CLASS: Msc MATHEMATICS IV SEM

SUBJECT CODE: H-4049
SUBJECT NAME: NUMBER THEORY

TAUGHT BY:DR SATISH KUMAR
ASSOCIATE PROFESSOR
DEPARTMENT OF MATHEMATICS
DN PG COLLEGE MEERUT

Dr Satish Kr Gupta
M.Sc. IV Sem. (Maths)

Ch-8 Quadratic Congruence And Quadratic Reciprocity Law

Th^m 1→ If the congruence $x^2 \equiv a \pmod{p}$, p is prime, is solvable then it has exactly two solutions.

Proof→ Let $x^2 \equiv a \pmod{p}$, p is prime. → ①

Let x_0 be any solution of ①.

$\Rightarrow x_0^2 \equiv a \pmod{p}$

If we replace x_0 by $(p - x_0)$, then

$(p - x_0)^2 \equiv (0 - x_0)^2 \pmod{p}$

It means $p - x_0$ is also a solution of $x^2 \equiv a \pmod{p}$.

$\Rightarrow x_0^2 \equiv a \pmod{p}$

Let x_1 be the third solution of $x^2 \equiv a \pmod{p}$.

Then

$$x_1^2 \equiv a \pmod{p}$$
$$x_0^2 \equiv a \pmod{p}$$
$$\Rightarrow x_1^2 - x_0^2 \equiv 0 \pmod{p}$$
$$\Rightarrow x_1^2 \equiv x_0^2 \pmod{p}$$
$$\Rightarrow p \mid (x_1 - x_0)(x_1 + x_0)$$
$$\Rightarrow p \mid (x_1 - x_0) \text{ or } p \mid (x_1 + x_0)$$

Now $p \mid (x_1 - x_0)$

$\Rightarrow x_1 \equiv x_0 \pmod{p}$

and $p \mid (x_1 + x_0)$

$\Rightarrow x_1 \equiv -x_0 \pmod{p}$

$\Rightarrow x_1 \equiv p - x_0 \pmod{p}$

$\Rightarrow x_1 \equiv x_0 \pmod{p}$

or $x_1 \equiv (p - x_0) \pmod{p}$

$\Rightarrow x^2 \equiv a \pmod{p}$ has exactly two solutions namely x_0 and $(p - x_0)$.

Th 2→ The congruence $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ ②, p is odd prime has exactly $\frac{1}{2}(p-1)$ solutions.

Proof→ Let $(a,p)=1$, $a \in I^+$, p is odd prime.

Then

$$a^{\phi(p)} \equiv 1 \pmod{p} \qquad \text{[by Fermat's theorem]}$$

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

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

$$\Rightarrow x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p} \longrightarrow ①$$

where $x = a^2 \in \left\{1^2, 2^2, \ldots\ldots, \left[\frac{1}{2}(p-1)\right]^2\right\}$

$\Rightarrow$ Eq^n ① has exactly $\frac{1}{2}(p-1)$ solutions which are $1^2, 2^2, 3^2, \ldots\ldots, \left[\frac{1}{2}(p-1)\right]^2$ respectively.

[As we know if $d \mid p-1$, then $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.
Here $d = \frac{1}{2}(p-1)$ and $\frac{1}{2}(p-1) \mid (p-1)$].

(1.) Find the solution of the congruence

$$x^{11} \equiv 1 \pmod{23}$$

Solu.→ Here $p = 23$ is prime

and $\frac{p-1}{2} = \frac{23-1}{2} = 11$

$\therefore$ $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ has exactly $\frac{1}{2}(p-1)$ solutions

i.e., $x^{11} \equiv 1 \pmod{23}$ has exactly 11 solutions which are

$$1^2 \pmod{23} \equiv 1 \pmod{23}$$
$$2^2 \pmod{23} \equiv 4 \pmod{23}$$
$$3^2 \pmod{23} \equiv 9 \pmod{23}$$
$$4^2 \pmod{23} \equiv 16 \pmod{23}$$
$$5^2 \pmod{23} \equiv 2 \pmod{23}$$

$6^2 \pmod{23} \equiv 13 \pmod{23}$
$7^2 \pmod{23} \equiv 3 \pmod{23}$
$8^2 \pmod{23} \equiv 18 \pmod{23}$
$9^2 \pmod{23} \equiv 12 \pmod{23}$
$10^2 \pmod{23} \equiv 8 \pmod{23}$
$11^2 \pmod{23} \equiv 6 \pmod{23}$

