Quadratic residues:- Let p be an odd prime.

The squares mod p are "quadratic residues.

The remaining elements are non-residues.

Ex:- $p=11$,

$1^2=1=10^2$

$2^2=4=9^2$

$3^2=9=8^2$

$4^2=5=7^2$

$5^2=3=6^2$

1, 3, 4, 5 and 9 are residues.

2, 6, 7, 8 and 10 are non-residues.

Note:- a is residue mod p, if $a \equiv b^2 \bmod p$.

For $b = 1, 2, 3, \ldots, \frac{p-1}{2}$, $b^2 \equiv a \bmod p$.

$\therefore$ There are 50% residues and 50% non-residu

(Residues are squares of $1, 2, \ldots, \frac{p-1}{2}$).

Generator mod p:- The positive integer g is a generator mod p, if powers of g runs over complete set of residues mod p.

i.e., $\{g, g^2, g^3, \ldots\ldots, g^{p-1}=1\} = \{1, 2, \ldots\ldots, p-1\} \bmod p$.

If g is a generator mod p, then any number a mod p can be written as $a=g^j$, for some j, $0 \leq j \leq p-1$.

Note:- a is residue mod p if and only if $a=g^j$, with j is <u>even</u> integer.

In fact, if a is a quadratic residue, then a is a square of $\pm g^{j/2}$, where g is a generator mod p.

The Legendre symbol :- Let p be an odd prime. Let a be an integer.

Legendre symbol,
$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a quadratic residue mod } p. \\ -1, & \text{if } a \text{ is a non-residue, mod } p. \end{cases}$$

Theorem :- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$

Proof :- If $p \mid a$, then $LHS \equiv 0 \equiv RHS$.

Let $p \nmid a$. $\Rightarrow a^{p-1} \equiv 1 \pmod p$ (F.L.T.)

i.e., $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$.

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

Let g be a generator mod p.

$\Rightarrow a = g^j$

But then a is quadratic residue iff j is even.

Now $a^{p-1/2} = g^{j(p-1)/2}$ and $g^{j(p-1)/2}$ is $+1$

iff $p-1 \mid j(p-1)/2$

i.e., if and only if j is even.

$\therefore\ a^{p-1/2} \equiv 1 \pmod{p}$ if and only if j is even.

$\Rightarrow \left(\dfrac{a}{p}\right) \equiv a^{p-1/2} \bmod p$ (by definition of $\left(\dfrac{a}{p}\right)$.

Properties:- (i) $\left(\dfrac{a}{p}\right)$ depends only on $a \bmod p$.

(ii) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$

(iii) If $\gcd(a,p)=1$, then $\left(\dfrac{ab^2}{p}\right) = \left(\dfrac{a}{p}\right)$.

(iv) $\left(\dfrac{1}{p}\right) = 1$ and $\left(\dfrac{-1}{p}\right) = (-1)^{p-1/2}$

Theorem :- $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Ex:- $\left(\frac{2}{7}\right) = +1 \quad (\because\ 7 \equiv -1 \pmod 8)$

Infact $2 = 3^2 \pmod 7 \Rightarrow 2$ is a residue.

But $\left(\frac{2}{11}\right) = -1 \quad (\because\ 11 \equiv 3 \pmod 8)$

Note: 1, 3, 4, 5 and 9 are the only residues mod 11.

Law of quadratic reciprocity:-

Let p and q be two odd primes. Then,

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) = \begin{cases} -\left(p/q\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ \left(p/q\right), & \text{otherwise.} \end{cases}$$

Note:- $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ for all pairs of odd primes p and q, when atleast one of them is $\equiv 1 \pmod 4$.

$\left(\frac{q}{p}\right) = -\left(p/q\right)$, when both p and q are $\equiv 3 \pmod 4$

Ex:- $\left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right)$ as $11 \equiv 3 \pmod 4$ and. $23 \equiv 3 \pmod 4$

But $\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right)$ as $17 \equiv 1 \pmod 4$

Ex:- $\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right)$ $\left(\because\ 9283 \equiv 3 \pmod 4,\ 7411 \equiv 3 \pmod 4\right)$

$= -\left(\frac{1872}{7411}\right)$ $\left(\because\ 9283 \equiv 1872 \pmod{7411}\right)$

$= -\left(\frac{2^4 \times 3^2 \times 13}{7411}\right)$

$= -\left(\frac{13}{7411}\right)$ $\left(\because\ \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\right)$

$= -\left(\frac{7411}{13}\right)$ $\left(\because\ 13 \equiv 1 \pmod 4\right)$

$= -\left(\frac{1}{13}\right)$ $\left(\because\ 7411 \equiv 1 \pmod{13}\right)$

$= -1$ ⇒ 7411 is a non-residue mod 9283

Ex:- Evaluate the following legendre symbol.

(i) $\left(\frac{11}{37}\right)$ (ii) $\left(\frac{19}{31}\right)$ (iii) $\left(\frac{97}{101}\right)$

(iv) $\left(\frac{43691}{65537}\right)$.