mathbb{F}$, there exist $\leq n$ elements $a \in \mathbb{F}$ such that $f(a) = 0$.

  Example: $x^2 + 1 \in \mathbb{R}[x]$ has 0 roots in $\mathbb{R}$. FINE ✓ $0 \leq 2$.

  We will use the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field for p prime.

Recall: For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ we define $\text{ord}_n(a) = \min\{d \geq 1 : a^d = 1 \bmod n\}$.

It follows from Euler's Totient Theorem that $\text{ord}_n(a) \mid \phi(n)$.

Check: Let $d = \mathrm{ord}_n(a)$ and suppose that $a^m = 1$ for some $m \geq 1$. Then I claim that $d \mid m$.

Proof: Consider the remainder:

$$\begin{cases} m = qd + r \\ 0 \leq r < d. \end{cases}$$

Note $a^r = a^{m-qd} = a^m \cdot (a^d)^{-q}$

$$= 1 \cdot (1)^{-q} = 1 \pmod n.$$

If $r \neq 0$ then $r < d$ contradicts the minimality of d. Hence we must have $r = 0$, and therefore $d \mid m$.

Euler's Totient Theorem says

$$a^{\phi(n)} = 1 \bmod n \quad \text{for } \gcd(a,n) = 1.$$

Hence, $\mathrm{ord}_n(a) \mid \phi(n)$

Recall: If $\text{ord}_n(a) = \phi(n)$ then we say that a is a "primitive root mod n" in which case,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{1, a, a^2, a^3, \ldots, a^{\phi(n)-1}\}$$

Jargon: In this case we say that $((\mathbb{Z}/n\mathbb{Z})^\times, \times, 1)$ is a "cyclic group."

Question: <u>When</u> is $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclic?

Primitive Root Theorem:

$(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for <u>prime</u> p.

(and a few other cases ...)

We need one more lemma before we are ready to prove this.

$\boxed{\text{Lemma:}}$ Let $a, n \in \mathbb{Z}$, $\gcd(a,n) = 1$ and let $d = \mathrm{ord}_n(a)$. Then for all $k \geq 1$ I claim that

$$\boxed{\mathrm{ord}_n(a^k) = \frac{d}{\gcd(k,d)}.}$$

Proof: $\lambda = \gcd(k,d)$

$$\left.\begin{array}{l} d = \lambda d' \\ k = \lambda k' \end{array}\right\} \gcd(d', k') = 1.$$

Want to show that

$$\mathrm{ord}_n(a^k) = \frac{d}{\lambda} = \frac{\lambda d'}{\lambda} = d'.$$

For this we need two things:

1. $(a^k)^{d'} \equiv 1 \mod n.$

2. $(a^k)^m \overset{\text{mod } n}{\equiv} 1 \Rightarrow d' \leq m.$
   $m \geq 1$

①
$$
\begin{aligned}
(a^k)^{d'} &= a^{kd'} \\
&= a^{\lambda k' d'} \\
&= a^{\underline{\lambda d'} k'} \\
&= a^{d k'} \\
&= (a^d)^{k'} = 1 \quad \text{mod } n.
\end{aligned}
$$

② Suppose $m \geq 1$, $(a^k)^m = 1 \text{ mod } n$.

$$a^{km} = 1 \quad \text{mod } n$$

$$
\begin{aligned}
\Longrightarrow \quad \text{ord}_n(a) &\mid km \\
d &\mid km \\
d\ell &= km \quad \text{for some } \ell \in \mathbb{Z}. \\
\cancel{\lambda} d'\ell &= \cancel{\lambda} k' m \\
d'\ell &= k'm
\end{aligned}
$$

$$d' \mid k'm \quad \& \quad \gcd(d', k') = 1$$

$$\underset{\text{Euclid}}{\Longrightarrow} \quad d' \mid m \quad \Longrightarrow \quad d' \leq m \qquad ✓$$

Finally,

Proof of the Primitive Root Theorem.

For all prime p we will show that $\exists\ \phi(p-1)$ primitive roots mod p.

Since $\phi(p-1) \geq 1$, $\exists$ at least one!

Recall that for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have $\mathrm{ord}_p(a) \mid \phi(p) = p-1$

$$\mathrm{ord}_p(a) \mid p-1$$

For any divisor $d \mid p-1$ we define

$$\psi(d) := \#\{a \in (\mathbb{Z}/p\mathbb{Z})^\times : \mathrm{ord}_p(a) = d\}.$$

$= \#$ elements of order d.

Ultimately we want to show that

$$\underbrace{\psi(p-1)}_{\#\text{ primitive roots}} = \phi(p-1).$$

In fact we will prove that for all $d \mid p-1$ we have

$$\psi(d) = 0 \text{ or } \phi(d).$$

Then it will follow that in fact we have $\psi(d) = \phi(d) \ \forall \ d \mid p-1$,

because

$$\underbrace{\sum_{d \mid p-1} \psi(d)}_{\substack{\text{add \# elts} \\ \text{of order } d}} = \underbrace{p-1}_{\substack{\text{total} \\ \text{\# elements}}} \qquad \left(\begin{array}{c}\text{every element} \\ \text{has \underline{some}} \\ \text{order}\end{array}\right)$$

On the other hand, we also know

$$\sum_{d \mid p-1} \phi(d) = p-1 \quad (\text{Lemma}).$$

Combining these gives

$$\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d)$$

Since $\psi(d) = \{0, \phi(d)\}$, this implies that in fact $\psi(d) = \phi(d)$ ✓

[Indirect]

It remains to show that

$$\psi(d) = \underline{0} \text{ or } \underline{\phi(d)}.$$

So fix some divisor $d \mid p-1$.