Therefore, the solution of the given congruence is given by

$x \equiv 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 \pmod{23}$ Ans

(2.) Solve the congruence

$$x^2 + 3x + 11 \equiv 0 \pmod{13}$$

Rough Work
Differentiating
$2x + 3$
Squaring
$4x^2 + 9 + 12x$

Solu.→ We have

$$x^2 + 3x + 11 \equiv 0 \pmod{13}$$
$$\Rightarrow 4x^2 + 12x + 44 \equiv 0 \pmod{13}$$
$$\Rightarrow (2x+3)^2 + 35 \equiv 0 \pmod{13}$$
$$\Rightarrow (2x+3)^2 \equiv -35 \pmod{13}$$
$$\Rightarrow (2x+3)^2 \equiv (-35 + 13k) \pmod{13}, \quad k \in I$$
$$\Rightarrow (2x+3)^2 \equiv 4 \pmod{13}, \quad k = 3$$
$$\Rightarrow 2x + 3 \equiv 2 \pmod{13}$$
$$\text{or } 2x + 3 \equiv -2 \pmod{13}$$

$$\Rightarrow 2x \equiv -1 \pmod{13}$$
$$\Rightarrow 2x \equiv (-1 + 13k_1) \pmod{13}, \quad k_1 \in I$$
$$\Rightarrow 2x \equiv 12 \pmod{13}, \quad k_1 = 1$$
$$\Rightarrow x \equiv 6 \pmod{13}, \quad \gcd(2, 13) = 1$$

and $2x + 3 \equiv -2 \pmod{13}$

$$2x \equiv -5 \pmod{13}$$
$$2x \equiv (-5 + 13k_2) \pmod{13}, \quad k_2 \in I$$
$$2x \equiv 8 \pmod{13}, \quad k_2 = 1$$
$$x \equiv 4 \pmod{13} \quad \gcd(2, 13) = 1$$

Hence, the required solutions are

$$x \equiv 4, 6 \pmod{13}$$ Ans

(3.) Solve the congruence

$$x^2 \equiv 5 \pmod{29}$$

Solu.⇒ Given

$$x^2 \equiv 5 \pmod{29}$$
$$\Rightarrow x^2 \equiv (5+29k) \pmod{29}, \quad k \in I$$
$$\Rightarrow x^2 \equiv 121 \pmod{29}, \quad k = 4$$
$$\Rightarrow x^2 \equiv 11^2 \pmod{29}$$
$$\therefore x_1 = 11 = x_0$$
$$x_2 = p - x_0 = 29 - 11 = 18$$

Hence, the required solutions are

$$x \equiv 11, 18 \pmod{29}$$ Ans

(4.) Solve the congruence

$$3x^2 + 5x + 9 \equiv 0 \pmod{11}$$

Solu.⇒ Given

$$3x^2 + 5x + 9 \equiv 0 \pmod{11}$$
$$\Rightarrow 36x^2 + 60x + 108 \equiv 0 \pmod{11}$$
$$\Rightarrow (6x+5)^2 + 108 - 25 \equiv 0 \pmod{11}$$
$$\Rightarrow (6x+5)^2 \equiv -83 \pmod{11}$$
$$\Rightarrow (6x+5)^2 \equiv (-83+11k) \pmod{11}, \quad k \in I$$
$$\Rightarrow (6x+5)^2 \equiv 5 \pmod{11}, \quad k = 8$$

Let $6x + 5 = y$

$$\therefore y^2 \equiv 5 \pmod{11}$$
$$\Rightarrow y^2 \equiv (5+11k_1) \pmod{11}, \quad k_1 \in I$$
$$\Rightarrow y^2 \equiv 16 \pmod{11}, \quad k_1 = 1$$
$$\Rightarrow y^2 \equiv 4^2 \pmod{11}$$
$$\Rightarrow y \equiv 4, -4 \pmod{11}$$

$y = 4$

$$6x + 5 \equiv 4 \pmod{11}$$
$$\Rightarrow 6x \equiv 4 - 5 \pmod{11}$$
$$\Rightarrow 6x \equiv -1 \pmod{11}$$

Rough Work

Differentiating

$6x + 5$

Squaring

$36x^2 + 25 + 60x$

$\Rightarrow 6x \equiv (-1 + 11k_2) \pmod{11}$, $k_2 \in I$

$\Rightarrow 6x \equiv 54 \pmod{11}$, $k_2 = 5$

$\Rightarrow x \equiv 9 \pmod{11}$

$y = -4$

$6x + 5 \equiv -4 \pmod{11}$

$\Rightarrow 6x \equiv -9 \pmod{11}$

$\Rightarrow 6x \equiv (-9 + 11k_3) \pmod{11}$, $k_3 \in I$

$\Rightarrow 6x \equiv 24 \pmod{11}$, $k_3 = 3$

$\Rightarrow x \equiv 4 \pmod{11}$

Hence, the required solutions are

$x \equiv 4, 9 \pmod{11}$ Ans

---

* **Quadratic Residue.**

Suppose p is prime and $\gcd(a, p) = 1$, then a is called a quadratic residue $(\text{mod } p)$ iff $x^2 \equiv a \pmod{p}$ has a solution

For eg → $x^2 \equiv 4 \pmod{5}$

Here, $\gcd(4, 5) = 1$, 5 is prime

and $x^2 \equiv (4 + 5k) \pmod{5}$, for some $k \in I$

$x^2 \equiv 9 \pmod{5}$, $k = 1$

$\Rightarrow x = 3, -3 \pmod{5}$

$\therefore$ Solution exists

$\Rightarrow$ 4 is a quadratic residue $(\text{mod } 5)$.

---

* **Euler's Criterion.**

If p is an odd prime and a is any integer such that $(a, p) = 1$ then a is a quadratic residue $(\text{mod } p)$ iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Ques → Find all the quadratic residue of 23. Also find non-quadratic residue of 23.

