Generators mod p

Fermat's little thm says if $a \not\equiv 0 \mod p$, then $a^{p-1} \equiv 1 \mod p$.

Recall from week 5 discussion:

Def: The order of $a \mod p$, $\text{ord}_p(a)$ is the smallest positive k s.t. $a^k \equiv 1 \mod p$.

Prop: If $a^n \equiv 1 \mod p$ then $\text{ord}_p(a) \mid n$.

Rephrased, we have

$$a^{p-1} \equiv 1 \mod p \iff \text{ord}_p(a) \leq p-1.$$

Q: Can we ever get equality?

A: Yes!

Def: If $\mathrm{ord}_p(a) = p-1$ then a is called a generator mod p (or primitive root mod p).

Thm: There are $\varphi(p-1)$ generators mod p, for p odd prime.

Lemma 1: Suppose $\mathrm{ord}_p(a) = m$. Then $\mathrm{ord}_p(a^k) = \frac{m}{(k,m)}$ for any $k \geq 1$.

Proof:
We have $(a^k)^{\frac{m}{(k,m)}} = (a^m)^{k/(k,m)} \equiv 1 \bmod p$

So $\operatorname{ord}_p(a^k) \leq k/(k,m)$.

Suppose $\operatorname{ord}_p(a^k) = t$. Then

$(a^k)^t = a^{kt} \equiv 1 \bmod p$

$\Rightarrow m \mid kt$. So $kt = ml$

for some $l \in \mathbb{Z}$ $\Longrightarrow \dfrac{k}{(k,m)} t = \dfrac{m}{(k,m)} l$

Since $\left(\dfrac{k}{(k,m)}, \dfrac{m}{(k,m)}\right) = 1$

$\Rightarrow \dfrac{m}{(k,m)} \mid t \Rightarrow t = \dfrac{m}{(k,m)}$ $\boxtimes$

<u>Corollary</u>: $\operatorname{ord}_p(a^k) = \operatorname{ord}_p(a)$

$\Longleftrightarrow (k, \operatorname{ord}_p(a)) = 1$.

Lemma 2: $\displaystyle\sum_{d|n} \varphi(d) = n$

Proof:

We have $\displaystyle\sum_{d|n} \varphi(d) = \sum_{dd'=n} \varphi(d)$

$$= \sum_{dd'=n} \varphi(d') = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

By def^n, $\varphi\left(\frac{n}{d}\right) = \#\left\{1 \le k \le \frac{n}{d} : \left(k, \frac{n}{d}\right) = 1\right\}$

note for any $m \in \mathbb{N}$, that

$$(m,n) = d \iff \left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

So this says $\varphi\left(\frac{n}{d}\right) = \#\{1 \le m \le n : (m,n) = d\}$.

i.e. $\varphi(\frac{n}{d}) = \#\{\text{integers } m \text{ with } \gcd(m,n)=d\}$

Each m satisfies $(m,n)=d$ for some $1 \le d \le n$, so falls into one of the sets listed above. Summing up the sizes of each set then says

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) \text{ as desired } \boxtimes$$

<u>Lemma 3:</u> If there is an element of order d mod p, there are exactly $\varphi(d)$ elements of order d.

<u>Proof:</u> An element a of order d

is a root of $x^d - 1$ mod p.

This has $\leq d$ roots, and the powers $1, a, a^2, \ldots, a^{d-1}$ are d distinct roots because a has order p, so these are <u>all</u> the roots.

By Lemma 2, the powers with order d are those with exponent relatively prime to d, of which there are $\varphi(d)$. ☒

<u>Theorem</u>: There are $\varphi(p-1)$ generators mod p.

<u>Proof</u>: Any element a has order

d for some $d \mid p-1$. Let $N_d(p)$

$:= \#\{\text{elements of order } d\}$

We have

$$p-1 = \sum_{d \mid p-1} N_p(d) \leq \sum_{d \mid p-1} \varphi(d) = p-1$$

$$\implies N_p(p-1) \neq 0$$

$$\implies N_p(p-1) = \varphi(p-1) \text{ by}$$

lemma 3 ☒

What about mod n?

Turns out: there is a generator

mod n $\iff$ $n = 2, 4, p^k, 2p^k$

for p odd prime.