Euler's Theorem :-

Let $a \in \mathbb{Z}_N^*$

$a^i \in \mathbb{Z}_N^*$ $\quad a^i \bmod N$

N is finite $\Rightarrow$ $\mathbb{Z}_N$ is also finite.

a, a^2, a^3, a^4, a^5

$\exists$ k such that $a^i = a^k$ for some $k \in \{0, \ldots i-1\}$.

k is called 'order of a'. / multiplicative order of a modulo N.

↳ smallest k.

Claim:- $a^k = 1$.

By defn $a^i = a^k$.

Since $a \in \mathbb{Z}_N^*$, $\bar{a}^{-1} \in \mathbb{Z}_N^*$

$$\bar{a}^{-1} a^i = \bar{a}^{-1} a^k$$

$$\Rightarrow a^{i-1} = a^{k-1}$$

Therefore, $a^0, a^1, a^2, \ldots, a^{k-1} \in \mathbb{Z}_N^*$ are all distinct.

Theorem:

Let N be a positive integer and $a \in \mathbb{Z}_N^*$ of multiplicative order k. Then for every $i \in \mathbb{Z}$, $a^i \equiv 1 \bmod N$ iff $k \mid i$

More generally, for all $i, j \in \mathbb{Z}$, $a^i \equiv a^j \bmod N$ iff $i \equiv j \bmod k$.

$a^{i-j} \equiv 1 \bmod N$

$i - j \equiv 0 \bmod k$

$\Rightarrow i \equiv j \bmod k$.

If: $a^i \equiv 1 \bmod N$, Now $i = kq + r$, $0 \le r < k$.

$$(a^k)^q \cdot a^r \equiv 1 \bmod N \Rightarrow a^r \equiv 1 \bmod N \Rightarrow r = 0$$

Thm: (Euler's Thm): Let N be a positive integer and $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} \equiv 1 \bmod N$. In particular, the multiplicative order of a divides $\phi(N)$.

Pf: $\tau_a : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ Is τ_a bijective?

$\tau_a(\beta) = a\beta \bmod N$.

$$\prod_{\beta \in \mathbb{Z}_N^*} \beta = \prod_{\beta \in \mathbb{Z}_N^*} a\beta \Rightarrow \prod_{\beta \in \mathbb{Z}_N^*} \beta = a^{\phi(N)} \prod_{\beta \in \mathbb{Z}_N^*} \beta \Rightarrow a^{\phi(N)} \equiv 1 \bmod N.$$

Thm: (Fermat's little Thm): For every prime p, and every $a \in \mathbb{Z}_p$, we have $a^p \equiv a \bmod p$.

Thm: Suppose $a \in \mathbb{Z}_N^*$ has multiplicative order k. Then for every $m \in \mathbb{Z}_1$ multiplicative order of a^m is $k/\gcd(m,k)$.

Thm: (Generalized Fermat's little Thm): For every positive integer N, and every $a \in \mathbb{Z}_N$, $a^N \equiv a^{N-\phi(N)} \bmod N$.

Thm: Show that for all primes p and any integer a.

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

Prove Fermat's little Thm from the above.

If: Let n be the order of a^m.

$\Rightarrow a^{mn} \equiv 1 \bmod N$.

$k \mid mn$.

$(a^m)^{k/\gcd(k,m)}$

$d = \gcd(m,k)$

$dv \mid dun$

$m = du$

$\Rightarrow v \mid n$.

$\Rightarrow (a^k)^{m/\gcd(k,m)} = 1$.

$k = dv$

$n \mid k/\gcd(m,k)$

$n = \alpha \cdot k/\gcd(k,m) + r$.

$0 \le r < n$.

$(a^m)^n = (a^m)^{\alpha k/\gcd(m,k)} \cdot a^{mr}$

Pf: $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

$$a^N = a^{p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}} \mod N.$$

$$= a^{N - \phi(N)}$$

$$= a^{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} - \left[\phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdots \phi(p_r^{e_r})\right]}.$$

$$= a^{\left[p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} - N \cdot \prod \left(1 - \frac{1}{p_i}\right)\right]}$$

$$= a$$

Quadratic Residue modulo N.

$Z \equiv a^2 \bmod N$.

↓

Quadratic Residue modulo N

"a is called the square root of Z mod N"

For any integer m, we define $\left(Z_N^*\right)^m = \left\{ \beta^m : \beta \in Z_N^* \right\}$.

Fact: $(\mathbb{Z}_N^*)^m$ is a non-empty set.

Thm: Let N be a positive integer. Let $\alpha, \beta \in \mathbb{Z}_N^*$ and let m be any integer. Then

(i) if $\alpha \in (\mathbb{Z}_N^*)^m$, then $(\alpha^{-1}) \in (\mathbb{Z}_N^*)^m$.

(ii) if $\alpha \in (\mathbb{Z}_N^*)^m$, $\beta \in (\mathbb{Z}_N^*)^m$, then $\alpha\beta \in (\mathbb{Z}_N^*)^m$.