Solu → Here $p = 23$

$$\frac{p-1}{2} = \frac{23-1}{2} = 11$$

All quadratic residue of mod 23 are

$1^2, 2^2, 3^2, \ldots\ldots, 11^2 \pmod{23}$

$1^2 \pmod{23} \equiv 1 \pmod{23}$
$2^2 \pmod{23} \equiv 4 \pmod{23}$
$3^2 \pmod{23} \equiv 9 \pmod{23}$
$4^2 \pmod{23} \equiv 16 \pmod{23}$
$5^2 \pmod{23} \equiv 2 \pmod{23}$
$6^2 \pmod{23} \equiv 13 \pmod{23}$
$7^2 \pmod{23} \equiv 3 \pmod{23}$
$8^2 \pmod{23} \equiv 18 \pmod{23}$
$9^2 \pmod{23} \equiv 12 \pmod{23}$
$10^2 \pmod{23} \equiv 8 \pmod{23}$
$11^2 \pmod{23} \equiv 6 \pmod{23}$

Thus, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16 and 18 are quadratic residue of 23.

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

$1^{11} \equiv 1 \pmod{23}$
$4^{11} \equiv 1 \pmod{23}$
$9^{11} \equiv 1 \pmod{23}$
$16^{11} \equiv 1 \pmod{23}$
$2^{11} \equiv 1 \pmod{23}$
$13^{11} \equiv 1 \pmod{23}$
$3^{11} \equiv 1 \pmod{23}$
$18^{11} \equiv 1 \pmod{23}$
$12^{11} \equiv 1 \pmod{23}$
$8^{11} \equiv 1 \pmod{23}$
$6^{11} \equiv 1 \pmod{23}$

Non-quadratic residue of 23 are

5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22

i.e., $5^{11} \equiv -1 \pmod{23}$

$7^{11} \equiv -1 \pmod{23}$

$10^{11} \equiv -1 \pmod{23}$
$11^{11} \equiv -1 \pmod{23}$
$14^{11} \equiv -1 \pmod{23}$
$15^{11} \equiv -1 \pmod{23}$
$17^{11} \equiv -1 \pmod{23}$
$19^{11} \equiv -1 \pmod{23}$
$20^{11} \equiv -1 \pmod{23}$
$21^{11} \equiv -1 \pmod{23}$
$22^{11} \equiv -1 \pmod{23}$

Ques.→ Find the quadratic residue and non-quadratic residue of 13.

Solu→ Here $p = 13$

$$\frac{p-1}{2} = \frac{13-1}{2} = 6$$

All quadratic residue of 13 are
$1^2, 2^2, 3^2, 4^2, 5^2, 6^2 \pmod{13}$

$1^2 \pmod{13} \equiv 1 \pmod{13}$.
$2^2 \pmod{13} \equiv 4 \pmod{13}$
$3^2 \pmod{13} \equiv 9 \pmod{13}$
$4^2 \pmod{13} \equiv 3 \pmod{13}$
$5^2 \pmod{13} \equiv 12 \pmod{13}$
$6^2 \pmod{13} \equiv 10 \pmod{13}$

Total quadratic residue of 13 are
1, 4, 9, 3, 12, 10
i.e., $1, 3, 4, 9, 10, 12 \pmod{13}$ Ans

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

$1^6 \equiv 1 \pmod{13}$
$3^6 \equiv 1 \pmod{13}$
$4^6 \equiv 1 \pmod{13}$
$9^6 \equiv 1 \pmod{13}$
$10^6 \equiv 1 \pmod{13}$
$12^6 \equiv 1 \pmod{13}$

Non-quadratic residue of 13 are
2, 5, 6, 7, 8, 11 Ans

i.e., $2^6 \equiv -1 \pmod{13}$
$5^6 \equiv -1 \pmod{13}$
$6^6 \equiv -1 \pmod{13}$
$7^6 \equiv -1 \pmod{13}$
$8^6 \equiv -1 \pmod{13}$
$11^6 \equiv -1 \pmod{13}$

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

Ques→ Find the quadratic residue and non-quadratic residue of 31.

Solu→ Here $p = 31$

$$\frac{p-1}{2} = \frac{31-1}{2} = 15$$

All quadratic residue of 31 are
$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2 \pmod{31}$

$1^2 \pmod{31} \equiv 1 \pmod{31}$
$2^2 \pmod{31} \equiv 4 \pmod{31}$
$3^2 \pmod{31} \equiv 9 \pmod{31}$
$4^2 \pmod{31} \equiv 16 \pmod{31}$
$5^2 \pmod{31} \equiv 25 \pmod{31}$
$6^2 \pmod{31} \equiv 5 \pmod{31}$
$7^2 \pmod{31} \equiv 18 \pmod{31}$
$8^2 \pmod{31} \equiv 2 \pmod{31}$
$9^2 \pmod{31} \equiv 19 \pmod{31}$
$10^2 \pmod{31} \equiv 7 \pmod{31}$
$11^2 \pmod{31} \equiv 28 \pmod{31}$
$12^2 \pmod{31} \equiv 20 \pmod{31}$
$13^2 \pmod{31} \equiv 14 \pmod{31}$
$14^2 \pmod{31} \equiv 10 \pmod{31}$
$15^2 \pmod{31} \equiv 8 \pmod{31}$