If $\psi(d) = 0$ then we're done.

elts
order d
mod p

So let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ be some element of order d. Then

$1, a, a^2, \ldots, a^{d-1}$ are all distinct.

And each of them is a root of the polynomial $x^d - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$.

This polynomial has degree d over a field $\mathbb{Z}/p\mathbb{Z}$, so it has at most d roots, hence $1, a, a^2, \dots, a^{d-1}$ are all of the roots.

Let b be any element of order d mod p. Then $b^d \equiv 1 \mod p$

$$b^p - 1 \equiv 0 \mod p.$$

$\Rightarrow$ b is a root of $x^d - 1$

$\Rightarrow$ $b = a^k$ for some $k \geq 1$.

We want to count these elements!

How many elements a^k have order d?

PAUSE

So far we have used the lemmas

- $p-1 = \sum_{d \mid p-1} \phi(d)$
- poly in $\mathbb{Z}/p\mathbb{Z}[x]$ has $\leq$ deg roots.

There is one more lemma we didn't use yet:

- $\text{ord}_p(a^k) = \dfrac{d}{\gcd(k,d)}$.

UNPAUSE

Recall: • $\text{ord}_p(a) = d$

- Every elt. order d has form a^k
- $\text{ord}_p(a^k) = \dfrac{d}{\gcd(k,d)}$. $\overset{?}{=} d$

Observe, this order $= d \iff$ $\gcd(k,d) = 1$.

times this happens is $\phi(d)$.

We conclude that $\psi(d) = \phi(d)$.

Q.E.D.

WHEW!

To summarize: For every prime p, there exists at least one (in fact $\phi(p-1)$) elements a such that

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, 3, \ldots, p-1\}$$
$$= \{1, a, a^2, \ldots, a^{p-2}\}.$$

Sometimes it is useful to express the elements in this form.

Next Topic: Legendre Symbol.

Recall: For $a, p \in \mathbb{Z}$ with p prime, we define the "Legendre symbol" by

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & a \text{ square mod } p, \\ 0 & a \equiv 0 \mod p, \\ -1 & a \text{ not square mod } p. \end{cases}$$

Why did Legendre define such an arbitrary-looking thing?

Because of (yet another) theorem of Euler.

Euler's Criterion: For all $a, p \in \mathbb{Z}$ with p prime, we have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

Consequence: The Legendre symbol is "multiplicative"

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2}$$

$$\equiv a^{(p-1)/2} b^{(p-1)/2}$$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.$$

If $p > 2$, this implies

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

as integers!

Jargon: We have a group homomorphism

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}.$$

Another Notation:

$\left(\frac{\cdot}{p}\right)$ is a "character" of the group $(\mathbb{Z}/p\mathbb{Z})^\times$, called the "quadratic character".

Fits into the subject of analytic number theory and Dirichlet's Theorem that $\exists\ \infty$ many primes $\equiv a \bmod b$ when $\gcd(a,b) = 1$.

Proof of Euler's Criterion.

Want to show

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

First, if $a \equiv 0 \mod p$ then both sides are 0. ✓

So suppose $a \not\equiv 0 \mod p$.

Observe:

$$\left(a^{(p-1)/2}\right)^2 \equiv a^{(p-1)} \underset{\text{Fermat}}{\equiv} 1 \mod p.$$

$a^{(p-1)/2}$ is a square root of $1 \mod p$.

Since p is prime, $\exists \leq 2$ square roots mod p. In fact $+1$ & -1 are the square roots.

$$a^{(p-1)/2} \equiv \pm 1 \mod p.$$

We need to show

$$a^{(p-1)/2} \equiv +1 \quad \text{when } a \text{ square}$$
$$\equiv -1 \quad \text{when } a \text{ not square.}$$

To show this, we will use a <u>primitive root</u>, $g \in (\mathbb{Z}/p\mathbb{Z})^\times$.

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, g, g^2, \dots, g^{p-2}\}.$$

Therefore $a = g^k$ for some k.

I claim:

① $a^{(p-1)/2} \equiv +1 \iff k$ even.

② $\left(\frac{a}{p}\right) = +1 \iff k$ even.

---

① Let $k = 2k'$. Then

$$a^{(p-1)/2} = (g^{2k'})^{(p-1)/2} = (g^{p-1})^{k'} \equiv +1$$

Fermat.

We have shown that

$$\underline{\underline{1, g^2, g^4, \dots, g^{p-1}}}$$

are roots of polynomial $x^{(p-1)/2} - 1$.

Since we have found $(p-1)/2$ distinct roots, there are no more.

i.e. $g^{\text{odd power}}$ <u>is not a root</u>.

[Remark: It will follow from this that exactly half of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares.]

(2) Let $k = 2k'$. Then

$$a = g^k = g^{2k'} = (g^{k'})^2 \text{ is square } \checkmark$$

Conversely, suppose g^k is square mod p, say $g^k = b^2$

But $b = g^l$ for some l since g is a primitive root.

Follows that

$$g^k = (g^l)^2$$

$$g^k = g^{2l}$$

$$g^{k-2l} = 1$$

$$(p-1) \mid (k-2l)$$

$$2 \mid (p-1)$$

$$2 \mid (k-2l)$$

$$\Longrightarrow k \text{ odd.}$$