(iii) if $\alpha \in (\mathbb{Z}_N^*)^m$, $\beta \notin (\mathbb{Z}_N^*)^m$, then $\alpha\beta \notin (\mathbb{Z}_N^*)^m$.

Thm: Let N be a positive integer. For each $\alpha \in \mathbb{Z}_N^*$, and all $l, m \in \mathbb{Z}$ with $\gcd(l, m) = 1$, if $\alpha^l \in (\mathbb{Z}_N^*)^m$, then $\alpha \in (\mathbb{Z}_N^*)^m$.

Pf: $lx + my = 1$ $\quad \alpha^l = \beta^m$, $\beta \in \mathbb{Z}_N^*$.

$$\alpha = \alpha^{lx+my} = \beta^{mx} \cdot \alpha^{my} = (\beta^x \alpha^y)^m \in (\mathbb{Z}_N^*)^m.$$

We will consider $m = 2$.

Defn: An integer a is called is a quadratic residue mod N.
if $\gcd(a, N) = 1$ and $\exists\ b \in \mathbb{Z}$ such that $a \equiv b^2 \bmod N$.
b is called "square root of a mod N"

In otherwords, $[a]$ is called a quadratic residue if

$$[a] \in (\mathbb{Z}_N^*)^2.$$

$$\mathbb{Z}_N = \{[0], [1], \ldots [N-1]\}$$

$$= \{0, 1, \ldots N-1\}$$

Quadratic Residue modulo odd prime p.

Thm: Let p be an odd prime, and $\beta \in \mathbb{Z}_p$. Then $\beta^2 \equiv 1 \bmod p$ iff.

$\beta = \pm 1 \bmod p$.

$p \mid \beta^2 - 1$

$\Rightarrow p \mid (\beta+1)(\beta-1)$

$\Rightarrow 1$ has two square roots $+1 \bmod p$, $-1 \bmod p$.

Thm: Let p be an odd prime and $\gamma, \beta \in \mathbb{Z}_p^*$. Then $\gamma^2 = \beta^2$ iff.

$\gamma = \pm \beta$.

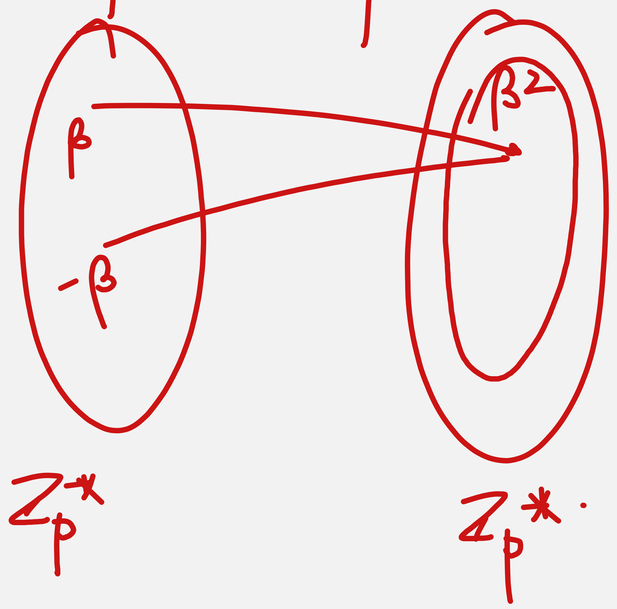
If: $\gamma^2 \equiv \beta^2 \bmod p$.

$\Rightarrow (\gamma/\beta)^2 \equiv 1 \bmod p$.

$\Rightarrow \alpha = \beta^2 \bmod p$, then α has two square roots, $+\beta \bmod p$, $-\beta \bmod p$.

Thm: Let p be an odd prime. Then $|(\mathbb{Z}_p^*)^2| = (p-1)/2$.

Pf: $f: \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, defined as $f(\beta) = \beta^2 \bmod p$.



Half of the elements of $\mathbb{Z}_p^*$ are square and half of the elements of $\mathbb{Z}_p^*$ are non-square.

Thm: (Euler's criteria).

Let p be an odd prime. and $\alpha \in \mathbb{Z}_p^*$.

(i) $\alpha^{(p-1)/2} = \pm 1$

(ii) If $\alpha \in (\mathbb{Z}_p^*)^2$, then $\alpha^{(p-1)/2} \equiv 1 \bmod p$.

(iii) If $\alpha \notin (\mathbb{Z}_p^*)^2$, then $\alpha^{(p-1)/2} \equiv -1 \bmod p$.

Pf:

Let $\gamma = \alpha^{(p-1)/2}$

$\gamma^2 = \alpha^{p-1} \equiv 1 \bmod p$.

$\alpha^{p-1} \equiv 1 \pmod p$

$\Rightarrow \left(\alpha^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$

$\alpha = \beta^2$

$\alpha^{(p-1)/2} = \beta^{p-1} \equiv 1 \bmod p$

$\alpha^2 \equiv \beta \pmod p$

Pf:

(iii) We consider $\varepsilon = \left(\prod_{\beta \in \mathbb{Z}_p^*} \beta\right)$.