Total quadratic residue of 31 are
1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8
i.e., 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 (mod 31)

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

$1^{15} \equiv 1 \pmod{31}$
$2^{15} \equiv 1 \pmod{31}$
$4^{15} \equiv 1 \pmod{31}$
$5^{15} \equiv 1 \pmod{31}$
$7^{15} \equiv 1 \pmod{31}$
$8^{15} \equiv 1 \pmod{31}$
$9^{15} \equiv 1 \pmod{31}$
$10^{15} \equiv 1 \pmod{31}$
$14^{15} \equiv 1 \pmod{31}$
$16^{15} \equiv 1 \pmod{31}$
$18^{15} \equiv 1 \pmod{31}$
$19^{15} \equiv 1 \pmod{31}$
$20^{15} \equiv 1 \pmod{31}$
$25^{15} \equiv 1 \pmod{31}$
$28^{15} \equiv 1 \pmod{31}$

Non-quadratic residue of 31 are
3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30

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

$3^{15} \equiv -1 \pmod{31}$
$6^{15} \equiv -1 \pmod{31}$
$11^{15} \equiv -1 \pmod{31}$
$12^{15} \equiv -1 \pmod{31}$
$13^{15} \equiv -1 \pmod{31}$
$15^{15} \equiv -1 \pmod{31}$
$17^{15} \equiv -1 \pmod{31}$
$21^{15} \equiv -1 \pmod{31}$
$22^{15} \equiv -1 \pmod{31}$
$23^{15} \equiv -1 \pmod{31}$

$24^{15} \equiv -1 \pmod{31}$
$26^{15} \equiv -1 \pmod{31}$
$27^{15} \equiv -1 \pmod{31}$
$29^{15} \equiv -1 \pmod{31}$
$30^{15} \equiv -1 \pmod{31}$

Theorem. If $(a, p)=1$, $a \in I^+$, p is odd prime then either $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ or $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$.

Proof → Let $(a, p)=1$, where $a \in I^+$ and p is odd prime. Then we have

$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{[by Fermat's theorem]}$$

$$\Rightarrow p \mid (a^{p-1}-1)$$

$$\Rightarrow p \mid [\{a^{\frac{1}{2}(p-1)}\}^2 - 1^2]$$

$$\Rightarrow p \mid (a^{\frac{1}{2}(p-1)}-1)(a^{\frac{1}{2}(p-1)}+1)$$

$$\Rightarrow p \mid a^{\frac{1}{2}(p-1)}-1 \longrightarrow (1)$$

or $$p \mid a^{\frac{1}{2}(p-1)}+1 \longrightarrow (2)$$

Eq^n (1) $\Rightarrow$

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

or

Eq^n (2) $\Rightarrow$

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

Hence, if $(a, p)=1$, then either $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ or $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$.

---

* Legendre symbol and its properties.

If p is an odd prime and a is any integer such that $(a,p)=1$ then Legendre symbol $\left(\frac{a}{p}\right)$ is defined as

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

For eg → ① $\left(\frac{3}{13}\right)$

Here $a=3,\ p=13$

g.c.d.$(3,13)=1$

$$\frac{p-1}{2}=\frac{13-1}{2}=6$$

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

$$3^6\equiv 729 \pmod{13}$$

$$\Rightarrow 3^6\equiv 1 \pmod{13}$$

$\Rightarrow 3$ is a quadratic residue (mod 13)

$$\therefore \left(\frac{3}{13}\right)=1$$

② $\left(\frac{5}{17}\right)$

Here $a=5,\ p=17$

g.cd.$(5,17)=1$

$$\frac{p-1}{2}=\frac{17-1}{2}=8$$

Quadratic residue of 17 are

$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2 \pmod{17}$

i.e.,

$1^2 \pmod{17}\equiv 1 \pmod{17}$

$2^2 \pmod{17}\equiv 4 \pmod{17}$

$3^2 \pmod{17}\equiv 9 \pmod{17}$

$4^2 \pmod{17}\equiv 16 \pmod{17}$

$5^2 \pmod{17}\equiv 8 \pmod{17}$

$6^2 \pmod{17}\equiv 2 \pmod{17}$

$7^2 \pmod{17} \equiv 15 \pmod{17}$

$8^2 \pmod{17} \equiv 13 \pmod{17}$

∴ Quadratic residue of 17 are

$1, 4, 9, 16, 8, 2, 15, 13 \pmod{17}$

i.e., $1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$

∴ 5 is a non-quadratic residue of 17

Hence, $\left(\frac{5}{17}\right) = -1$

Ques→ Evaluate $\left(\frac{2}{19}\right)$.

Solu.→ Here $a = 2$, $p = 19$

$g.c.d(2, 19) = 1$

$$\frac{p-1}{2} = \frac{19-1}{2} = 9$$

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

$$2^9 \equiv 512 \pmod{19}$$

$$2^9 \equiv -1 \pmod{19}$$

∴ 2 is a non-quadratic residue of 19.

Hence, $\left(\frac{2}{19}\right) = -1$ Ans

Ques→ Evaluate $\left(\frac{504}{23}\right)$.

