

Thm: p prime. Then there are $\phi(p-1)$ congruence classes mod p of order $p-1$. (Recall order of $a \pmod{p}$ is smallest n s.t. $a^n \equiv 1 \pmod{p}$)

Remark: g has order $p-1 \Rightarrow \{0, 1, g, \dots, g^{p-2}\}$ is a complete res. sys.

Proof:

Lemma 1: If a has order $h \pmod{m}$, then the integers k for which $a^k \equiv 1 \pmod{m}$ are those k divisible by h .

(Proof last time.)

Lemma 2: If a has order $h \pmod{m}$, then a^k has order $h / (h, k)$.

Proof: By L1, if $r = \text{order } a^k$, $(a^k)^r \equiv 1 \pmod{m} \Rightarrow a^{kr} \equiv 1 \pmod{m} \Rightarrow$

$$h \mid kr. \Rightarrow \frac{h}{(h, k)} \mid \frac{k}{(h, k)} r \quad \left(\frac{h}{(h, k)}, \frac{k}{(h, k)} \right) = 1 \Rightarrow \frac{h}{(h, k)} \mid r$$

On the other hand, $(a^k)^{h/(h, k)} = (a^h)^{1/(h, k)} \equiv 1 \pmod{m}, \Rightarrow$

$r \mid \frac{h}{(h, k)}$ by Lemma 1.

Lemma 3: If a has order h , b order k , $(h, k) = 1$, then ab has order $kh \pmod{m}$.

Proof: $r = \text{order of } ab$.

$$(ab)^{rk} = (a^k)^r (b^k)^r \equiv (1)^r (1)^r \equiv 1 \pmod{m}.$$

By Lemma 1, $r \mid kh$.

$$\text{look at } b^{rh} \equiv (a^h)^r b^{rh} \equiv (ab)^{rh} \equiv 1 \pmod{m}$$

$$\Rightarrow k \mid rh \Rightarrow k \mid r.$$

similarly, $h \mid r. \Rightarrow hk \mid r. \Rightarrow hk = r$

Lemma 4: If $d \mid p-1$, then $x^d = 1 \pmod{p}$ has d solutions. (p prime)

$$d \mid p-1. \quad y^e - 1 = (y-1)(1+y+y^2+\dots+y^{e-1})$$

plug in x^d for y .

$$\underbrace{x^{p-1} - 1}_{p-1 \text{ soln}} = \underbrace{(x^d - 1)}_{d \text{ soln}} \underbrace{(1 + x^d + x^{2d} + \dots + x^{(e-1)d})}_{d(e-1) \text{ soln}}$$

(Fermat's Little Thm) \therefore combining these, $\leq d + d(e-1)$ sol'n to RHS

By counting, must have equality.

Lemma 5: p, q primes. $q^a \mid p-1$. Then there are $q^a - q^{a-1}$ residue classes mod p of order q^a .

proof: $x^{q^a} \equiv 1 \pmod{p}$ has q^a solns.

If $a^h \equiv 1 \pmod{p}$ and a has order $< q^a \Rightarrow \exists h < q^a$ s.t. $a^h \equiv 1 \pmod{p}$.

By Lemma 1, $h \mid q^a \Rightarrow h \mid q^{a-1}. \quad a^{q^{a-1}} \equiv 1 \pmod{p}$.

By Lemma 4, there are q^{a-1} solns to $x^{q^{a-1}} \equiv 1 \pmod{p}$.

Thus, of order q^a there are $q^a - q^{a-1}$ res. classes mod p .

Proof of Thm

$$p-1 = q_1^{a_1} \dots q_r^{a_r}. \quad \exists a_i \text{ of order } q_i^{a_i} \text{ for all } i$$

$g = a_1 \dots a_r$ has order $p-1$ by Lemma 3.

$\{0, g, g^2, \dots, g^{p-1}\}$ is complete residue system.

$$g^{i-j} \equiv 1 \pmod{p} \text{ and } i-j \in \{0, p-1\} \Rightarrow i-j=0.$$

What is order of g^i ?

By Lemma 2, this is $\frac{p-1}{i}$, so those with order $p-1$ are precisely those s.t. $\gcd(i, p-1) = 1$, so there are $\phi(p-1)$ of them.

Def. a is called a quadratic residue mod m if $x^2 \equiv a \pmod{m}$ has a solution. If not, call a a quadratic non-residue. (Don't consider 0)

Ex: $m=7$, what are q.r.'s?

x	1, 2, 3, 4, 5, 6	q.r.'s = {1, 2, 4}
x^2	1, 4, 2, 2, 4, 1	q.n.r.'s = {3, 5, 6}

Def. p odd prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ q.r.} \\ -1 & a \text{ q.n.r.} \\ 0 & p \mid a \end{cases}$$

Thm. p odd prime.

- 1) $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$
- 2) $\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- 3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$