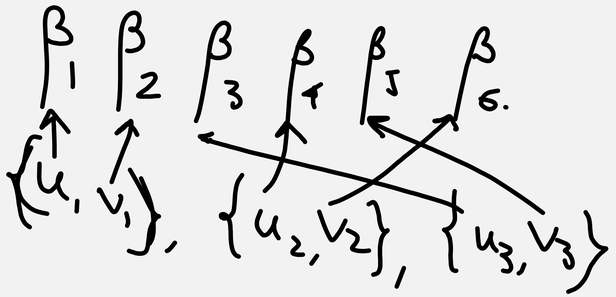
We will show that $\varepsilon = \alpha^{(p-1)/2}$ and $\varepsilon \equiv -1 \bmod p$.

We show that $\prod_{\beta \in \mathbb{Z}_p^*} \beta = \alpha^{(p-1)/2}$.

Fix $\alpha \in \mathbb{Z}_p^*$. and consider a pair of elements $\{u, v\} \subseteq \mathbb{Z}_p^*$ such that $u \cdot v = \alpha$. Can $u = v$

$$\varepsilon = \prod_{\beta \in \mathbb{Z}_p^*} \beta = \prod_{\{u,v\} \subseteq \mathbb{Z}_p^*} u \cdot v$$

$$= \prod_{uv = \alpha} \alpha = \alpha^{(p-1)/2}$$



Fix $1 \in \mathbb{Z}_p^*$

Consider all $\{u, v\} \subseteq \mathbb{Z}_p^*$ such that $uv \equiv 1 \bmod p$.

Can $u = v$?

$u^2 \equiv 1 \bmod p$.

$\Rightarrow u \equiv \pm 1 \bmod p$.

$$\prod_{\beta \in \mathbb{Z}_p^*} \beta = +1 \cdot -1 \cdot \prod_{\{u,v\} \subseteq \mathbb{Z}_p^* \setminus \{1,-1\}} u \cdot v$$

Corollary: Let p be an odd prime. Then

$$\prod_{\beta \in \mathbb{Z}_p^*} \beta \equiv -1 \bmod p.$$

$$= 1 \cdot \prod_{\beta \in \mathbb{Z}_p^*} \beta = (p-1)! \equiv -1 \bmod p.$$

Thm: Let p be an odd prime and $\alpha, \beta \in \mathbb{Z}_p^*$. If $\alpha \notin (\mathbb{Z}_p^*)^2$, and $\beta \notin (\mathbb{Z}_p^*)^2$, then $\alpha\beta \in (\mathbb{Z}_p^*)^2$

Remark: All the results established so far hold true with respect to mod p^e, where p is an odd prime and e be any positive integer.

Thm: Let p be an odd prime and e be a positive integer. Let a be any integer. Then a is a quadratic residue modulo p^e iff a is a quadratic residue mod p.

$$a \in \left(\mathbb{Z}_{p^e}^*\right)^2$$

$\exists b$:

$$a \equiv b^2 \bmod p^e \qquad p \mid p^e \mid (a - b^2)$$

$\gcd(a, p^e) = 1 \Rightarrow \gcd(a, p) = 1$. $p \mid (a - b^2) \Rightarrow a \equiv b^2 \bmod p$.

$a \in \left(\mathbb{Z}_p^*\right)^2$.

Now, we prove that if a is a quadratic residue mod p, then a is a quadratic residue mod p^e.

Let a is not a quadratic residue mod p^e.

- If a is divisible by p, then by defn a is not a quadratic residue mod p.
- Let us assume that a is not divisible by p.

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1).$$

Since, a is not a quadratic residue mod p^e, by Euler's criteria, we have.

$$a^{p^{e-1}\cdot(p-1)/2} \equiv -1 \bmod p^e. \Rightarrow a^{p^{e-1}(p-1)/2} \equiv -1 \bmod p$$

By Fermat's little theorem.

$$a^p \equiv a \bmod p.$$
$$a^{p^2} \equiv a^p \bmod p = a \bmod p.$$
$$a^{p^{e-1}} \equiv a \bmod p.$$
$$\left(a^{p^{e-1}}\right)^{(p-1)/2} \equiv a^{(p-1)/2} \bmod p. \equiv -1 \bmod p.$$

Square roots of $-1 \bmod p$.

Consider an odd prime p.

-1 has a quadratic residue mod p iff and only $p \equiv 1 \bmod 4$.

pf: By Euler's criteria -1 has a quadratic residue mod p iff

$(-1)^{p-1/2} \equiv 1 \bmod p$.

Remark: When $p \equiv 1 \bmod 4$, then any non-square in $\mathbb{Z}_p^*$ yields a square root of -1.

Thm: Let $p \equiv 1 \bmod 4$; $\gamma \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$. Let $\beta = \gamma^{(p-1)/4}$. Then:

$$\beta^2 \equiv -1 \bmod p$$