Solu.→ We have $p = 23$, $\frac{p-1}{2} = \frac{23-1}{2} = 11$

$$\left(\frac{504}{23}\right) = \left(\frac{6^2 \times 14}{23}\right)$$

$$= \left(\frac{6^2}{23}\right)\left(\frac{14}{23}\right)$$

$$= \left(\frac{14}{23}\right) \quad \left[\because \overset{g.c.d.}{\wedge}(6, 23) = 1 \Rightarrow \left(\frac{6^2}{23}\right) = 1\right]$$

2	504
2	252
2	126
3	63
3	21
7	7
	1

Now quadratic residue of 23 are

$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2 \pmod{23}$

i.e., $1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 \pmod{23}$

⇒ 14 is non-quadratic residue of 23

$\therefore \left(\frac{504}{23}\right) = -1$ Ans (13) $\left[\because \left(\frac{14}{23}\right) = -1\right]$

Theorem.→ If p is an odd prime and a and b are any integers coprime to p then the Legendre symbol has the following properties:

(i) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) $\left(\frac{a^2}{p}\right) = 1$

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, (iv) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$

Proof→ Let p is an odd prime and g.c.d. $(a, p) = 1$, g.c.d. $(b, p) = 1$, $a, b \in I^+$

(i) To prove $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is quadratic residue of } p \\ -1, & \text{if } a \text{ is non-quadratic residue of } p \end{cases}$

a is quadratic residue mod $p \Leftrightarrow x^2 \equiv a \pmod p$ has a solution
$\Leftrightarrow x^2 \equiv b \pmod p$ has a solution $\longrightarrow$ (1)
$[\because a \equiv b \pmod p]$

Again,
if a is non-quadratic residue mod $p \Leftrightarrow x^2 \equiv a \pmod p$ does not have solution
$\Leftrightarrow x^2 \equiv b \pmod p$ does not have solution $\longrightarrow$ (2)

From (1) and (2), we have
$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) To prove $\left(\frac{a^2}{p}\right) = 1$

Since the integer a satisfies the congruence
$x^2 \equiv a^2 \pmod p$
This means $x^2 \equiv a^2 \pmod p$ has a solution.
Therefore, $\left(\frac{a^2}{p}\right) = 1$

(iii) To prove $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

$$\text{L.H.S.} = \left(\frac{ab}{p}\right)$$
$$= (ab)^{\frac{1}{2}(p-1)}$$
$$= a^{\frac{1}{2}(p-1)} \cdot b^{\frac{1}{2}(p-1)}$$
$$= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$
$$= \text{R.H.S.}$$

(iv) $\left(\frac{1}{p}\right) = (1)^{\frac{1}{2}(p-1)}$

$= 1$, clearly

$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$

Theorem → If p is an odd prime then

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$$

Proof → Let g.c.d. $(a,p)=1$, where $a \in I^+$ and p is odd prime

Let r be a primitive root of p.

$\Rightarrow r, r^2, r^3, \ldots\ldots, r^{\phi(p)}$ are just a permutation of $1, 2, 3, \ldots\ldots, (p-1) \pmod p$.

Thus for any a, $1 \leq a \leq (p-1)$, $\exists$ a unique integer k, $1 \leq k \leq (p-1)$ such that

$$a \equiv r^k \pmod p$$

Now $\left(\frac{a}{p}\right) = \left(\frac{r^k}{p}\right)$

$$\equiv (r^k)^{\frac{1}{2}(p-1)} \pmod p$$
$$\equiv \{r^{\frac{1}{2}(p-1)}\}^k \pmod p$$
$$\equiv (-1)^k \pmod p$$

[$\because r$ is primitive root of p so $r^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$]

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) \equiv \sum_{k=1}^{p-1}(-1)^k \pmod p \qquad (15)$$

We know in $\left(\frac{a}{p}\right)$, there are $\frac{1}{2}(p-1)$ quadratic residues mod p and $\frac{1}{2}(p-1)$ are non-quadratic residues mod p.

$$\Rightarrow \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$$

Theorem → Let $(m_1, m_2)=1$, then a is quadratic residue of $m_1 m_2 \Leftrightarrow a$ is quadratic residue common to both m_1 and m_2.

Proof → Let $(m_1, m_2)=1$

Let a is quadratic residue of $m_1 \Leftrightarrow x^2 \equiv a \pmod{m_1}$
a is quadratic residue of $m_2 \Leftrightarrow x^2 \equiv a \pmod{m_2}$ } → (1)

Now consider

$$\left.\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \end{aligned}\right\} \longrightarrow (2)$$

$$, (m_1, m_2) = 1$$

Let the system (1) has solution x_0.

(1) $\Rightarrow$

$$\left.\begin{aligned} x_0 \equiv x_1 \pmod{m_1} &\Rightarrow x_0^2 \equiv x_1^2 \pmod{m_1} \\ x_0 \equiv x_2 \pmod{m_2} &\Rightarrow x_0^2 \equiv x_2^2 \pmod{m_2} \end{aligned}\right\} \longrightarrow (3)$$

Put $x = x_0$ in (1)

$$\left.\begin{aligned} x_0^2 &\equiv a \pmod{m_1} \\ x_0^2 &\equiv a \pmod{m_2} \end{aligned}\right\} \longrightarrow (4)$$

Now (3) and (4) $\Rightarrow$

$$x_0^2 \equiv x_1^2 \equiv a \pmod{m_1}$$
$$x_0^2 \equiv x_2^2 \equiv a \pmod{m_2}$$
$$\Rightarrow x_0^2 \equiv a \pmod{m_1 m_2}$$
$\Rightarrow a$ is quadratic residue of $m_1 m_2$.

