Theorem: Let $o(a) = k \pmod n$

and $h > 0$, then

$$o(a^h) = \frac{k}{\gcd(h,k)} \text{ (modulo } n)$$

Proof: Let $d = \gcd(h,k)$

$$h = h_1 d \qquad h_1, k_1 \in Z'$$

$$k = k_1 d \qquad (h_1, k_1) = 1$$

$$(a^h)^{k_1} = (a^{h_1 d})^{\frac{k}{d}} = (a^k)^{h_1}$$

$$\equiv 1 \pmod n$$

Let $o(a^h) = r$

$$\Rightarrow (a^h)^r \equiv 1 \pmod n$$

$$\Rightarrow a^{hr} \equiv 1 \pmod n$$

$$\Rightarrow k \mid hr \Rightarrow k_1 d \mid h_1 d r \Rightarrow k_1 \mid h_1 r.$$

as $(k_1, h_1) = 1 \Rightarrow k_1 \mid r$

$$\Rightarrow o(a^h) = k_1 = \frac{k}{d}$$

Quadratic Congruence: An equation of the form $x^2 \equiv a \pmod{p}$ is called quadratic congruence.

1. If $p \mid a$, then $x \equiv 0 \pmod{p}$ is its only solution.

2. To find nontrivial solution, we will assume $p \nmid a$.

3. Let x_0 is a solution of

$$x^2 \equiv a \pmod{p} \quad - \quad (*)$$

then $p - x_0$ is also a solution of $(*)$.

4. $x_0 \not\equiv p - x_0 \pmod{p}$

5. $x^2 \equiv a \pmod{p}$ has exactly two solutions or no solution.

Quadratic Residue of p:

Let $(a,p)=1$, $p>2$ is a prime.

If the quadratic congruence

$$x^2 \equiv a \pmod{p}$$

has a solution, then a is said to be a quadratic residue of p.

Otherwise, a is called quadratic nonresidue of p.

e.g Consider $x^2 \equiv a \pmod{13}$

Find how many of $1,2,3,\ldots,12$ are quadratic residue of p.

$1^2 \equiv 1 \pmod{13}$

$2^2 \equiv 4 \pmod{13}$

$3^2 \equiv 9 \pmod{13}$

$4^2 \equiv 3 \pmod{13}$

161

$5^2 \equiv 12 \pmod{13}$

$6^2 \equiv 10 \pmod{13}$

$7^2 \equiv 10 \pmod{13}$

$8^2 \equiv 12 \pmod{13}$

$9^2 \equiv 3 \pmod{13}$

$10^2 \equiv 9 \pmod{13}$

$11^2 \equiv 4 \pmod{13}$

$12^2 \equiv 1 \pmod{13}$

$\Rightarrow$ 1, 3, 4, 9, 10, 12 are Quadratic residues

and 2, 5, 6, 7, 8, 11 are Quadratic non residues.

Euler's Criterion: Let p be an odd prime and $\gcd(a,p) = 1$. Then a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Proof: suppose that a is a quadratic residue of p, so that $x^2 \equiv a \pmod{p}$ has a solution x_1.

$\therefore \quad (a,p) = 1$

$\Rightarrow \quad (x_1, p) = 1$

By Fermat's theorem $x_1^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \pmod{p}$.

Conversely, Let $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Let r be a primitive root of p. Then

$$a \equiv r^k \pmod{p} \quad \text{for some } k \in \mathbb{Z}$$

$$1 \leq k \leq p-1$$

$$\therefore \quad r^{k\left(\frac{p-1}{2}\right)} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\because \quad o(r) = p-1$$

$$\Rightarrow \quad p-1 \mid \frac{k(p-1)}{2}$$

$$\Rightarrow \quad k = 2j$$

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p}$$

$$\Rightarrow r^j \text{ is a solution of } x^2 \equiv a \pmod{p}$$

$$\Rightarrow a \text{ is a quadratic residue of } p.$$

Result: $(a,p)=1$

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

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Or $$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

not both $\because$ if both hold, then

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

$\Rightarrow p|2$ a contradiction as $p>2$.

A quadratic nonresidue of p does not satisfy $a^{p-1/2} \equiv 1 \pmod{p}$

$$\Rightarrow \quad a^{p-1/2} \equiv -1 \pmod{p}$$

165

Result: Let $p > 2$ be a prime and $(a, p) = 1$. Then a is a quadratic residue or nonresidue of p according to whether

$$a^{p-1/2} \equiv 1 \pmod{p}$$

or

$$a^{p-1/2} \equiv -1 \pmod{p}$$

Exc: $p = 13$

$$2^{13-1/2} = 2^6 \equiv -1 \pmod{13}$$

$\Rightarrow$ 2 is a quadratic nonresidue of 13

$$3^{13-1/2} = 3^6 \equiv 1 \pmod{13}$$

$\Rightarrow$ 3 is a quadratic residue of 13.