Ques→ Find all quadratic residue of 35.

Solu.→ $35 = 5 \times 7$
$= m_1 \times m_2$

$m_1 = 5,\ m_2 = 7$
$(m_1, m_2) = 1$

All quadratic residue of 5 less than 35 are
1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 26, 29, 31, 34

As $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$
$a^{\frac{1}{2}(5-1)} \equiv 1 \pmod 5$
$a^2 \equiv 1 \pmod 5$

[a is quadratic residue mod p $\Rightarrow a^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$]

For $m_2 = 7$, $a^{\frac{1}{2}(7-1)} \equiv 1 \pmod 7$
$a^3 \equiv 1 \pmod 7$

∴ Quadratic residue of 7 less than 35 are
1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32

Common residues are
1, 4, 9, 11, 16, 29
which are quadratic residue of 35.

---

* Gauss Lemma.

Let p be an odd prime number and let $\gcd(a,p)=1$, where a is a positive integer. If n denotes the number of integers in the set

$$S = \left\{1a, 2a, 3a, \ldots\ldots, \left(\frac{p-1}{2}\right)a\right\}$$

whose remainders upon division by p is greater than $\frac{p}{2}$, then

$$\left(\frac{a}{p}\right) = (-1)^n$$

Proof→ Let $\gcd(a,p)=1$, $a \in I^+$, p is odd prime.

Let

$$S = \left\{1.a, 2a, 3a, \ldots\ldots, \left(\frac{p-1}{2}\right)a\right\}$$

Out of these none of integers is congruent to zero and none are congruent to each other (mod p).

Let $r_1, r_2, \ldots, r_m$ be those remainders mod p such that $0 < r_i < \frac{p}{2}$ and let $s_1, s_2, s_3 \ldots, s_n$ be those remainders mod p such that

$$\frac{p}{2} < s_i < p$$

then $m + n = \frac{1}{2}(p-1)$

and the integers $r_1, r_2, \ldots, r_m, p-s_1, p-s_2, \ldots, p-s_n$ are all distinct positive and less than $\frac{p}{2}$.

If not

$r_i = p - s_j$ for some $i \neq j$

$\Rightarrow \exists$ integers u and v s.t. $1 < u \leq \frac{p-1}{2}$

$$1 \leq v \leq \frac{p-1}{2}$$

satisfying

$$s_j \equiv ua \pmod{p}$$
$$r_i \equiv va \pmod{p}$$

$$s_j + r_i \equiv (u+v)a \pmod{p}$$
$$p \equiv (u+v)a \pmod{p}$$
$$\Rightarrow (u+v)a \equiv p \pmod{p}$$
$$\Rightarrow (u+v)a \equiv 0 \pmod{p}$$
$$\Rightarrow (u+v)a \equiv 0 \cdot a \pmod{p}$$
$$\Rightarrow (u+v) \equiv 0 \pmod{p}, \quad (a,p) = 1$$

which is a contradiction as $1 \leq u < \frac{1}{2}(p-1)$

$$1 \leq v < \frac{1}{2}(p-1)$$

$\Rightarrow r_1, r_2, \ldots, r_m, p-s_1, p-s_2, \ldots, (p-s_n)$ are all distinct.

We know that these numbers $r_1, r_2, \ldots, r_m, p-s_1, p-s_2, \ldots, p-s_n$ equals $1, 2, 3, \ldots, \left(\frac{p-1}{2}\right)$ in some order.

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots \frac{1}{2}(p-1) = r_1 r_2 \ldots r_m (p-s_1)(p-s_2)\ldots(p-s_n)$$

$$\left\{\frac{1}{2}(p-1)\right\}! \equiv r_1 r_2 \ldots r_m (-s_1)(-s_2)\ldots(-s_n) \pmod{p}$$
$$\equiv (-1)^n r_1 r_2 \ldots r_m s_1 s_2 \ldots s_n \pmod{p}$$

We know

$r_1, r_2, \ldots, r_m, s_1, s_2, \ldots s_n$ are congruent to $a, 2a, \ldots \frac{1}{2}(p-1)a$ in some order

$$\left[\frac{1}{2}(p-1)\right]! = (-1)^n \{1a.2a.3a \ldots \left(\frac{p-1}{2}\right)a\} \pmod p \quad (13)$$

$$= (-1)^n \left[\frac{1}{2}(p-1)\right]! \, a^{\frac{1}{2}(p-1)} \pmod p$$

$$1 = (-1)^n a^{\frac{1}{2}(p-1)} \pmod p$$

$$(-1)^n \equiv (-1)^n (-1)^n a^{\frac{1}{2}(p-1)} \pmod p$$

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

$$a^{\frac{1}{2}(p-1)} \equiv (-1)^n \pmod p$$

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

Ques.→ Evaluate n of Gauss Lemma for $\left(\frac{5}{13}\right)$

Solu.→ Here $a = 5$, $p = 13$

$$\therefore \frac{p-1}{2} = \frac{13-1}{2} = 6$$

So, $S = \{1.5, 2.5, 3.5, \ldots \left(\frac{p-1}{2}\right)5\}$

$$= \{5, 10, 15, 20, 25, 30\}$$

Now
$5 \pmod{13} \equiv 5 \pmod{13}$
$10 \pmod{13} \equiv 10 \pmod{13}$
$15 \pmod{13} \equiv 2 \pmod{13}$
$20 \pmod{13} \equiv 7 \pmod{13}$
$25 \pmod{13} \equiv 12 \pmod{13}$
$30 \pmod{13} \equiv 4 \pmod{13}$

$$\frac{p}{2} = \frac{13}{2} = 6.5$$

The integers greater than $\frac{p}{2}$ are 10, 7, 12. These are three in numbers.

$\therefore \boxed{n = 3}$ Ans

Ques.→ Evaluate n of Gauss Lemma for $\left(\frac{5}{19}\right)$.

Solu.→ Here $a = 5$, $p = 19$

Therefore, $\frac{p-1}{2} = \frac{19-1}{2} = 9$

So, $S = \{1.5, 2.5, 3.5, \ldots \left(\frac{p-1}{2}\right)5\}$

$S = \{5, 10, 15, 20, 25, 30, 35, 40, 45\}$

Now
$5 \pmod{19} \equiv 5$
$10 \pmod{19} \equiv 10$
$15 \pmod{19} \equiv 15$
$20 \pmod{19} \equiv 1$
$25 \pmod{19} \equiv 6$
$30 \pmod{19} \equiv 11$
$35 \pmod{19} \equiv 16$
$40 \pmod{19} \equiv 2$
$45 \pmod{19} \equiv 7$

$\frac{p}{2} = \frac{19}{2} = 9.5$

The integers greater than $\frac{p}{2}$ are 10, 15, 16, 11
There are four in numbers.

$\therefore \boxed{n = 4}$ Ans

Ques → Evaluate n of Gauss lemma for $\left(\frac{11}{23}\right)$.

Solu → Here $a = 11$, $p = 23$

$\therefore \frac{p-1}{2} = \frac{23-1}{2} = 11$

So, $S = \left\{1.11, 2.11, 3.11, \ldots \left(\frac{p-1}{2}\right).11\right\}$

$= \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121\}$

Now
$11 \pmod{23} \equiv 11$
$22 \pmod{23} \equiv 22$
$33 \pmod{23} \equiv 10$
$44 \pmod{23} \equiv 21$
$55 \pmod{23} \equiv 9$
$66 \pmod{23} \equiv 20$
$77 \pmod{23} \equiv 8$
$88 \pmod{23} \equiv 19$
$99 \pmod{23} \equiv 7$
$110 \pmod{23} \equiv 18$
$121 \pmod{23} \equiv 6$

$\frac{p}{2} = \frac{23}{2} = 11.5$

The integers greater than $\frac{p}{2}$ are 22, 21, 20, 19, 18
There are five in numbers.

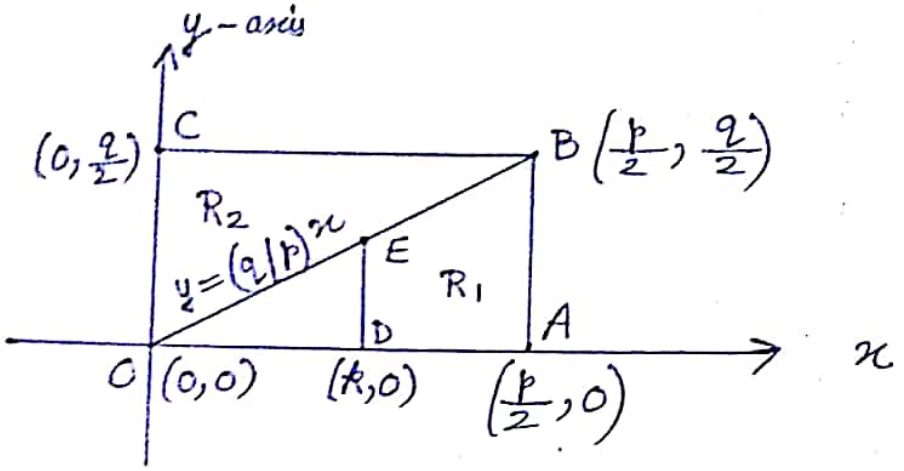
$\therefore \boxed{n = 5}$ Ans

* Quadratic Reciprocity Law:

Theorem. If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}, \quad (p,q)=1$$

Proof →



We consider a rectangular region R with vertices $O(0,0)$, $A\left(\frac{p}{2},0\right)$, $B\left(\frac{p}{2},\frac{q}{2}\right)$ and $C\left(0,\frac{q}{2}\right)$ as in figure.

A lattice point (m,n) inside the boundary $OABC$ satisfies

$$1 \leq m \leq \frac{p-1}{2}$$

$$1 \leq n \leq \frac{q-1}{2}$$

Since p and q are odd

$$\therefore mn = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \quad \text{(total lattice points)} \longrightarrow (1)$$

Now, equation of OB is

$$y = \frac{q}{p}x \longrightarrow (2)$$

To show there is no lattice point on OB.

Suppose (m,n) lies on OB.

$$\Rightarrow n = \frac{q}{p}m$$

$$\Rightarrow pn = qm$$

$$\Rightarrow p \mid qm$$

$$\Rightarrow p \mid m \qquad [\because (p,q)=1]$$

But p cannot divide m as $m < \left(\frac{p-1}{2}\right)$

$\Rightarrow (m,n)$ cannot lie on OB.

(21) Let R_1 be the region OAB and R_2 be the region OBC.

Coordinates of E are $\left(k, \frac{q}{p}k\right)$ $\left(\frac{p-1}{2}\right)$

$\therefore$ Total no. of lattice points in $R_1 = \sum_{k=1}^{} \left[\frac{q}{p}k\right]$

Similarly, total no. of lattice points in $R_2 = \sum_{k=1}^{\left(\frac{q-1}{2}\right)} \left[\frac{p}{q}k\right]$

$\therefore$
$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\left(\frac{p-1}{2}\right)} \left(\frac{q}{p}k\right) + \sum_{k=1}^{\left(\frac{q-1}{2}\right)} \left(\frac{p}{q}k\right) \longrightarrow (3)$$

By Gauss theorem,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left(\frac{q}{p}k\right) + \sum_{k=1}^{\left(\frac{q-1}{2}\right)} \left(\frac{p}{q}k\right)}$$

$$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \qquad \text{(from (3))}$$

Theorem → If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if both } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Proof → We know that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

$$= \begin{cases} 1, & \text{if } \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \text{ is even} \\ -1, & \text{if } \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \text{ is odd} \end{cases}$$

$$= \begin{cases} 1, & \text{if at least one of } p \text{ and } q = 4k+1 \\ -1, & \text{if both } p \text{ and } q = 4k+3 \end{cases}$$

$$= \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Hence proved.

Theorem. If p is an odd prime then

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

Hence,

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$$

Proof → By Gauss Lemma, we have

$$\left(\frac{2}{p}\right) = (-1)^n$$

where n is the number of positive integers in the set

$$S = \left\{2.1, 2.2, 2.3, \ldots\ldots, 2.\left(\frac{p-1}{2}\right)\right\}$$

which on division by p have the remainder greater than $\frac{p}{2}$.

Suppose $2k < \frac{p}{2}$

We have $k < \frac{p}{4}$

$\Rightarrow$ There are $\left[\frac{p}{4}\right]$ integers in the above set less than $\frac{p}{2}$.

Therefore,

$n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$, where $[\cdot]$ denotes bracket function

Since p is odd prime, so p must be of the form $8k+1$ or $8k+3$ or $8k+5$ or $8k+7$

Now,

if $p = 8k+1 \Rightarrow n = 4k - 2k = 2k$

if $p = 8k+3 \Rightarrow n = 4k+1-2k = 2k+1$

if $p = 8k+5 \Rightarrow n = 4k+2-(2k+1) = 2k+1$

and if $p = 8k+7 \Rightarrow n = 4k+3-(2k+1) = 2k+2$

$$\left(\frac{2}{p}\right) = (-1)^n$$

$$= \begin{cases} 1, & \text{if } p = 8k+1 \text{ or } p = 8k+7 \\ -1, & \text{if } p = 8k+3 \text{ or } p = 8k+5 \end{cases}$$

(23) $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$

Now consider

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} (-1)^{\frac{(8k+1)^2-1}{8}}, & \text{if } p = 8k+1 \\ (-1)^{\frac{(8k+3)^2-1}{8}}, & \text{if } p = 8k+3 \\ (-1)^{\frac{(8k+5)^2-1}{8}}, & \text{if } p = 8k+5 \\ (-1)^{\frac{(8k+7)^2-1}{8}}, & \text{if } p = 8k+7 \end{cases}$$

$$= \begin{cases} (-1)^{\frac{64k^2+16k}{8}}, & \text{if } p = 8k+1 \\ (-1)^{\frac{64k^2+48k+8}{8}}, & \text{if } p = 8k+3 \\ (-1)^{\frac{64k^2+80k+24}{8}}, & \text{if } p = 8k+5 \\ (-1)^{\frac{64k^2+112k+48}{8}}, & \text{if } p = 8k+7 \end{cases}$$

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p = 8k+1 \text{ or } p = 8k+7 \\ -1, & \text{if } p = 8k+3 \text{ or } p = 8k+5 \end{cases}$$

$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

$$\Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Hence proved.

---

* **Jacobi's symbol.**

If $p > 1$ is an odd integer and $p = p_1 p_2 p_3 \cdots\cdots p_r$ where each p_i is prime then for any integer a, the Jacobi's symbol denoted by $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1 p_2 \cdots\cdots p_r}\right)$$

$$= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\cdots\left(\frac{a}{p_r}\right)$$

Theorem. If $a \equiv b \pmod{p}$, Then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof → Let $p = p_1 p_2 \cdots p_r$

Then

$a \equiv b \pmod{p} \Leftrightarrow a \equiv b \pmod{p_i}$, $i = 1, 2, \ldots, r$

$\Rightarrow \left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$

Hence

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$

$$= \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_r}\right)$$

$$= \left(\frac{b}{p}\right)$$

Hence proved.